Office of Inspector General

OFFICE OF TECHNOLOGY, FINANCIAL, AND ANALYTICS

EVALUATION REPORT

THE DEPARTMENT OF ENERGY'S UNCLASSIFIED CYBERSECURITY PROGRAM – 2021

DOE-OIG-22-33
JUNE 2022

Department of Energy
Washington, DC 20585

June 6, 2022

Memorandum for The Secretary

From: Teri L. Donaldson
Inspector General

Subject: Evaluation Report on The Department of Energy's Unclassified Cybersecurity Program – 2021

Highlights

What We Reviewed and Why

Entities within the United States have recently been the target of several high-profile cyberattacks designed to compromise information or shut down an organization's operations. The Department of Energy's extensive information technology assets and significant amounts of sensitive data were not immune to those attacks. In fact, Department facilities across the Nation were challenged to fend off these and other cyberattacks while continuing to operate information technology networks and systems for essential operations required to accomplish their national security, research and development, and environmental management missions. In addition, the Department continued to face the challenge of maintaining security over its information and systems even as a large component of its workforce worked remotely due to COVID-19. Although the Department continues to deal with challenges and make cybersecurity related improvements, the most recent *Federal Information Technology Acquisition Reform Act* scorecard noted that its cybersecurity ratings continued to be low.

The *Federal Information Security Modernization Act of 2014* (FISMA) 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. FISMA also mandates that the Office of Inspector General conduct an independent evaluation to determine whether the Department's unclassified cybersecurity program adequately protected its data and information systems. As part of that evaluation, the Office of Inspector General is required to assess the Department's cybersecurity program according to FISMA 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. These metrics are focused around five cybersecurity functions and nine security domains and are aligned with the *National Institute of Standards and Technology* (*NIST*) *Framework for Improving Critical Infrastructure Cybersecurity* (Cybersecurity Framework). This report documents the results of our evaluation of the Department's cybersecurity program for fiscal year (FY) 2021.

What We Found

Our FY 2021 evaluation determined that the Department, including the National Nuclear Security Administration, had taken actions to address many previously identified weaknesses related to its unclassified cybersecurity program. For instance, Department programs and sites had taken corrective actions related to configuration management, identity and access management, contingency planning, and system development lifecycle controls, which resulted in the closure of 27 of 35 (77 percent) recommendations made during our prior year evaluation. Although the Department's actions should help improve its cybersecurity posture, additional effort is needed to enhance security over systems and information. In particular, our FY 2021 evaluation identified weaknesses in each of the five function areas included in the NIST Cybersecurity Framework—Identify, Protect, Detect, Respond, and Recover. This included weaknesses related to areas such as risk management, supply chain risk management, configuration management, identity and access management, data protection and privacy, security training, information security continuous monitoring, incident response, and contingency planning. Many of the deficiencies were similar in type to those identified in our prior evaluations. We determined the following:

- The Identify cybersecurity function area includes program elements related to risk management and supply chain risk management. During our FY 2021 review, we identified several weaknesses related to these program elements. For instance, we found that seven locations did not effectively categorize and/or communicate the importance of information systems in enabling their missions and business functions. In addition, we determined that four locations did not effectively implement supply chain risk management programs for unclassified information systems.

- Configuration management, identity and access management, data protection and privacy, and security training are categories that support the Protect cybersecurity function area. During our FY 2021 review, we identified weaknesses related to the Department's implementation of these categories. For instance, seven locations reviewed had critical- or high-risk vulnerabilities on the workstations and servers tested. Our testing at 1 location identified over 10,000 critical- or high-risk vulnerabilities related to missing security patches. In addition, at three sites, we found multiple vulnerabilities that could be used to obtain unauthorized access to web applications or perform other unauthorized actions. Further, at a different site, we identified that annual access reviews of database and privileged user accounts for certain operating systems had not been conducted.

- Information security continuous monitoring is the focus of the Detect cybersecurity function area, which requires that the Department develop and implement appropriate activities to identify the occurrence of a cybersecurity event. However, during FY 2021,

we determined that three locations reviewed had not performed adequate security assessments to properly ensure that information security had been built into information systems, identified weaknesses and deficiencies, and provided essential information needed to make risk-based decisions as part of security authorization processes.

- Incident response is the focus of the Respond cybersecurity function area, which requires that the Department develop and implement appropriate activities to act against a detected cybersecurity incident. However, our evaluation identified weaknesses in this area at certain locations. For instance, two locations did not effectively collaborate with stakeholders to ensure onsite technical assistance or surge capabilities would be leveraged for quickly responding to incidents.

- The Recover cybersecurity function area requires the Department to develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident. The primary objectives of the Recover cybersecurity function relate to contingency planning. During FY 2021, we identified several weaknesses at locations related to the implementation of contingency planning activities. For instance, six locations had not appropriately designed or conducted sufficient contingency plan testing exercises.

The weaknesses identified during our evaluation of the Department's unclassified cybersecurity program occurred for a variety of reasons. For instance, 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, identity and access management weaknesses occurred, in part, because officials were unaware of current account management requirements. For example, at one site, the database management team was unaware of updated policy requirements, as many of the database service accounts were created prior to the development of the site's current requirements for service account management. We also determined that supply chain risk management weaknesses existed, in part, because locations reviewed had not always taken the necessary steps to implement the controls introduced in NIST Special Publication, 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*.

Without improvements to address the weaknesses identified in our report, the Department may be unable to adequately protect its information systems and data from compromise, loss, or modification. Further, as cybersecurity remains an ongoing challenge, it is important that programs and sites make improvements that contribute to enhancing the Department's overall security posture. In addition, because the Office of Inspector General, other independent reviewers, and internal assessments continue to identify weaknesses related to each of the five cybersecurity function areas, it is imperative that the Department enhance its cybersecurity operations to ensure that it adequately secures its information systems and data.

Finally, in June 2021, the House of Representatives, Committee on Oversight and Reform, requested that we assess any vulnerabilities created or exacerbated by the Department's use of remote access software to facilitate telework during COVID-19 and whether any such vulnerabilities were effectively mitigated. The Committee recommended that we examine eight

specific areas related to remote work as part of our annual FISMA evaluation. We performed the requested review at eight of the Department's programs or locations. The results of our inquiry are included in Appendix 2.

What We Recommend

To help improve the Department's cybersecurity posture and correct the weaknesses identified, we made 61 recommendations to its programs and sites during FY 2021, including 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. Throughout the FY, we also provided opportunities for improvement at certain 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 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 are included in Appendix 5.

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

Table of Contents

Background and Objective

Background

The *Federal Information Security Modernization Act of 2014* (FISMA) requires the Office of Inspector General (OIG) to conduct an annual independent evaluation to determine whether the Department of Energy's unclassified cybersecurity program adequately protected its data and information systems during the fiscal year (FY). As part of that evaluation, the OIG is required to assess the Department's cybersecurity program according to FISMA 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. As noted in the table below, these metrics are focused around five cybersecurity functions and nine security domains and are aligned with the *National Institute of Standards and Technology* (*NIST*) *Framework for Improving Critical Infrastructure Cybersecurity* (Cybersecurity Framework).

Cybersecurity Functions		Security Domains
Identify	Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.	Risk Management
		Supply Chain Risk Management
Protect	Develop and implement appropriate safeguards to ensure delivery of critical services.	Configuration Management
		Identify and Access Management
		Data Protection and Privacy
		Security Training
Detect	Develop and implement appropriate activities to identify the occurrence of a cybersecurity event.	Information Security Continuous Monitoring
Respond	Develop and implement appropriate activities to take action regarding a detected cybersecurity incident.	Incident Response
Recover	Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.	Contingency Planning

Source: Cybersecurity Framework and FY 2021 FISMA security metrics

We assessed the effectiveness of the Department's information security program on a maturity model spectrum where the foundational levels ensure that sound policies and procedures are developed, and the advanced levels capture the extent to which those policies and procedures have been institutionalized. The overall maturity of the Department's information security program was calculated by cybersecurity function area based on the average rating of the associated domains. Within the context of the maturity model, an information security program is operating at an effective level of security if it is assessed at the "Managed and Measurable" level.

To support our evaluation, we conducted control testing and assessments of various aspects of the unclassified cybersecurity programs at 27 Department locations under the purview of the

National Nuclear Security Administration, Under Secretary for Science and Innovation, Under Secretary for Infrastructure, Office of Environmental Management, and certain staff offices. Our review included general and application control testing, technical vulnerability scanning, and validating corrective actions taken to remediate prior year weaknesses. We also relied on the results from other cybersecurity related reviews conducted by the OIG in FY 2021 and the results from the FISMA security metric work performed at five Department locations during FY 2021.

Further, in June 2021, the OIG was encouraged by the U.S. House of Representatives, Committee on Oversight and Reform, to include in its annual FISMA evaluation an assessment of any vulnerabilities created or exacerbated by the Department's use of remote access software to facilitate telework during COVID-19 and whether any such vulnerabilities were effectively mitigated.[1] The request included eight topics for examination. We performed the requested review at eight of the Department's programs or locations. The results of our inquiry are included in Appendix 2.

Report Objective

We conducted this evaluation to determine whether the Department's unclassified cybersecurity program adequately protects data and information systems.

[1] https://oversight.house.gov/sites/democrats.oversight.house.gov/files/Letters%20to%20Inspectors%20General%20-%20Cyber%20Vulnerabilities.pdf (Page 21).

Results of Review

Our FY 2021 evaluation determined that the Department had taken actions to address many previously identified weaknesses. Specifically, Department programs and sites had taken corrective actions related to configuration management, identity and access management, contingency planning, and system development lifecycle controls, which resulted in the closure of 27 of 35 (77 percent) recommendations made during our prior year evaluations. Although the Department's actions should help improve its cybersecurity posture, additional effort is needed to enhance security over systems and information. In particular, our FY 2021 evaluation identified weaknesses in each of the five Cybersecurity Framework function areas. This included weaknesses related to risk management, supply chain risk management, configuration management, identity and access management, data protection and privacy, information security continuous monitoring, incident response, and contingency planning. Our test work resulted in 53 new and 8 repeat recommendations at 11 locations.

Identify

The Identify cybersecurity function requires that the Department develop an organizational understanding to manage cybersecurity risks to systems, people, assets, data, and capabilities. It includes two information security domains—risk management and supply chain risk management. The Identify cybersecurity function relates to several cybersecurity controls found in NIST Special Publication (SP) 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, including those related to asset management, governance, and risk assessment. During our FY 2021 evaluation, we found that the Department had not effectively implemented security controls related to risk management and supply chain risk management.

Risk Management

The risk management security domain focuses on an organization's progress related to asset management, business environment, governance, risk management, and risk management strategy. The Department had taken action to address one system development lifecycle weakness related to risk management identified in our prior year review. However, our FY 2021 work identified several risk management concerns. For instance:

- Four locations reviewed had not effectively implemented risk management programs for unclassified information systems. For example, the locations did not effectively utilize technology/automation to provide a centralized, enterprise-wide view of cybersecurity risk management activities across the site, including risk control and remediation activities, dependencies, risk scores/levels, and management dashboards. Although one site had implemented an automated solution that provided a centralized, enterprise-wide view of cybersecurity risk, the solution did not perform scenario analysis and model potential responses, including the potential of a threat exploiting a vulnerability and the resulting impact to organizational systems and data.

- Three locations had deficiencies related to performing risk assessments. Specifically, while one site had performed system-level risk assessments, the results were not incorporated into an organization-wide cybersecurity and privacy risk assessment. A second site had not always developed or updated system-level risk assessments, and a third site did not perform system-level risk assessments to allow officials to incorporate results into a cybersecurity risk register.

- Seven of the locations reviewed did not effectively categorize and/or communicate the importance of information systems in enabling missions and business functions. For example, prior to our review, one site identified the need to recategorize two systems that supported access to email and file servers, as well as desktop and laptop computing functions, from low- to moderate-impact security categorizations. However, corrective actions had not been completed in accordance with the established plan of action and milestones (POA&M), and certain tasks were overdue by up to 25 months. During our audit, we found that financial personnel saved emails with sensitive procurement data, such as bank names and account numbers, to an unencrypted shared drive that resided on one of the miscategorized information systems.

- Five locations did not effectively utilize POA&Ms to ensure that identified security weaknesses were addressed. For example, at one site, POA&Ms were developed to address security control deficiencies and weaknesses, but milestones did not adequately describe actionable tasks needed to remediate the identified issue and many had exceeded their established due dates. In addition, although two sites had consistently utilized POA&Ms to effectively mitigate security weaknesses, the sites did not monitor and analyze qualitative and quantitative performance measures on the effectiveness of its POA&M activities and use that information to make appropriate adjustments.

- Two locations reviewed had not fully developed risk management strategies necessary to adequately manage their information and system risks. In particular, officials at one site did not develop an effective risk management strategy to include defined organizational risk tolerance, risk assessment methodologies, and risk monitoring processes. At the second site, the Authorizing Official had not provided explicit approval for deviations from the NIST-based security controls even though risk acceptance was required to be documented and formally accepted. Specifically, our analysis found that 90 of 277 required common security controls and enhancements for moderate-impact systems or enclaves were not fully implemented, and there was no documentation to support the Authorizing Official's acceptance of resulting risk. The same site also did not maintain supporting documentation to properly address the risk of less-than-fully implemented security controls, which contradicted the site's established cybersecurity risk management approach documentation.

Without adequate risk management controls, the Department may be unable to effectively prioritize cybersecurity activities and manage the likelihood that an event will occur.

Supply Chain Risk Management

The supply chain risk management security domain evaluates the extent to which an organization-wide strategy is used to manage the supply chain risks associated with the development, acquisition, maintenance, and disposal of systems, system components, and system services. We concluded that four locations reviewed did not effectively implement supply chain risk management programs for unclassified information systems. For example, these locations did not establish processes to detect and prevent counterfeit components from entering the organization's systems. Two of the four locations had not defined, implemented, or communicated component authenticity policies and procedures. Another site had defined and communicated its component authenticity policies and procedures but did not consistently implement those processes, conduct related training, or implement configuration controls. Although the fourth site provided evidence that it was consistently implementing relevant policies and procedures, the site did not conduct training that focused on component authenticity or implement configuration control over system components out for repair and service.

According to Federal requirements, all Executive Branch agencies must be compliant with NIST standards within 1 year of the publication date for legacy systems. Agencies are also expected to meet the requirements of, and be in compliance with, NIST standards and guidelines immediately upon system deployment for information systems under development or for legacy systems undergoing significant changes. NIST SP 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*, was published in September 2020 to strengthen security and privacy controls, including supply chain risk management. While the majority of our test work was performed prior to the 1-year publication date, we determined that the identified weaknesses existed, in part, because certain locations reviewed had not yet taken the necessary steps to implement the mandated changes. For instance, officials at one site explained that the supply chain risk management requirements were not applicable because the requirements were not included in the site's contract. As a result, the site had not progressed in implementing the required security controls. Failure to implement currently required security controls could leave the Department's programs and sites susceptible to threats that could significantly impact operations and critical systems.

Protect

The Protect cybersecurity function requires the Department to develop and implement appropriate safeguards to ensure delivery of critical services. It includes configuration management, identity and access management, data protection and privacy, and security training security domains. The Protect cybersecurity function relates to several cybersecurity controls found in NIST SP 800-53, Revision 4, including categories related to identity and access management, awareness and training, and maintenance. Our FY 2021 evaluation identified weaknesses related to the Department's implementation of the four domains included in the Protect cybersecurity function.

Configuration Management

The configuration management security domain focuses on an organization's progress related to areas such as utilization of system baselines and secure configurations, vulnerability

management, and system change controls. The Department had taken action to address six of the configuration management weaknesses identified in our prior reviews. However, we found that configuration management weaknesses continued to exist, including the continuation of two prior year findings. For instance:

- Five locations did not effectively implement configuration management programs for unclassified information systems. In particular, two sites had not developed organization-wide configuration management plans with the necessary and required components. A third site had not integrated its configuration management plan with its risk management and continuous monitoring programs. Further, although two other locations reviewed had consistently implemented organization-wide configuration management plans and had integrated them with risk management and continuous monitoring programs, neither site had adequately measured the effectiveness of its configuration management plans.

- Our testing at three locations identified vulnerabilities that could be used to obtain unauthorized access to web applications or perform other unauthorized actions. Specifically, we determined that tested applications at the sites accepted malicious input data. For instance, at two sites, the applications accepted malicious input data files from authenticated users and incorporated those into the application. The malicious input data accepted at both sites could have been used to launch attacks against legitimate application users and result in unauthorized access to the applications.

- One site maintained web servers that were configured to allow anonymous access to certain directories storing sensitive information or that were vulnerable to attacks that could allow arbitrary access to files on the servers. We also identified several devices at the site that were configured with default credentials or allowed connections without authentication.

- One site maintained several firewalls that inappropriately included rules that granted access to any service within a certain group. Officials stated that when working with researchers, the site typically allowed open access through the firewall first and restricted it later, upon request.

- Seven locations reviewed were running unsupported software. For instance, at two locations, we identified critical- and high-risk vulnerabilities on workstation and server operating systems that were no longer supported. One location had critical- and high-risk vulnerabilities related to unsupported software on 16 of 29 (55 percent) servers tested. We also identified another location with critical- and high-risk vulnerabilities related to unsupported software on 173 of 351 (49 percent) workstations tested. This finding was similar to issues identified at the same location during our FY 2020 review. Further, one location had 132 instances of unsupported software identified across 223 tested devices on a system. The same location also had outdated antivirus definitions identified on 34 system devices and 3 devices that had no antivirus software installed.

- Seven locations were operating workstations and/or servers that had missing critical- and high-risk vulnerability security patches or updates. We found that 495 of 1,507 (33 percent) workstations tested were operating with missing patches or updates that had not been applied within each location's established timeframes. For instance, at 1 location, 295 workstations tested had missing patches that could have addressed more than 10,000 critical- and high-risk vulnerabilities. In addition, we determined that 30 of 235 servers tested at 5 locations were missing critical- or high-risk patches or updates.

- We also noted several configuration management weaknesses at another site. For instance, the site did not always maintain an accurate inventory of applications located on its internal network. Although an inventory of applications was maintained, the inventory did not identify within which enclave the application was installed. We also found that the site had not developed a configuration management plan that defined detailed processes and procedures for how configurations were used and managed to support system development lifecycle activities.

The identified weaknesses related to configuration management occurred for various reasons. For instance, at three locations, weaknesses existed, in part, because the sites did not implement application-level security controls designed to block malicious input. In addition, the locations' application development and vulnerability management programs did not include adequate testing processes and procedures to identify vulnerabilities related to attacks against web application functionality. At two other locations, weaknesses were due, in part, to the sites' configuration management processes. Specifically, one site's process did not ensure that anonymous access and default credentials were changed prior to connecting the systems to the production network and throughout the system lifecycle. The site's vulnerability management processes also did not ensure that systems with anonymous access and default credentials on the production network were identified, monitored, and remediated. At the second location, the site's firewall management standard did not ensure that network access to new devices in the production environment was immediately restricted. Rather, the site's approach was to allow more access than necessary and restrict it later. Further, at one other location, Federal oversight officials and system managers had not recognized a certain system as a Federal information system. As such, applicable cybersecurity controls prescribed by NIST SP 800-53, Revision 5, were not implemented on the system and required processes, such as patch and vulnerability management and configuration management, had not been developed and implemented.

Identity and Access Management

The identity and access management security domain emphasizes the need for organizations to implement procedures related to identity, credential, and access management such as the use of personal identity verification credentials, effective management of privileged and non-privileged accounts, and remote access controls. Although the Department had taken action to address seven of the identity and access management weaknesses identified in prior year reviews, we found that access management weaknesses continued to exist. For example, our review determined that:

- Four locations did not effectively implement identity and access management programs for unclassified information systems. Specifically, the locations did not always ensure that appropriate configuration or connection requirements were maintained for remote access connections. Two locations reviewed had not implemented appropriate remote access timeouts due to inactivity, while a third location had not consistently implemented processes for reviewing user logs. In addition, the fourth site had not ensured that all end-user devices were appropriately configured prior to allowing remote access or restricted the ability to transfer data accessed remotely to unauthorized devices.

- One location had not conducted annual access reviews of database and operating system privileged user accounts for certain applications, as required by the site's internal policy on *Access Control and Management of User Accounts*. We determined that privileged accounts for these applications had not been reviewed since at least February 2020.

- At one site, we found that officials had not fully implemented access controls to properly manage privileged user access and enforce separation of duties for the tested application. In particular, our review identified eight server administrators and developers with access to the command that allows a general user to masquerade as a "super user." In another instance, we identified a weakness related to access control implementation over database service accounts wherein 148 database service accounts were created without identification of a unique account owner.

- Separation of duties weaknesses related to certain roles and responsibilities were also identified at another site. In particular, we found combinations of access to source code, server administrator, and application end-user accounts that were contrary to separation of duties requirements. We also identified accounts with access to source code; however, the users were either no longer employed by the site or users had conflicts due to least privilege requirements. In addition, the site did not include users with access to service accounts in its consideration of potential separation of duties conflicts. Further, the site could not provide evidence that service account passwords were reset when individuals with access to shared accounts left the organization or were no longer in a role that required such access.

- At one site, application user roles had not been fully reviewed. Our FY 2021 general controls testing found that a review of user roles had not been completed for all financial process areas to ensure appropriate user access. In addition, the site had not ensured the separation of conflicting information technology roles. Specifically, two users were assigned the roles of application administrator, database administrator, and developer. A person with these roles could implement changes to the application or alter data within the system without authorization.

The identity and access management weaknesses noted above occurred, in part, because officials were unaware of current account management requirements. For instance, at one site, the database management team was unaware of updated policy requirements, as many of the database service accounts were created prior to the development of the site's current requirements for service account management. In addition, two locations did not ensure that the appropriate

separation of duties controls were established to address related risks. Officials at one of the locations did not implement a sufficient control to retain evidence of password changes made in response to personnel changes. Further, another location's weaknesses were due, in part, to the informal nature of an application's access review process. While site policy required an annual review of user access to the application, it did not have a process in place to ensure that all role reviews were completed, as required. The same site also had neither established a policy to identify and separate conflicting roles that could allow an individual to make unauthorized system changes nor created a process to document and approve unusual circumstances that required conflicting roles and responsibilities. Such access was also not reviewed on a periodic basis to ensure ongoing appropriateness.

Data Protection and Privacy

The data protection and privacy security domain focuses on the extent to which agencies protect personally identifiable and other sensitive information and have controls in place to prevent data exfiltration. Throughout our evaluation, we identified weaknesses related to the data protection and privacy programs implemented at sites across the Department. In particular, four locations reviewed had not effectively implemented data protection and privacy programs for their unclassified information systems. Our review determined that:

- Four locations did not effectively implement Data Breach Response Plans, as appropriate, to respond to privacy events. Specifically, three sites did not perform table-top exercises that focused on testing the implementation of developed data breach response activities. The fourth site did not monitor and analyze qualitative and quantitative performance measures on the effectiveness of its Data Breach Response Plan.

- Three locations did not effectively implement security controls to protect personally identifiable information and other agency sensitive data, as appropriate, throughout the data lifecycle. Although the three sites monitored for untrusted removable media, they had not consistently implemented procedures to prevent the use of such media.

Without adequate data protection and privacy cybersecurity controls, personally identifiable information and other sensitive information may not be adequately managed to protect the confidentiality, integrity, and availability of information.

Security Training

The security training domain aims to ensure that an effective cybersecurity training and awareness program has been implemented. Our evaluation of security training activities determined that four of the locations reviewed had not effectively implemented security training programs for unclassified information systems. In particular:

- None of the four sites effectively utilized security awareness and training strategies or plans that leveraged a skills assessment and were adapted to the site's mission and risk environment. In addition, while these sites had implemented organization-wide security awareness and training plans, they had not utilized performance metrics to measure their plans' effectiveness.

- Three sites had not effectively ensured that specialized security training was provided to individuals with significant security responsibilities. One site did not have policies and procedures established to ensure users with significant security responsibilities received adequate role-based cybersecurity training. A second site had not consistently required role-based training for individuals with significant security responsibilities across the organization. Although the third site provided training for individuals with significant security responsibilities, officials did not measure and analyze the training's effectiveness.

Without an adequate security awareness and training program, an organization's users and those with significant security responsibilities, including privileged users, may not be fully educated or trained to perform their cybersecurity related duties and responsibilities consistent with policies, procedures, and agreements.

Detect

The Detect cybersecurity function requires that the Department develop and implement appropriate activities to identify the occurrence of a cybersecurity event. It includes one information security domain—information security continuous monitoring (ISCM). The Detect cybersecurity function relates to several security assessment and authorization cybersecurity controls in NIST SP 800-53, Revision 4, including categories related to ISCM, anomalies and events, and detection processes. During FY 2021, we identified various weaknesses at programs and sites related to the implementation of the Detect cybersecurity function.

Information Security Continuous Monitoring

The focus of the ISCM domain is to ensure organizations develop and implement processes for performing ongoing information system assessments, granting system authorizations, including developing and maintaining system security plans, and monitoring system security controls. However, we found deficiencies existed related to the effectiveness of ISCM processes implemented throughout the Department, including the reissuance of one prior year finding. For instance:

- Four locations reviewed had not effectively implemented ISCM programs for unclassified information systems. For example, these locations did not adequately develop and implement processes for collecting and analyzing ISCM performance measures and reporting findings. While two sites had consistently captured qualitative and quantitative performance measures on the performance of their ISCM programs, the sites had not utilized the performance metrics to increase the effectiveness of the programs to deliver persistent situational awareness to their stakeholders. A third site had not identified and defined performance measures used to assess the effectiveness of its ISCM program, achieve situational awareness, and control ongoing risk.

- Three sites had not performed adequate security assessments to ensure that their information systems met information security requirements, identified weaknesses and deficiencies, and provided essential information needed to make risk-based decisions as part of security authorization processes. While 1 site performed security assessments, we

determined that 30 of 127 (24 percent) critical controls and control enhancements were not included in the site's security control assessment plan for FY 2021. The other two sites did not perform ongoing security control assessments to support their authorizations to operate.

- Another location had not fully implemented database audit logging and monitoring of certain databases. In particular, while the site logged privileged account activities, no routine review, monitor, and report of database event logs occurred. This issue was first identified during our FY 2020 evaluation and had not been corrected at the time of our FY 2021 review. To its credit, the site was in the process of conducting a feasibility study to determine if database audit logging and monitoring functionality could be built into its existing software platform.

The identified ISCM weaknesses occurred for various reasons. For example, one location did not conduct 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. Database administrators at the site had database access to perform their job duties; however, this also provided them with read and write access to audit log files because the account permissions could not be restricted. Because database audit log monitoring was not implemented, unauthorized changes to the log files may not be detected. In addition, weaknesses at two other sites existed, in part, due to a lack of program management activities. Specifically, officials had not fully implemented effective cybersecurity risk management strategies or developed effective oversite structures. For instance, the monitoring weaknesses we identified at those locations were due to deficiencies in weakness tracking oversight and security authorization processes, including ongoing authorizations to operate.

Respond

The Respond cybersecurity function requires the Department to develop and implement appropriate activities to act against a detected cybersecurity incident and includes the incident response security domain. The Respond cybersecurity function relates to the incident response cybersecurity controls found in NIST SP 800-53, Revision 4, including categories related to response planning, communications, analysis, mitigation, and improvements. During FY 2021, we identified weaknesses related to the implementation of the Respond cybersecurity function.

Incident Response

The incident response security domain includes an emphasis on ensuring that the organization utilizes an incident response plan to provide a formal, focused, and coordinated approach to responding to incidents, including incident detection, analysis, handling, and information sharing. Our review identified two locations that did not effectively implement incident response programs for unclassified information systems. Neither location effectively collaborated with stakeholders to ensure onsite technical assistance or surge capabilities could be leveraged for quick incident response support. In addition, the sites had not fully implemented the Department of Homeland Security's Einstein 1 and 2 to screen all traffic entering and leaving the sites' networks through a trusted internet connection.

Recover

The Recover cybersecurity function requires the Department to develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident. The Recover cybersecurity function includes one information security domain—contingency planning. The Recover cybersecurity function relates to the contingency planning cybersecurity controls found in NIST SP 800-53, Revision 4, including categories related to recovery planning, improvements, and communication. During FY 2021, we identified several weaknesses related to the implementation of this cybersecurity function.

Contingency Planning

The contingency planning security domain includes an emphasis on ensuring that the Department develops and tests business impact analyses and contingency plans and can recover after a disruption. The Department had taken action to address one contingency planning weakness identified in our prior review. However, during our 2021 testing, we identified several weaknesses related to this domain area. For instance:

- Four sites had not effectively implemented contingency planning programs for unclassified information systems. For example, three sites had not always ensured that contingency plans were defined, maintained, and developed for information systems. The fourth site had not fully integrated its contingency plans with other continuity areas such as organization and business process continuity, disaster recovery planning, incident management, insider threat implementation plan, and occupant emergency plans.

- Six locations had not appropriately designed or conducted sufficient contingency plan testing exercises. While two sites consistently implemented contingency plan testing, they did not utilize automated mechanisms for testing those contingency plans more thoroughly and effectively. In addition, four other sites did not test their information system contingency plans.

- Another site reviewed had not established alternate storage site locations for all of its information system backups. Contrary to NIST requirements, the site had not established an alternate storage location for its Windows server backups, which included database, patch management, and monitoring server data.

The weaknesses identified related to contingency planning occurred, in part, because policies, procedures, and plans were not developed or maintained to fully facilitate the implementation of the contingency planning controls reviewed. For example, one of the site's system security plans indicated that the alternate storage site cybersecurity control was fully implemented even though Windows server backups were co-located with the servers from which the data was created. In addition, another site had not adequately developed policies and procedures that contained sufficient detail regarding contingency plan testing.

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, or modification. This underscores the crucial need to focus efforts on maturing the Department's overall cybersecurity posture. For instance, although we considered existing mitigating controls, continued findings at some Department sites related to system integrity of web applications revealed vulnerabilities that could have allowed malicious attacks, resulting in unauthorized access to sensitive data that could have affected application functionality. In addition, such 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.

Further, we continued to identify deficiencies related to developing, updating, or implementing policies and procedures that could adversely affect the Department's ability to properly secure its information systems and data. Also, the identity and access management weaknesses noted during our review may increase the risk of unauthorized system access or data modification. Additionally, 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 2021 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 FY 2021, the Department completed its 2-year *DOE Cyber Agency Priority Goal Campaign* with successful completion of all goals, which included a 100-percent assessment of all High Value Assets, updated risk management strategies, and implementation of continuous monitoring principles. In addition, the Department developed and issued multiple enterprise-wide policy and guidance documents related to Department Order 205.1C, *Department of Energy Cybersecurity Program*. These included the *DOE Enterprise Information Technology Services Common Security Controls*, *Office of the Chief Information Officer [OCIO] Enterprise Security Assessment and Authorization Process*, and *DOE Cybersecurity Risk Management Methodology*. 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 61 recommendations to the Department's programs and sites during FY 2021, including those identified during this evaluation and in other issued reports. Specific recommendations were made to each of the locations where weaknesses were identified. They were related to areas such as system integrity of web applications, configuration management, vulnerability management, and access controls. During FY 2021, we also issued reports and recommendations related to the Department's Mission Information Protection Program and cybersecurity program management 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 those as formal findings and recommendations.

Management Comments

Management concurred with the recommendations issued to programs and sites related to improving the Department's overall cybersecurity program. Management indicated that it would continue to address the weaknesses at all organizational levels to adequately protect the Department's information assets and systems from harm.

Management's comments are included in Appendix 5.

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
Federal Information Security Modernization Act of 2014	FISMA
Fiscal Year	FY
Information Security Continuous Monitoring	ISCM
National Institute of Standards and Technology	NIST
Office of Inspector General	OIG
Plan of Action and Milestones	POA&M
Special Publication	SP

Appendix 2

Response to Congressional Request

In June 2021, the U.S. House of Representatives, Committee on Oversight and Reform, encouraged the Office of Inspector General to include, as part of its annual *Federal Information Security Modernization Act of 2014* evaluation, an assessment of any vulnerabilities created or exacerbated by the Department of Energy's use of remote access software to facilitate telework during COVID-19 and whether any such vulnerabilities were effectively mitigated. The request noted that the National Institute of Standards and Technology had previously warned of security concerns associated with telework and requested that eight topics be examined.

To address the Committee's request, we conducted an inquiry of three of the Department's program offices, four field sites, and a power marketing administration. Our responses to the Committee's areas of concern are summarized below.

1. **The acquisition, deployment, management, and security of remote connections to Department networks, including those facilitated by VPNs [virtual private networks] and/or virtual network controllers.**

   Our inquiry did not identify any significant concerns with the acquisition, deployment, management, and security of remote access connections at the entities reviewed. We found that each of the eight entities reviewed had implemented VPN capabilities. In addition, six of the entities also implemented virtual desktop infrastructure capabilities to allow individuals to work remotely.

   In many instances, Department officials informed us that these capabilities were in place prior to COVID-19, but various components of their respective infrastructure were scaled up to better accommodate the increased remote workforce. However, one entity noted that it had no remote access capability prior to COVID-19 and, as a result, had to acquire all the necessary components such as licenses, VPN infrastructure, and laptops to enable its employees to work remotely.

2. **The acquisition, deployment, management, and security of collaboration platforms such as Microsoft Teams, Zoom, Slack, and Cisco Webex.**

   Our inquiry did not identify any significant concerns with the acquisition, deployment, management, and security of collaboration platforms in use across the Department. In particular, most of the entities reviewed had implemented or were in the process of transitioning to collaborative platforms when COVID-19 began. As noted in our response to the first question, one entity did not allow remote access prior to COVID-19 and, as such, did not have the ability to host collaborative sessions until it acquired the necessary infrastructure and platforms.

   Officials from each of the entities reviewed commented that employees could only host video conferences on the collaborative tools that each entity managed. However, six entities had

no restrictions on which platforms their employees could join meetings as participants. We identified two entities that placed restrictions on which collaborative tools could be used and how they could be accessed (i.e., application or web browser) based on the classification or sensitivity of information being discussed.

We also determined that the organizations reviewed had varying methods of securing their collaborative tools. For instance, officials from three entities indicated that the use of an unauthorized collaborative tool to host a conference would be prevented by restricting the user's administrative rights to his or her device or black/whitelisting applications or websites. Two additional entities noted that they monitored their networks for unauthorized collaborative tools usage. In addition to these security measures, several entities also discussed how they restricted collaborative sessions to only authorized officials. For example, one organization noted that personal identification numbers were required whenever one of its employees hosted a meeting. In addition, the employee responsible for the hosted meeting was also required to review the participant list to ensure that only expected attendees were present in the meeting. Another entity configured the settings on one of its collaborative tools so that anonymous users were automatically placed in the meeting's lobby, which would require the host to allow them to join the meeting.

3. **Whether the Department, and all components, has implemented security controls to prevent the unauthorized dissemination of controlled unclassified information, personally identifiable information, or sensitive but unclassified information via third-party collaboration platforms.**

   Our inquiry identified that three entities had not implemented any type of technical controls on their collaborative platforms. Instead, these locations were relying on user training provided by each site that described how to handle certain types of information. Conversely, five entities had implemented controls restricting data transfers during collaborative sessions or relied on their internal review process, which limited the types of collaborative platforms that could be used for hosting purposes. While some of these actions could potentially reduce the risk of disclosure, officials from two of the organizations reviewed noted that individuals could not be prevented from verbalizing or taking a picture of sensitive information shared over video during a collaborative session.

4. **The identity, credential, and access management of users that permit remote access to Department networks, including the extent to which the Department has enabled multi-factor authentication and implemented procedures to disable inactive and potentially unauthorized user accounts.**

   Our inquiry did not identify any significant concerns with remote-user authentication at the entities reviewed. In particular, we determined that each entity had implemented some form of multifactor authentication for both general and privileged remote sessions. However, we

found that the procedures to disable inactive or potentially unauthorized user accounts varied from entity to entity. Five of the eight organizations reviewed disabled inactive sessions in under an hour, while three entities allowed inactive connections to continue for hours or never disconnected them at all.

5. **The distribution and management of virtual and physical assets that facilitate telework, including laptop computers, smartphones, and RSA tokens.**

   Our inquiry found that the distribution and management was handled differently among the entities reviewed. For example, two organizations only distributed assets in person while the remaining six entities also included the ability to ship information technology assets directly to employees. Our inquiry also determined that each of the entities reviewed centrally managed and tracked their information technology assets for inventory and accountability purposes. However, the extent to which assets should be tracked (i.e., laptops, monitors, RSA tokens) varied between the entities. Overall, we did not identify any significant concerns related to the distribution of virtual and physical assets.

6. **The Department's adherence to Trusted Internet Connection 3.0 guidance.[2]**

   Our inquiry found that the implementation of Trusted Internet Connection 3.0 guidance varied from entity to entity. For example, two entities responded that they were not adhering to the Trusted Internet Connection guidance at the time of our review. Of these organizations, only one was actively working toward becoming aligned with the guidance, while the other site did not consider the guidance relevant to itself because its associated program was not participating. Aside from these two sites, officials from the remaining entities reviewed were able to describe how they aligned with the guidance. However, we cannot attest to the accuracy and completeness of those efforts as we did not audit Trusted Internet Connection implementation across the Department.

7. **Whether the Department's Chief Information Officer and all component Chief Information Officers implemented additional security policies in response to telework related to COVID-19 and how they are enforcing those policies.**

   Our inquiry found that most of the entities reviewed indicated that there were no major policies issued in response to telework due to COVID-19. In certain instances, officials commented that while the overall policy had not changed, there were minor adjustments or clarifications needed. While many of the entities had an established policy for telework, one of the entities reviewed had to develop a new policy because it had to create new remote capabilities as a result of COVID-19.

[2] Cybersecurity and Infrastructure Security Agency, *TIC 3.0 Core Guidance Documents* (accessed on April 22, 2021) (online at www.cisa.gov/publication/tic-30-core-guidance-documents).

8. Whether the Department has implemented continuous monitoring and scanning of networks to identify vulnerabilities.

Continuous monitoring and vulnerability management continue to challenge the Department as detailed in our evaluation reports on the Department's unclassified cybersecurity program. However, our inquiry found that the maximum telework posture resulting from COVID-19 did not appear to introduce additional complications. Each of the entities reviewed indicated that they were conducting vulnerability scans to help identify vulnerabilities. We also found that the entities reviewed continued to conduct their established continuous monitoring activities across their environments during telework due to COVID-19. Some entities indicated that the maximum telework posture created no measurable impact on their already established continuous monitoring efforts, while at least one entity needed to make adjustments that better captured the remote-work environment in monitoring activities. One official noted that continuous monitoring activities were able to be performed remotely; therefore, the work remained the same even though the means of conducting the monitoring efforts were different.

Appendix 3

Objective, Scope, and Methodology

Objective

We conducted this evaluation to determine whether the Department of Energy's unclassified cybersecurity program adequately protects data and information systems.

Scope

We conducted the evaluation from March 2021 through March 2022 at 27 Department locations primarily under the responsibility of the Administrator for the National Nuclear Security Administration, Under Secretary for Science and Innovation, Under Secretary for Infrastructure, Office of Environmental Management, and certain staff offices. Of the 27 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* (FISMA) 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.

At the request of the U.S. House of Representatives, Committee on Oversight and Reform, we conducted an inquiry into any vulnerabilities created or exacerbated by the Department's use of remote access software to facilitate telework during COVID-19, and whether any such vulnerabilities were effectively mitigated. This inquiry was conducted across select Headquarters' elements and the same five locations selected for our FISMA metric review.

Our evaluation 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 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 A21TG011.

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 FISMA 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.

The 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.

Due to 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 FISMA, 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 as a whole.

Management officials waived an exit conference on May 26, 2022.

Appendix 4

Related Reports

Office of Inspector General

- Audit Report on *Management of a Department of Energy Site Cybersecurity Program* (DOE-OIG-22-05, November 2021). The site had not implemented an effective cybersecurity program in accordance with Federal and Department of Energy requirements. Our review identified control weaknesses in 15 of 18 control families tested as described in National Institute of Standards and Technology Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*. The issues we identified were primarily related to the ineffective implementation of controls within the National Institute of Standards and Technology's program management family of controls. In particular, we tested 10 program management controls and determined that 6 were not effectively implemented.

- Audit Report on *Management of the Cybersecurity Program at a Department of Energy Site* (DOE-OIG-21-35, August 2021). The Office of Inspector General initiated a review of the cybersecurity program at a selected Department site to determine whether it effectively managed its cybersecurity program in accordance with Federal and Department requirements. Our review found that the site had not implemented an effective cybersecurity program in accordance with Federal and Department requirements. Specifically, we identified weaknesses related to vulnerability management and flaw remediation, system and communications protection, system and services acquisition, configuration management, and contingency planning.

- Audit Report on *The Office of Environmental Management's Mission Information Protection Program* (DOE-OIG-21-32, July 2021). The Office of Inspector General initiated this audit to determine whether the Mission Information Protection Program provided effective and efficient services while meeting its goals and objectives. Our limited testing did not identify any issues with the Mission Information Protection Program's Headquarters Security System component. However, we determined that the Information Security Continuous Monitoring function had not always provided effective and efficient services or fully met its goals and objectives. Specifically, the Information Security Continuous Monitoring team had not always ensured that issues identified through its assessments were appropriately carried forward for evaluation and followup testing in subsequent years. Further, we found that over 400 weaknesses documented within Information Security Continuous Monitoring's assessment reports had not been recorded in the Office of Environmental Management's central tracking system to ensure that key program officials had an accurate picture of the organization's overall cybersecurity and risk posture.

- Evaluation Report on *The Department of Energy's Unclassified Cybersecurity Program – 2020* (DOE-OIG-21-18, March 2021). 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 fiscal year 2019 evaluation, which resulted in the closure of 42 of 54 (78 percent) prior year weaknesses. Although these actions were positive, our current evaluation identified weaknesses in areas including system integrity of web applications, configuration management, vulnerability management, access controls, and contingency planning, many of which were consistent with our prior reports.

- 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 fiscal year 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.

Government Accountability Office

- *CYBERSECURITY AND INFORMATION TECHNOLOGY: Federal Agencies Need to Strengthen Efforts to Address High-Risk Areas* (GAO-21-105325, July 2021)
- *CYBERSECURITY: Federal Agencies Need to Implement Recommendations to Manage Supply Chain Risks* (GAO-21-594T, May 2021)
- *HIGH-RISK SERIES: Federal Government Needs to Urgently Pursue Critical Actions to Address Major Cybersecurity Challenges* (GAO-21-288, March 2021)
- *INFORMATION TECHNOLOGY: Federal Agencies and OMB Need to Continue to Improve Management and Cybersecurity* (GAO-20-691T, August 2020)
- *DATA CENTER OPTIMIZATION: Agencies Report Progress, but Oversight and Cybersecurity Risks Need to Be Addressed* (GAO-20-279, March 2020)
- *CRITICAL INFRASTRUCTURE PROTECTION: Additional Actions Needed to Identify Framework Adoption and Resulting Improvements* (GAO-20-299, February 2020)
- *INFORMATION TECHNOLOGY: DHS Directives Have Strengthened Federal Cybersecurity, but Improvements Are Needed* (GAO-20-133, February 2020)

Appendix 4

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

Management Comments

Department of Energy
Washington, DC 20585

May 16, 2022

MEMORANDUM FOR TERI L. DONALDSON
INSPECTOR GENERAL

FROM: ANN DUNKIN
CHIEF INFORMATION OFFICER

SUBJECT: Inspector General's Draft Report on "The Department of Energy's Unclassified Cybersecurity Program-2021"

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 - 2021.*" 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 61 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 areas such as risk management, supply chain risk management, configuration management, identity and access management, data protection and privacy, security training, information security continuous monitoring, incident response, and contingency planning. 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.

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.