Office of Inspector General

OFFICE OF TECHNOLOGY, FINANCIAL, AND ANALYTICS

EVALUATION REPORT -

THE DEPARTMENT OF ENERGY'S UNCLASSIFIED CYBERSECURITY PROGRAM - 2020

DOE-OIG-21-18
MARCH 2021

Department of Energy
Washington, DC 20585

March 25, 2021

Memorandum for The Secretary

Teri L. Donaldson

From: Teri L. Donaldson
Inspector General

Subject: Evaluation Report on "The Department of Energy's Unclassified Cybersecurity Program – 2020"

Highlights

What We Reviewed and Why

The Department of Energy operates many facilities across the Nation that depend on information technology systems and networks for essential operations required to accomplish its 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. In its *Federal Information Security Modernization Act of 2014 Fiscal Year 2019 Report to Congress*, the Office of Management and Budget reported that the number of agency-reported incidents across the Federal Government decreased by 8 percent between fiscal years (FY) 2018 and 2019. However, this decline in incidents did not at all indicate a reduction in the cybersecurity threat posed to the Federal Government. In fact, the systems used to support the Department's various missions continue to face millions of cybersecurity threats each year, ranging from unsophisticated hackers to advanced persistent threats using state-of-the-art intrusion tools and techniques. In addition, during FY 2020, the Department faced the unprecedented challenge of maintaining security over its information and systems even as a large component of its workforce worked remotely in response to COVID-19.

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's cybersecurity program for FY 2020.

What We Found

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 throughout FY 2020 to address previously identified weaknesses related to its cybersecurity program. In particular, programs and sites made progress remediating weaknesses identified in our FY 2019 evaluation, which resulted in the closure of 42 of 54 (78 percent) prior year recommendations. Although these actions were positive, our current evaluation identified weaknesses in areas, including, but not limited to, system integrity of web applications, configuration management, vulnerability management, access controls, and contingency planning, many of which were consistent with our prior reports. In addition, although the types of deficiencies identified were mostly consistent with our prior evaluations, our FY 2020 review disclosed weaknesses at several new locations. For example, we found the following:

- Weaknesses related to system integrity of web applications were identified at four locations. The weaknesses included applications that accepted malicious input data and files that could have been used to launch attacks against legitimate application users. 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.

- Configuration management weaknesses existed at two sites. For instance, firewall rules at one location were not configured properly and allowed certain systems to inappropriately access an industrial control system and related devices at the site. At the same location, we also found several devices that were configured with default credentials and others that were configured to allow connections without authentication. The use of secure configurations that emphasize hardening of systems against flaws can result in greater levels of security and protection from future vulnerabilities.

- Seven locations reviewed had critical- and/or high-risk vulnerabilities on the workstations and servers tested. For example, we determined that 293 of 1,449 (20 percent) workstations tested and 23 of 308 (7 percent) servers tested were operating systems and/or applications with missing patches/updates that had not been applied within each location's established timeframes. At one location, we determined that there were 12,256 high-risk vulnerabilities related to missing security patches or software no longer supported by the vendor on at least 145 of the 365 workstations included in our sample at that location. Because our testing only included a sample of workstations and servers, it is likely that the locations reviewed had many more vulnerabilities than our test results demonstrated.

- Although the Department had corrected previously identified weaknesses related to access controls, new issues were identified at four locations. For instance, our test work identified weaknesses related to inappropriate database role assignments. In addition, we identified inappropriately implemented password requirements and session lock settings.

- Weaknesses related to the implementation of information system contingency planning requirements existed at six locations. Specifically, one location had not adequately protected the confidentiality and integrity of system backup information, nor had officials appropriately designed and documented necessary components related to contingency plan testing. At the same location, training for personnel with contingency plan roles and responsibilities did not fully address contingency plan elements. Another site had not updated its business impact assessment since 2013, including identification of information technology resources considered critical to the site's mission. A third site did not have processes in place to develop and implement business impact assessments, contingency plan testing, or information system backup and storage that included the use of alternate storage and processing sites. Further, as noted in our report, *Contingency Planning Efforts for Information Technology Mission Support Systems at Selected Department of Energy Locations* (DOE-OIG-21-08, December 2020), we found that three of the four sites reviewed had not fully developed information system contingency plans in accordance with Federal requirements.

The weaknesses identified throughout our evaluation of the Department's unclassified cybersecurity program occurred for a variety of reasons. For instance, the identified weaknesses related to system integrity of web applications generally occurred because those applications were configured without implementing adequate security controls designed to reject malicious input. In addition, vulnerability management programs at the sites reviewed did not always include testing processes and procedures to identify vulnerabilities related to attacks against web application functionality. We also noted that vulnerability management weaknesses existed at one location because the vulnerability management process was not fully effective in addressing known vulnerabilities, including those related to unsupported software and missing patches. For instance, although weekly authenticated scans were conducted at the site, processes for analyzing, prioritizing, tracking, and remediating discovered vulnerabilities had not been fully established and/or implemented.

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. In addition, because cybersecurity remains a challenge area for the Department, it is important that programs and sites remain vigilant in making continued improvements to the Department's overall security posture. Furthermore, 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.

Subsequent to our test work, it was reported that Federal agencies, including the Department and the National Nuclear Security Administration, encountered a serious and sophisticated cybersecurity attack. Due to the timing of our review, we did not evaluate the circumstances surrounding any potential impact to the Department or the National Nuclear Security Administration, or how such an attack could have impacted our results, if at all. We will continue to follow developments related to any potential impact as we continue our future test work.

What We Recommend

To correct the cybersecurity weaknesses identified throughout the Department, we made 83 recommendations to programs and sites during FY 2020 to include those identified during this evaluation and in other issued reports. Corrective actions to address each of the recommendations, 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.

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 Comments

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 4.

cc: Acting Deputy Secretary
Chief of Staff
Acting Administrator, National Nuclear Security Administration

Table of Contents

Background and Objective

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 under the purview of the National Nuclear Security Administration, Under Secretary for Science and Energy, Energy Information Administration, and certain staff offices. Our review included network and application control testing, technical vulnerability scanning, and validating corrective actions taken to remediate prior year weaknesses. To the extent appropriate, we also relied on results from Office of Inspector General reviews conducted in fiscal year (FY) 2020, and conducted test work at five Department locations to assess cybersecurity program maturity, according to the *Federal Information Security Modernization Act of 2014* security metrics issued by the Department of Homeland Security, the Office of Management and Budget, and the Council of the Inspectors General on Integrity and Efficiency.

Our FY 2020 evaluation determined that the Department had taken actions to address previously identified weaknesses. Specifically, Department programs and sites had taken corrective actions related to vulnerability and configuration management, access controls, and system integrity of web applications, which resulted in the closure of 42 of 54 (78 percent) recommendations made during our prior year evaluation. Although the Department's actions 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 2020 revealed that most identified weaknesses were similar in type to those identified during prior evaluations.

Report Objective

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

Results of Review

Our FY 2020 evaluation identified weaknesses related to system integrity of web applications, configuration management, vulnerability management, access controls, contingency planning, system development lifecycle, audit and accountability, 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 2020 review disclosed weaknesses at several new locations. Specifically, our test work resulted in 29 new and 6 repeat recommendations at 9 different locations.

System Integrity of Web Applications

While the Department had taken action to remediate two of its prior year findings, two other prior findings remained open. Furthermore, we identified weaknesses related to system integrity of web applications at two additional locations. In particular, we found that 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 application access. At one of the locations, the web application did not verify whether an authenticated user was authorized to access files stored within the application, which could have allowed an attacker to obtain files uploaded to the application by other users.

The identified weaknesses related to system integrity of web applications generally occurred because cybersecurity officials had not configured web application session management with adequate application level security controls designed to decline malicious input. 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 attacks against web application functionality. 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.

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, including the continuation of one prior year finding 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 several firewalls had not been properly configured to restrict access to internal enclaves and included unnecessary rules that could have allowed more access than necessary. For example, multiple firewalls had rules that could have permitted any system in the "Users" enclave to access the Supervisory Control and Data Acquisition (SCADA) system and related devices through at least one unsecure protocol. During testing, we determined that firewalls did not properly restrict access to 50 SCADA or SCADA-related devices over this unsecured protocol. Without an effective configuration change review process, unauthorized firewall rule changes may not be detected and could potentially allow unauthorized access to restricted resources.

- At the same location, we identified configuration management weaknesses related to access control issues on network systems, including weak authentication configurations. For instance, several devices were configured with default credentials, and others were configured to allow connections without authentication. In addition, several servers' names were set to "public," which could have allowed an attacker to obtain detailed information and configuration settings in order to prepare more sophisticated attacks. Without effective configuration management procedures and practices related to access controls over the addition of systems into the production environment, unauthorized access to key systems and the disclosure or unauthorized modification of sensitive information could occur.

- Another location had developed a corrective action plan to address prior year recommendations related to configuration management weaknesses. While most of the flaws detected in FY 2019 had been remediated, and vulnerability management procedures, information technology asset compliance, and validation procedures had been updated, officials had not completed actions included in the corrective action plan to address the identified conditions, causes, and recommendations. In addition, during our FY 2020 review, we identified similar types of weaknesses that were noted in the prior year. While the site had developed a plan to address the weaknesses, certain phases were not scheduled for completion until after our test work was completed.

The identified weaknesses related to configuration management at one location occurred, in part, because site officials had not performed quarterly firewall reviews and/or spot tests to determine the effectiveness of firewall rules in accordance with the site's procedure. Weaknesses also occurred because the site had not fully developed and implemented configuration management policies and procedures for all types of information technology devices. For instance, the site's configuration management process did not ensure that anonymous access was disabled and that default credentials were changed for all types of devices and services prior to connecting them to the network. At another location, weaknesses were due, in part, to configuration management processes not ensuring that anonymous access and default credentials were changed prior to connecting the systems to the production network and throughout the system lifecycle.

Vulnerability Management

The Department had taken actions to address many of the vulnerability management weaknesses identified in our prior review. However, this year, we continued to note that vulnerability management remains a challenge, including identification of critical- and high-risk vulnerability management weaknesses related to unsupported software or missing patches at seven locations. Vulnerability management is the process of identifying, evaluating, and either mitigating or formally accepting the risks.

Our review determined the following:

- Six locations reviewed were running unsupported software on network servers and/or workstations. In particular, we identified workstation and server operating systems that were no longer supported, including Red Hat Linux, Mac OS X, and Windows Server 2008, at various sites. For instance, our limited testing at one location found critical- and high-risk vulnerabilities related to unsupported software on 6 of 15 (40 percent) servers tested. Furthermore, six locations reviewed had unsupported software running on workstations. Officials at one of those locations stated that action had been taken to address the identified vulnerabilities, and all but two had been remediated as of August 2020.

- Seven locations were operating workstations and servers that had missing critical- and high-risk vulnerability security patches and/or updates. In particular, we found that 293 of 1,449 (20 percent) workstations tested were operating with missing patches and/or updates that had not been applied within each location's established timeframes. At 1 location, 145 of 365 (40 percent) workstations tested had missing patches that could have addressed critical- and high-risk vulnerabilities. For instance, we identified 12,256 high-risk vulnerabilities on the 365 workstations tested. At another location, 79 of 271 (29 percent) workstations tested had missing patches to address critical- and high-risk vulnerabilities. We also determined that 23 of 308 (7 percent) servers tested at 6 locations were missing critical- or high-risk patches and/or updates. For instance, at 1 location, 4 of 9 servers tested were missing patches to address critical- and high-risk vulnerabilities. While this was an improvement over the prior year's results in this area, it is important that the Department maintains its focus on vulnerability management to ensure continued improvement.

The vulnerability management weaknesses noted above occurred for many reasons. For instance, at one site, the vulnerability management process was not fully effective in addressing known vulnerabilities, including vulnerabilities related to unsupported software and missing patches. Although the site conducted weekly authenticated scans, processes for analyzing, prioritizing, tracking, and remediating discovered vulnerabilities had not been fully established and/or implemented. Without effective vulnerability management practices, applications that are missing security patches for known vulnerabilities are at risk for malicious attacks that could give attackers unauthorized access to and/or control of the applications or, potentially, the site's network.

Access Controls

Access controls enable the authorized use of a resource while preventing its use in an unauthorized manner. Although the Department corrected four of the access control-related weaknesses identified during our prior year review, one remained open and our current evaluation identified new weaknesses related to access controls at four locations. For instance:

- Two locations had various weaknesses related to access controls. For example, one site had not fully implemented its plan for managing passwords, and user profiles were not in compliance with defined password requirements. During our prior year review, the same location had a similar finding, and corrective actions had not been fully implemented at the time of our current review. Another site had not appropriately implemented password requirements and session lock settings dictated by applicable policies and procedures. Inadequate security controls over account passwords increase the risk that accounts may be compromised, and that financial or other sensitive information may be inappropriately modified or altered. In addition, inconsistent implementation of entity-level information technology policies and procedures increases the risk that controls will be ineffective or inadequate to prevent against threats.

- At two locations, we identified weaknesses related to database account management. Specifically, at one site, a non-privileged user was inappropriately assigned a database administrator role. Similarly, officials at another site granted users sensitive roles in a production database. The site also granted financial roles without the appropriate approvals and had not disabled or removed accounts in a timely manner. Absent proper database account management, these weaknesses may result in non-privileged users executing privileged functions on the databases and increase the risk of modifying the data contained within those databases.

- At one location, we found that the access authorization processes for users of two separate applications had not been defined in its policies and procedures. As such, officials had not sufficiently documented new user authorizations or approvals. Instead, new users for those applications were approved verbally, and sufficient evidence of those user access authorizations was not maintained. The lack of an explicit requirement for written documentation of authorization increased the risk of inappropriate access to systems and data and could result in the unauthorized access to and modification of financial information.

The identified weaknesses related to access controls occurred because site officials had not performed periodic reviews, based on job duties and continuing need, of user and/or privileged accounts to determine if the accounts should be disabled, removed, or reauthorized. For example, at one location, database administrator accounts were created prior to the implementation of procedures for privileged database account management. Although the database administrator accounts were periodically reviewed and reauthorized by management, no such review was performed on non-administrator accounts. As a result, the database administrator role that was inappropriately assigned was never identified and removed. At another site, a user requested Human Resource-related sensitive roles in the development environment, but the roles were also incorrectly added to the production database. At the same location, expired accounts remained active in the production database because disabling and/or removing the accounts was a manual process, and no routine review of the expired accounts had occurred.

In addition to the findings above, our recent report, *Security of Information Technology Peripheral Devices at Select Office of Science Locations* (DOE-OIG-20-47, July 2020), disclosed access control weaknesses at two Office of Science locations in which peripheral devices had not been securely configured to protect against unauthorized access. Moreover, none of the four sites reviewed had fully implemented security standards found within the Department's Office of the Chief Information Officer's removable media policy, including requiring that all mass storage devices provided encryption, ensured onboard antivirus capability, and used only government-furnished equipment. During our followup review, we noted that actions had been taken at the two locations to address the issues we identified. As a result, the findings were closed this year.

Contingency Planning

Our evaluation of contingency planning activities identified multiple weaknesses at various locations. For instance:

- At one location, the confidentiality and integrity of system backup information was not adequately protected in accordance with Federal guidance related to moderate impact information. Officials indicated that information contained on most of the site's server backups, which included potentially sensitive business information, was not encrypted at rest. Furthermore, it was unclear whether the site's Authorizing Official was aware of the risk these practices presented.

- Components related to contingency plan testing were not adequately designed and documented. Although site officials indicated that a contingency plan test had been conducted in conjunction with its incident response plan, we found little evidence to support that contingency planning activities had been considered. For instance, testing material did not disclose specific information related to contingency planning activities such as an assessment of the disruption impact and damaged equipment, coordination of activities, or necessary recovery and reconstitution procedures. At the same location, training for personnel with contingency plan roles and responsibilities did not adequately address specific contingency plan elements, such as coordination and communication, reporting procedures, and security requirements.

- Two locations did not have required policies or procedures in place. Specifically, one site had not updated its business impact assessment since 2013, including identification of information technology resources considered critical to the site's mission. A business impact assessment predicts the consequences of disruption on a business function and process, and gathers information needed to develop recovery strategies. The other location did not have processes in place to ensure business impact assessments, contingency plan testing, or information system backup and storage were fully implemented.

- Our recent report, *Contingency Planning Efforts for Information Technology Mission Support Systems at Select Department of Energy Locations* (DOE-OIG-21-08, December 2020), found that three of the four sites reviewed had not fully implemented contingency planning requirements related to development of a Business Impact Analysis as identified in Federal requirements. In addition, sites had not fully developed information system contingency plans in accordance with Federal guidance for 10 of the 17 systems reviewed. Even when contingency plans were developed, some were missing key information pertaining to specific information systems.

The identified weaknesses occurred, in part, because officials had not ensured that potentially sensitive data at rest was protected in accordance with Federal requirements. Although the site had implemented numerous contingency planning-related security controls to protect its information and systems, the weaknesses we identified related to encryption of data could put the confidentiality and integrity of its sensitive information at risk. In addition, the issues related to contingency plan testing and related training could leave personnel unable to execute contingency planning responsibilities should an actual emergency occur. Further, the weaknesses we identified related to the Department's information technology mission support systems and functions were due primarily to inappropriate interpretations of contingency planning requirements by Federal and contractor officials.

System Development Lifecycle

Our evaluation disclosed deficiencies related to the system development lifecycle at one location. In particular, the site completed a conversion from an on-premise application to a cloud-hosted application, but testing related to the system development lifecycle and implementation identified that certain controls were not fully designed and implemented. Specifically, the site mapped its common controls to the cloud application's complementary user entity controls, or control requirements that are the user entity's responsibility, and determined that the controls substantially met the site's requirements. However, a review of the crosswalk identified deficiencies in policy and procedure documentation supporting the control's design within the cloud environment and insufficient evidence supporting implementation of several controls.

The issues identified at the site occurred, in part, because management approved the cloud application's production implementation prior to completing testing and design processes to ensure controls would be implemented and operating effectively at the implementation date. Additionally, officials had not designed or implemented a process for managing the use of cloud-based services that included reviewing the cloud service provider's security documentation prior to the system's implementation. Insufficiently designed and implemented general controls may increase the risk of system data being inappropriately accessed or modified. Without appropriate monitoring of system activity, such changes could go undetected in the site's human capital application, which includes sensitive personal and financial data.

Audit and Accountability

Our evaluation of audit logging and monitoring controls at select sites revealed weaknesses at one location. In particular, audit logging and monitoring had not been implemented on one database application used by the site and was not fully implemented on another. Specifically, privileged account activities were logged on one database application, but there was no routine monitoring or review of event logs. Furthermore, audit logs were not retained for 180 days, as required by the site. Finally, database administrators had read and write access to the directory where the database logs resided, which could have allowed them to update and delete audit logs without detection.

The identified weaknesses occurred because the system security plan only required the implementation of operating system and network events to be collected and analyzed. Site officials had not conducted an analysis to determine the feasibility of implementing database audit logging and monitoring controls or performed subsequent activities to properly accept the risk of not implementing these controls. In addition, due to limited storage capacity, database administrators aligned audit log retention time with the backup retention period. Database administrators were also given Oracle account access to perform their job duties within the database, which also gave them read and write access to audit log files. The data in the databases was used for financial reporting for environmental management systems and other business applications. Without effective database audit logging and monitoring controls, the weaknesses noted during our review may increase the risk of modifying financial data.

Cybersecurity and Privacy Training

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

- Two locations had not fully developed and implemented a cybersecurity training program. Specifically, neither site had defined nor communicated roles and responsibilities for security awareness and stakeholder training across the organization. Although one of the locations had annual cybersecurity training requirements in place, officials had not established rules of behavior for all its users despite having a Plan of Action and Milestones (POA&M) in place since 2016 with a scheduled completion of 2017. As of December 2020, the site had implemented a briefing that required user acknowledgement of the rules of behavior and had closed the POA&M. Site officials reported that 75 percent of users had completed the briefing. Officials from the second site reported that they did not have a security awareness and training strategy or plan in place and did not have policies and procedures for security awareness or specialized security training. The site had previously identified this issue and had an open POA&M since April 2018 to address these deficiencies.

- Two sites had not provided role-based privacy training for individuals responsible for managing or conducting activities that involved personally identifiable information (PII). Federal guidance requires targeted role-based privacy training for personnel having responsibility for PII or for activities that involve PII. In today's digital world, effective privacy for individuals depends on the safeguards employed within the information systems that are processing, storing, and transmitting PII, and the environments in which those systems operate. Through the implementation of a privacy training and awareness strategy, the organization would promote a culture of privacy.

The issues noted above occurred because site officials had not ensured that cybersecurity and privacy training policies were fully developed and implemented. For instance, we noted that one site had not adequately defined training requirements within its policies and procedures. In addition, two sites had not adequately defined privacy requirements in policies and procedures in accordance with 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. Specifically, one location was in the process of rebuilding its continuous monitoring program but still had numerous activities to complete. Although draft documents were provided by site officials, those policies and procedures had not been finalized at the time of this review. In addition, our review of the documents determined that they did not include items such as a detailed identification of primary stakeholder roles and responsibilities, the organization's defined risk tolerance, and continuous monitoring program performance measures. The second site had not developed and communicated a continuous monitoring strategy. As such, there were no processes in place for performing ongoing system-level security control assessments or monitoring. Site personnel stated that they were in the process of developing an overarching POA&M corrective action item to address these deficiencies.

During our recent audit of cybersecurity activities at a Department location, we found that officials had not developed a security controls self-assessment plan or fully tested controls for any of the site's systems. In fact, the effectiveness of security controls for one of the site's systems had not been assessed in over 2 years. Although Headquarters officials had performed annual assessments at the site, the majority of weaknesses identified by the assessment teams that were older than 90 days had not been documented as a POA&M, and site officials could not verify whether any corrective actions had occurred.

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. Absent an effective continuous monitoring process, officials may be unable to maintain an ongoing awareness of the security impact of changes to the operating environment in support of organizational risk management decisions.

Risk to Information and Systems

Without improvements to address the weaknesses identified, the Department's information systems and data may be at a higher-than-necessary risk of compromise, loss, and/or modification. This underscores the crucial need to focus efforts on maturing the Department's overall security posture. For instance, persistent findings at several Department sites related to system integrity of web applications could have allowed malicious attacks, resulting in unauthorized access to sensitive data that could have affected application functionality. Attackers could leverage web application vulnerabilities to gain unauthorized access to the application's functionality and sensitive data. In addition, these vulnerabilities could allow an attacker to gain unauthorized access to authorized users' desktops or other systems and applications on the internal network. Finally, web application attacks could disrupt normal business operations or have a negative impact on application and data reliability.

Furthermore, we continue to identify deficiencies related to developing, updating, and/or implementing policies and procedures that could adversely affect the Department's ability to properly secure its information systems and data. Also, without effective access controls, the weaknesses noted during our review may increase the risk of unauthorized system or data modification. Further, without a comprehensive cybersecurity training program, individuals may not be fully aware of their role in the Department's cybersecurity program. They also may not understand their responsibilities related to the proper use and protection of the information and technology resources entrusted to them. During our FY 2020 review, we found that locations had made progress to close findings from our previous reviews and, in some cases, had implemented mitigating controls to reduce the risk from other findings.

Notably, in 2020, the Department issued its High Value Asset Program Plan designed to ensure that high value assets are properly identified and assessed, and that appropriate cybersecurity capabilities are implemented. In addition, throughout 2020 it issued multiple amplification guides related to Department Order 205.1C, *Department of Energy Cybersecurity Program*. These included the *Authorizing Official Guidebook*, *Information System Security Officer Guide* and *POA&M Guide*. However, it remains to be seen how the plans and guidance will be implemented by the Department's elements. While these are positive steps, our test work determined that additional action is necessary to further strengthen the Department's unclassified cybersecurity program.

Recommendations

To correct the cybersecurity weaknesses identified throughout the Department, we made 83 recommendations to programs and sites during FY 2020 to include in this evaluation and other issued reports. Specifically, throughout the year, we made recommendations to each of the locations where weaknesses were identified. Recommendations were related to areas such as system integrity of web applications, configuration management, vulnerability management, and access controls. During the fiscal year, we also issued reports and recommendations related to areas such as security over information technology peripheral devices and contingency planning at selected locations. Corrective actions to address each of the recommendations, if fully implemented, should enhance the Department's unclassified cybersecurity program. In some instances, we also provided opportunities for improvement at reviewed locations but did not issue them as formal findings and recommendations.

Management Comments

Management concurred with the recommendations issued to its programs and sites related to improving the Department’s overall cybersecurity program. Management noted that it will continue to address each of these weaknesses at all organizational levels to adequately protect the Department’s information assets and systems from harm.

Management’s comments are included in Appendix 4.

Office of Inspector General Response

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

Appendix 1

Commonly Used Terms

Department of Energy	Department or DOE
Fiscal Year	FY
Office of Inspector General	OIG
Personally Identifiable Information	PII
Plan of Action and Milestones	POA&M
Supervisory Control and Data Acquisition	SCADA

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 were in accordance with Federal and Department requirements.

Scope

We conducted the evaluation from March 2020 through January 2021 at 28 Department locations primarily under the responsibility of the Acting Administrator for the National Nuclear Security Administration, Administrator for the U.S. Energy Information Administration, Acting Under Secretary for Science and Energy, and certain staff offices. Of the 28 locations reviewed, 5 were selected for Office of Inspector General (OIG) reviews to measure program maturity in accordance with the *Federal Information Security Modernization Act of 2014* metrics established by the Department of Homeland Security, the Office of Management and Budget, and the Council of the Inspectors General on Integrity and Efficiency. The focus of our evaluation was the Department's unclassified cybersecurity program. This work involved a limited review of general information technology controls in areas such as security assessments, 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 A20TG008.

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 measure cybersecurity program maturity in alignment with the *Federal Information Security Modernization Act of 2014* metrics established by the Department of Homeland Security, the Office of Management and Budget, and the Council of the Inspectors General on Integrity and Efficiency. The metric reviews were conducted at five locations across various Department 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. 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 March 16, 2021.

Appendix 3

Related Reports

Office of Inspector General

- Audit Report on *Contingency Planning Efforts for Information Technology Mission Support Systems at Selected Department of Energy Locations* (DOE-OIG-21-08, December 2020). The Office of Inspector General initiated this audit to determine whether the Department of Energy had adequately planned for the restoration of information technology mission support systems and functions in accordance with established requirements to ensure functionality in the event of a disruption. We found that the Department had not always adequately planned for the restoration of information systems in accordance with established requirements to ensure availability and functionality in the event of a disruption. Specifically, we found that three of the four sites reviewed had not fully implemented contingency planning requirements related to the development of a Business Impact Analysis as identified in Federal requirements. In addition, sites had not fully developed Information System Contingency Plans in accordance with Federal guidance for 10 of the 17 systems reviewed. Even when Information System Contingency Plans were developed, some were missing key information pertaining to specific information systems.

- Evaluation Report on the *Security over Information Technology Peripheral Devices at Select Office of Science Locations* (DOE-OIG-20-47, July 2020). The Office of Inspector General initiated an evaluation to determine whether the Department's Office of Science secured information technology peripheral devices in accordance with Federal and Department requirements. Our review focused on technical and policy controls for the following types of peripheral devices: printers, scanners, copiers, fax machines, Voice over Internet Protocol phones, thumb drives, and external hard drives. Our evaluation of devices at four Office of Science locations identified weaknesses related to access controls and configuration settings. The deficiencies were similar in type to those identified in prior evaluations of the Department's unclassified cybersecurity program.

- 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 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 2020* (DOE-OIG-20-09, November 2019). The challenges identified for fiscal year (FY) 2020 remained largely consistent with previous years. These challenges included Contract Oversight, Contractor Management, Subcontract Management, 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 – 2019* (DOE-OIG-20-12, November 2019). The Department, including the National Nuclear Security Administration, had taken actions to address previously identified weaknesses related to its cybersecurity program. Programs and sites made progress remediating weaknesses identified in our FY 2018 evaluation, which resulted in the closure of 21 of 25 (84 percent) 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, cybersecurity and privacy training, security control testing, and continuous monitoring.

- 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. 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.

Government Accountability Office

- *INFORMATION TECHNOLOGY: Agencies and OMB Need to Continue Implementing Recommendations on Acquisitions, Operations, and Cybersecurity* (GAO-20-311T, December 2019)

- *DATA CENTER OPTIMIZATION: Agencies Report Progress, but Oversight and Cybersecurity Risks Need to Be Addressed* (GAO-20-279, March 2020)

- *INFORMATION TECHNOLOGY: DHS Directives Have Strengthened Federal Cybersecurity, but Improvements Are Needed* (GAO-20-133, February 2020)

- *CLOUD COMPUTING SECURITY: Agencies Increased Their Use of the Federal Authorization Program, but Improved Oversight and Implementation Are Needed* (GAO-20-126, December 2019)

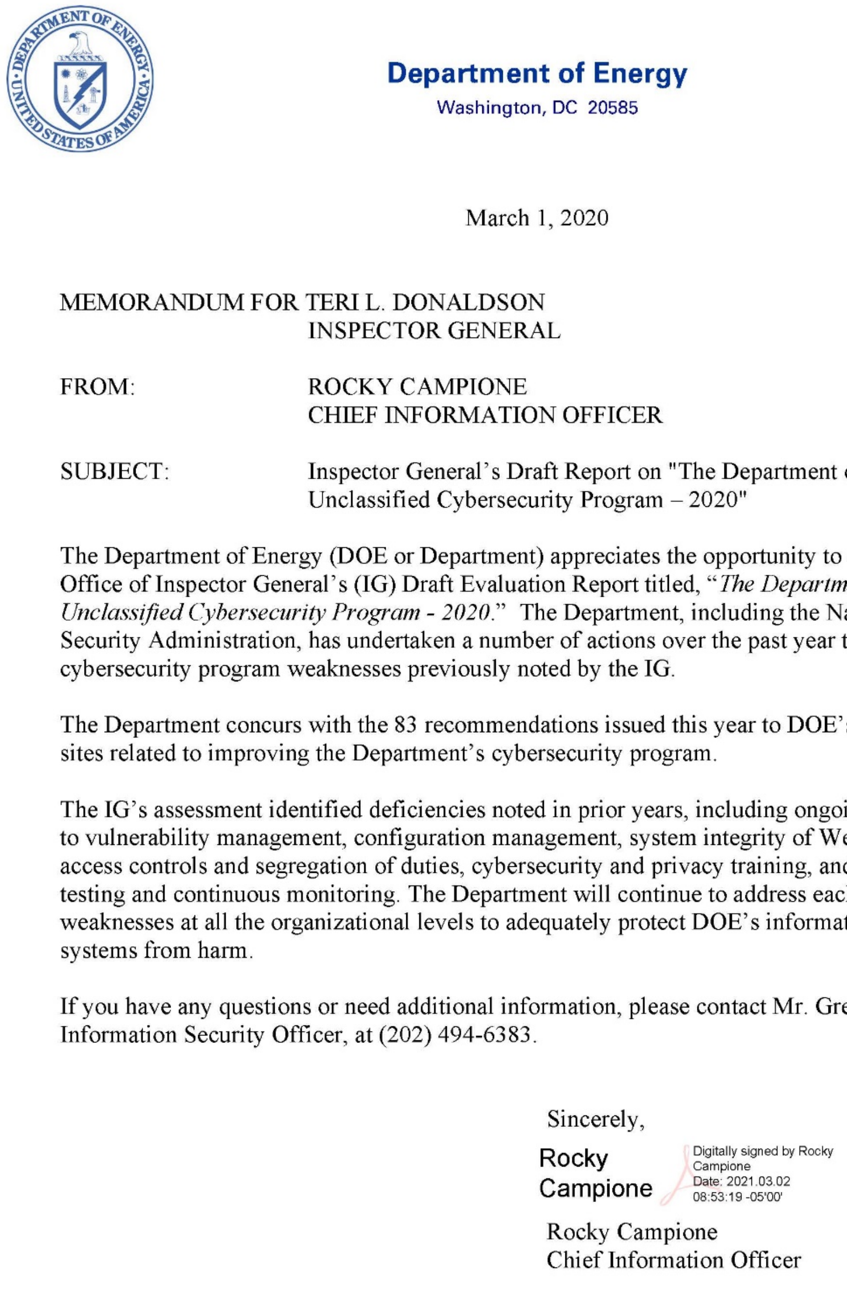
- *INFORMATION SECURITY: Supply Chain Risks Affecting Federal Agencies* (GAO-18-667T, July 2018)

- *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)

Appendix 4

Management Comments



Department of Energy
Washington, DC 20585

March 1, 2020

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 – 2020"

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 - 2020*." 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 83 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. Greg Sisson, Chief Information Security Officer, at (202) 494-6383.

Sincerely,

Rocky Campione
Digitally signed by Rocky Campione
Date: 2021.03.02 08:53:19 -05'00'

Rocky Campione
Chief Information Officer

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.