Office of Inspector General

OFFICE OF CYBER ASSESSMENTS AND DATA ANALYTICS

EVALUATION REPORT

THE DEPARTMENT OF ENERGY'S UNCLASSIFIED CYBERSECURITY PROGRAM – 2022

DOE-OIG-23-20
MAY 2023

Department of Energy
Washington, DC 20585

May 2, 2023

MEMORANDUM FOR THE SECRETARY

SUBJECT: Evaluation Report on The Department of Energy's Unclassified Cybersecurity Program – 2022

The attached report discusses the results of our fiscal year 2022 Federal Information Security Modernization Act of 2014 evaluation. Our evaluation determined that the Department of Energy, including the National Nuclear Security Administration, had not taken appropriate actions to address many previously identified weaknesses related to its unclassified cybersecurity program. Specifically, 38 of 61 (62 percent) recommendations from our prior year evaluations remained open. We also issued 35 new recommendations throughout fiscal year 2022, many of which were similar in type to the deficiencies identified in our previous reports. If fully implemented, the recommendations should help to enhance the Department's unclassified cybersecurity program. In most instances, management concurred with the findings and recommendations and indicated that corrective actions had been taken or were planned. Although the Office of River Protection nonconcurred with two recommendations, management indicated that it had taken corrective actions to address the identified weaknesses.

We conducted this evaluation from March 2022 through March 2023 in accordance with the Council of the Inspectors General on Integrity and Efficiency's *Quality Standards for Inspection and Evaluation* (December 2020). 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. In many cases, officials have initiated corrective actions to address the identified vulnerabilities. We appreciate the cooperation and assistance received during this evaluation.

Teri L. Donaldson
Inspector General

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

DOE-OIG-23-20

Department of Energy
Office of Inspector General

The Department of Energy's Unclassified Cybersecurity Program – 2022
(DOE-OIG-23-20)

WHY THE OIG PERFORMED THIS REVIEW

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 include an assessment of FISMA security metrics, to determine whether the Department of Energy's unclassified cybersecurity program adequately protected its data and information systems.

What Did the OIG Find?

Our fiscal year 2022 FISMA evaluation determined that the Department, including the National Nuclear Security Administration, had not taken appropriate actions to address many previously identified weaknesses related to its unclassified cybersecurity program. Although actions were taken to close 23 of 61 recommendations from our prior evaluations, 38 recommendations remained open. We also issued 35 new recommendations, many of which were similar in type to the deficiencies identified in our previous reports.

The weaknesses identified occurred for a variety of reasons. For instance, weaknesses related to system integrity of web applications generally occurred because the applications were configured without adequate security controls designed to reject malicious input. In addition, identity and access management weaknesses occurred because officials were unaware of, or had not implemented, current account management requirements.

What Is the Impact?

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. Weaknesses will continue to exist in areas such as risk management, configuration management, identity and access controls, and security continuous monitoring. Additionally, as cybersecurity remains an ongoing challenge, it is important that programs and sites make improvements that contribute to enhancing the Department's cybersecurity posture.

What Is the Path Forward?

When fully implemented, the recommendations made during fiscal year 2022 should help to enhance the Department's unclassified cybersecurity program. The Department should emphasize ensuring that findings are closed in a timely manner, especially those findings repeated from prior years.

Table of Contents

Background and Objective

Background

The Federal Information Security Modernization Act of 2014 (FISMA) 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. 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 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 Framework for Improving Critical Infrastructure Cybersecurity*. In fiscal year (FY) 2022, significant changes were made to the FISMA reporting approach to support Executive Order 14028, *Improving the Nation's Cybersecurity*, and Office of Management and Budget guidance to agencies to further the modernization of Federal cybersecurity. The most notable change was transitioning the evaluation of metrics to a multi-year cycle. Specifically, a set of core metrics will be evaluated annually, and the remaining metrics will be evaluated on a 2-year cycle. As such, the scope of our review included an evaluation of the core metrics for FY 2022.

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
		Identity 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: *National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity* and FY 2022 FISMA security metrics.

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, the 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 the FISMA security metric work performed at six Department locations during FY 2022.

Report Objective

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

Results of Review

Our FY 2022 evaluation determined that the Department had not taken appropriate actions to address many previously identified weaknesses. Although actions were taken to close 23 of 61 recommendations from our prior evaluations, we found that 38 (62 percent) of the recommendations remained open related to areas such as configuration management, audit logging and monitoring, and identity and access management. We also issued 35 new recommendations throughout FY 2022, many of which were similar in type to the deficiencies identified in our previous reports. Our FY 2022 evaluation identified weaknesses in four of the five *National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity* function areas. This included weaknesses related to risk management, configuration management, identity and access management, data protection and privacy, information security continuous monitoring (ISCM), incident response, and contingency planning. Further, we identified opportunities for improvement during our FISMA security metric work and noted them throughout this report for management's consideration. Based on the results of our review, we determined that additional effort is needed to adequately protect the Department's data and information systems.

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 the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*, including those related to asset management, governance, and risk assessment. During our FY 2022 evaluation, we concluded that the Department had not always fully implemented security controls and associated processes related to 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. Our review identified one location that had not subjected an emergency communications system to required Federal cybersecurity risk management processes. Specifically, despite being in operation for almost 4 years, officials had not assessed the cyber risks associated with operating the system, categorized the impact of system loss to the organization, or selected and implemented appropriate security controls. These weaknesses occurred because Federal oversight officials and system managers had not recognized the system as a Federal information system in accordance with NIST requirements. As such, applicable cybersecurity controls prescribed by NIST SP 800-53 were not implemented on the system, nor was the Risk Management Framework completed, as required by NIST SP 800-37, Revision 2, *Risk Management Framework for Information Systems and Organizations*. Completion of the Risk Management Framework would have identified and addressed many of the cybersecurity issues found during our testing.

Based on our FISMA security metric work, we also identified some opportunities to improve the Department's risk management programs for unclassified information systems. For example, we found that two sites were not consistently using 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. Additionally, although three sites 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. We noted another area of improvement at four sites related to managing security risks at the organizational, mission/business process, and information system levels. Specifically, three sites did not use a risk register to manage risks, nor did they perform lessons learned over the effectiveness of cybersecurity risk management processes. The fourth site had weaknesses related to performing and/or documenting system-level and privacy risk assessments. 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. Notably, we found that four sites were incorporating supplier risk evaluations into their continuous monitoring practices to maintain situational awareness of supply chain risks, and another site was analyzing the impact of material changes to security and supply chain risk management assurance requirements and ensuring that acquisition tools, methods, and processes were updated as soon as possible.

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 5, including categories related to access controls, awareness and training, and data security and information protection. Our FY 2022 evaluation identified weaknesses related to the Department's implementation of the four domains included in the Protect cybersecurity function. During our test work, we made 48 recommendations to the Department related to configuration management, identity and access management, and security training.

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 some of the configuration management weaknesses identified in our prior reviews, and as a result, we

were able to close eight prior year recommendations. However, we found that configuration management weaknesses continued to exist, including the issuance of 16 new recommendations and the continuation of 9 prior year recommendations. For instance:

- Our testing at three locations identified vulnerabilities that could be used to obtain unauthorized access to web applications or perform other unauthorized actions. At one site, the application accepted malicious input data files from authenticated users and incorporated those into the application. The accepted malicious input data could have been used to launch attacks against legitimate application users and result in unauthorized access to the applications. This issue was first identified during our FY 2021 evaluation and was not expected to be completed until after our FY 2022 test work. At the second location, we identified a hypertext transfer protocol cookie containing user authentication session tokens that was scoped to the application's parent domain, which could have exposed the session tokens to all other websites and web applications in the parent domain. An attacker could have exploited this vulnerability to obtain unauthorized access to the application as different users with various access rights. The application reviewed at the third location did not properly verify whether user accounts were authorized to use certain functions, including modifying user account roles. This lack of authorization verification allowed lower-privileged accounts to perform actions that should have been limited to higher-privileged accounts.

- 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. This issue was first identified during our FY 2021 evaluation; however, the site had not fully remediated the identified issue at the time of our testing.

- One location 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. These issues existed even though they were first identified during our FY 2021 evaluation.

- We identified six locations with numerous devices that were running unsupported software across workstations and/or servers. We found that almost half of the workstations tested were not configured with the latest known versions of application software. For example, one location had critical-risk vulnerabilities related to unsupported software on 95 of 99 (96 percent) workstations tested. We also identified another location with critical-risk vulnerabilities related to unsupported software on 103 of 123 (84 percent) workstations tested.

- Six locations were operating workstations and servers that had missing critical- and high-risk vulnerability security patches or updates. We found that 287 of 453 (63 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, 91

workstations tested had missing patches that could have addressed almost 1,000 critical- and high-risk vulnerabilities. The same location also had over 800 missing critical- or high-risk patches or updates on 9 servers. It is important that the Department maintains its focus on vulnerability management to ensure that vulnerabilities are remediated in a timely manner to protect its information and information systems.

- At 1 location, we found 26 devices running network services that inappropriately transmitted data in clear text. We also found six unnecessary system components that were not being used. In addition, we identified another 51 components during system testing that site officials neither knew what they were nor whether they were needed.

- At one site, we found that database password parameters were not configured in accordance with requirements for several characteristics, including maximum password age, minimum password length, and complexity requirements, among others. Specifically, the policy governing the data reviewed required that user account passwords must be at least 8 characters long, must be changed every 31 days for passwords less than 16 characters, and contain a mix of 3 different character types (uppercase alpha, lowercase alphanumeric, and special characters). However, during our review, we found that there was no maximum password age, minimum password length, or complexity requirements configured on the databases reviewed.

- Although two locations had consistently implemented and maintained secure configuration settings for its information systems, we found that these sites could benefit from additional improvements by employing automation to help monitor configuration settings and making appropriate modifications when needed. In addition, although one location reviewed had documented flaw remediation processes in place, it had not tested patches for effectiveness and potential side effects prior to installation.

The identified weaknesses related to configuration management occurred for various reasons. For instance, at three locations, weaknesses existed because the sites' application development and vulnerability management programs did not include adequate testing processes and procedures to identify vulnerabilities related to attacks against web application functionality. One of these sites also did not implement application-level security controls designed to block malicious input. At two other locations, weaknesses were due, in part, to inadequate 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. The second 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.

In addition, for five locations, patch management deployment tools were not operating effectively and did not apply patches, as intended. We also found that some of these sites' vulnerability management processes were not fully effective in addressing known vulnerabilities,

including vulnerabilities related to unsupported software and missing patches. At another location, weaknesses occurred because Federal oversight officials and system managers had not recognized the system as a Federal information system. As such, applicable cybersecurity controls prescribed by NIST SP 800-53 were not implemented on the system, and required processes, such as patch and vulnerability management and configuration management, had not been developed and implemented. Further, officials at another location had not implemented password configuration requirements in accordance with defined parameters.

Identity and Access Management

The identity and access management security domain ensures organizations 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. However, our FY 2022 test work identified numerous access management concerns that resulted in the issuance of 22 recommendations, including the reissuance of 11 prior year recommendations. For instance:

- One location did not adequately manage and monitor database shared accounts. We determined that three database administrators used the default "System" account to perform their job duties. When multiple database administrators were performing work on the database at the same time, management was unable to demonstrate the ability to trace user activity to a specific user account for individual accountability purposes. Further, the site had not completed adequate user access reviews, which resulted in a terminated employee's account not being disabled or removed in a timely manner.

- Contrary to NIST requirements and site policies, we found weaknesses related to access reviews of standard and/or privileged accounts at three locations. Consistent with our prior year's finding, one location had not conducted annual access reviews of database and operating system privileged user accounts for certain applications. We determined that privileged accounts for these applications had not been reviewed since at least February 2020. At another location, application and database user access reviews were not performed to ensure appropriate user access. A third location had not documented periodic reviews of standard and privileged user accounts on a critical business system. Although periodic reviews were initiated by providing system owners with a user account listing, a response or acknowledgement of the users' continued need for system access was not required, requested, or tracked. Failure to regularly review and validate user access increases the risk that unauthorized users could retain access to and potentially modify information.

- Officials at one site reviewed had not fully implemented access controls to properly manage privileged user access and enforce separation of duties for the tested application. Specifically, our prior review identified server administrators and developers with access to the command that allows a general user to masquerade as a "superuser[1]." This issue

[1] Superuser accounts are highly privileged accounts primarily used for administration by specialized information technology employees. These users/accounts may have unlimited privileges, or ownership, over a system.

was first identified during our FY 2021 evaluation and was not expected to be completed until after our FY 2022 test work. We also identified a weakness related to access control implementation over database service accounts where 148 database service accounts were created without identification of a unique account owner, which prevented the site from revalidating the accounts. As such, there is an increased risk that unauthorized accounts exist, potentially impacting the confidentiality of the systems.

- At one location, site officials had not fully implemented account management controls for the Linux servers in accordance with Federal and site-level requirements. In particular, five users were granted system administrator ("root" level) access to the tested production application and database servers without proper account authorization documentation. As a result of our test work, officials removed the users from having "root" level access and initiated the proper account request process. We also noted that two server system administrators did not have authorized access to the servers. Further, site officials had not performed annual account reviews and reauthorizations for certain privileged accounts to validate the continued need for such access.

- Three sites had not removed user accounts in a timely manner when they were no longer needed. At one site, the annual application user access review identified eight user accounts that were requested for removal; however, none of the accounts had been disabled or deactivated at the time of our review. At another location, one database administrator user account was not removed until 7 months after the administrator's access had not been revalidated even though site policy required the removal of accounts no more than 10 days after the revalidation process was completed. At a third location, we concluded that contractor accounts may not be removed in a timely manner upon employee termination. Although the site had implemented a process to manually run scripts to identify, disable, and delete inactive accounts, the process did not include scripts to disable or deactivate contractor accounts immediately upon termination.

- Weaknesses in separation of duties related to certain roles and responsibilities were identified at three sites. For instance, at one site, 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 even though 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 another location, we determined that a developer had inappropriately promoted changes to the production environment in at least two instances, and in another instance, the change was not approved prior to the promotion of the change to the production environment.

Superuser account privileges may allow full read/write/executive privileges, creating or installing files or software, modifying files and settings, and/or deleting users and data.

- One location had not ensured that reviews of application user roles were completed for all financial process areas. This issue was first identified during our FY 2021 evaluation, and management indicated that corrective actions would be completed in FY 2023. 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 conflict that could permit a person with these roles to 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, and many of the database service accounts were created prior to the development of the site's current requirements for service account management. In addition, four locations did not ensure that appropriate separation of duties controls were established to address related risks. Officials at one of these locations also did not implement a sufficient control to retain evidence of password changes made in response to changes in roles or personnel that no longer required access. 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, the site did not have a process in place to ensure that all role reviews were completed, as required. The same site also had not established a policy to identify and separate conflicting roles that could allow an individual to make unauthorized system changes; moreover, the site did not create 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. Further, we found that four locations did not have fully documented policies and procedures that specified requirements for account management, including the processes for managing and monitoring database shared accounts; conducting periodic user access reviews; and/or requesting, approving, and authorizing server accounts. Finally, one location had a system flaw where terminated dates were not required to be inputted which resulted in terminated contractor accounts not being automatically disabled.

Data Protection and Privacy

The data protection and privacy security domain focuses on the extent to which agencies protect personally identifiable information and other sensitive information and have controls in place to prevent data exfiltration. Throughout our test work, we identified weaknesses related to the data protection and privacy programs implemented at sites across the Department. In particular, our review determined that, contrary to NIST requirements, one site had not defined security controls to protect personally identifiable information and other sensitive agency data, as appropriate, throughout the data lifecycle. To its credit, the site had created a plan of action and milestones to address this weakness. In addition, another location had not monitored and analyzed qualitative and quantitative performance measures on the effectiveness of data exfiltration and enhanced network defenses, and a third location did not monitor or audit its Domain Name System records, which would aid in preventing attackers from obtaining unauthorized access and disrupting normal business operations. We also found that a fourth location had not fully implemented security controls to prevent data exfiltration. 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 one of the locations reviewed had not effectively implemented security training programs for unclassified information systems. In particular, we found that individuals with privileged system access or other security-related responsibilities had not taken role-based security training, as required. In addition, site officials had not identified which roles and associated access levels should be subject to role-based training. These weaknesses occurred, in part, because officials had not established a role-based training program for personnel with privileged system access or other security-related responsibilities. Without an adequate security awareness and training program, privileged system users and those with significant security responsibilities, may not be fully educated or trained to perform their cybersecurity-related duties and responsibilities consistent with policies, procedures, and agreements. To the Department's credit, five locations reviewed adequately assessed the skills, knowledge, and abilities of their workforces and addressed any identified gaps through training and/or talent acquisition.

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—ISCM. The Detect cybersecurity function relates to several security assessment and authorization cybersecurity controls in NIST SP 800-53, Revision 5, including categories related to ISCM, anomalies and events, and detection processes. During FY 2022, we identified various weaknesses at programs and sites related to the implementation of the Detect cybersecurity function.

ISCM

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 two prior year recommendations. For instance, one location had not fully implemented database audit logging and monitoring of certain databases. 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 still had not been corrected at the time of our FY 2022 review. Management indicated that the site was in the process of implementing database audit logging and monitoring and that corrective actions were to be completed by the end of FY 2022. The identified ISCM weaknesses occurred because the site did not conduct an analysis to determine the feasibility of implementing database audit logging and monitoring controls, and the site did not perform 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, such access 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.

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 5, including categories related to response planning, communications, analysis, mitigation, and improvements. During FY 2022, we identified some areas of improvement related to the implementation of the Respond cybersecurity function.

Incident Response

The incident response security domain includes an emphasis on ensuring that the organization uses 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 concluded that three locations had not monitored and analyzed qualitative and quantitative performance measures on the effectiveness of their incident handling to ensure the scope and results of incident handling activities are comparable and predictable across the organization. In addition, two of the sites had not monitored performance measures on the effectiveness of their incident detection and analysis processes.

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 function relates to the contingency planning cybersecurity controls found in NIST SP 800-53, Revision 5, including categories related to recovery planning, improvements, and communication. During FY 2022, we identified an opportunity to improve 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. Our review identified that although three sites consistently implemented contingency plan testing, they did not use automated mechanisms for testing those contingency plans more thoroughly and effectively. To the Department's credit, we concluded that each of the locations reviewed had conducted organizational and system-level business impact analyses and integrated the results of the analyses into enterprise risk management processes.

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. Such risk 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. During our FY 2022 review, we found that locations had made only limited progress to close findings from our previous reviews. In some cases, sites had implemented mitigating controls to reduce the risk from identified weaknesses.

Notably, in FY 2022, Office of the Chief Information Officer officials stated that they continued to make progress towards improving the organization's cybersecurity posture through a risk-based approach. For example, Department officials noted that they implemented an ISCM dashboard to provide visibility to executive leadership. The officials also noted that the Department is focused on, among other things, combating advanced persistent threats, forging interagency and sector partnerships to protect critical infrastructure, enhancing policy and guidance, and advancing technologies for cyber defense. 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 73 recommendations (of which 38 were made during prior evaluations) to the Department's programs and sites, 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 2022, we also issued notices of findings and recommendations related to cybersecurity program management at a selected location. Corrective actions to address each of the recommendations, if fully implemented, should enhance the Department's unclassified cybersecurity program.

Management Comments

Management concurred with all but two recommendations issued to programs and sites related to improving the Department's cybersecurity program. Management also 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. Further, management commented that certain actions had been taken to remediate weaknesses identified, including weaknesses related to the two recommendations for which management nonconcurred.

Management's comments are included in Appendix 4.

Office of Inspector General Response

Management's comments and planned corrective actions were generally responsive to recommendations made during our evaluation. Due to the timing of our test work, we did not validate any noted corrective actions. In response to management's comments, we modified certain language in the report to ensure that it was not Controlled Unclassified Information.

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
Special Publication	SP

Appendix 2

Objective, Scope, and Methodology

Objective

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

Scope

We conducted the evaluation from March 2022 through March 2023 at 27 Department locations primarily under the responsibility of the Administrator for the National Nuclear Security Administration, Under Secretary for Science and Innovation, the Office of Environmental Management, and certain staff offices. Of the 27 locations reviewed, 6 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 Office of Management and Budget and the Council of the Inspectors General on Integrity and Efficiency. In fiscal year 2022, significant changes were made to the FISMA approach to include evaluating a set of core metrics annually and evaluating the remaining metrics on a 2-year cycle. As such, our scope was reduced to an evaluation of the core metrics over the Department's unclassified cybersecurity program.

Our evaluation involved a limited review of general information technology controls in the areas of access reviews, account management, configuration management, and segregation of duties. Where vulnerabilities were identified, the review did not include a determination of whether all 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 unclassified cybersecurity program. This evaluation was conducted under OIG project number A22TG009.

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 core FISMA metrics established by the Office of Management and Budget and the Council of the Inspectors General on Integrity and Efficiency in conjunction with the OIG's contract auditor, KPMG LLP (KPMG). The metric reviews were conducted at six locations across various Department programs/elements and performed in accordance with Office of Management and Budget M-22-05, *Fiscal Year 2021-2022 Guidance on Federal Information Security and Privacy Management Requirements* and the *FY 2022 Core IG FISMA Metrics Evaluation Guide*.

- Evaluated selected Headquarters offices and field sites in conjunction with the annual audit of the Department's consolidated financial statements, using work performed by KPMG.

Work by the OIG and KPMG 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, 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.

We conducted this evaluation in accordance with the Council of the Inspectors General on Integrity and Efficiency's *Quality Standards for Inspection and Evaluation* (December 2020). 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 comprehensive assessment of each site and organization each fiscal year. As such, and as permitted by FISMA, we used 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 diverse 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.

We held an exit conference with management officials on April 26, 2023.

Appendix 3

Related Reports

Office of Inspector General

- Evaluation Report on *The Department of Energy's Unclassified Cybersecurity Program – 2021* (DOE-OIG-22-33, June 2022). The Department of Energy, including the National Nuclear Security Administration, had taken actions to address many previously identified weaknesses related to its unclassified cybersecurity program. Department programs and sites had taken many corrective actions 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, our current evaluation identified weaknesses in areas including 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 which were similar in type to those identified in our prior evaluations.

- 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 unclassified 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 recommendations. 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 evaluations.

Government Accountability Office

- *CRITICAL INFRASTRUCTURE PROTECTION: Agencies Need to Assess Adoption of Cybersecurity Guidance* (GAO-22-105103, February 2022)

- *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)

Appendix 3

- *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)

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

Management Comments

Department of Energy
Washington, DC 20585

April 10, 2023

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-2022"

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 - 2022*." 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 all but 2 recommendations issued this year to DOE's programs and sites related to improving the Department's cybersecurity program. The Department also requests that the OIG review the sentence in the MEMORANDUM FOR THE SECRETARY referencing the Office of River Protection (ORP) and consider updating it to remove the specific types of recommendations and avoid this type of sensitive information being released to the public when the report is issued. As written, this sentence is Controlled Unclassified Information, as it ties specific issues to a specific site, which could help malicious actors narrow their attack vectors and increase the threat to EM's ORP systems.

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. Dan Lagraffe, Acting Deputy Chief Information Officer for Cybersecurity, at (202) 586-5632.

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.