Office of Inspector General

OFFICE OF CYBER ASSESSMENTS AND DATA ANALYTICS

EVALUATION REPORT

THE DEPARTMENT OF ENERGY'S UNCLASSIFIED CYBERSECURITY PROGRAM – 2023

DOE-OIG-24-17
MAY 2024

Department of Energy
Washington, DC 20585

May 17, 2024

MEMORANDUM FOR THE SECRETARY

SUBJECT: Evaluation Report on The Department of Energy's Unclassified Cybersecurity Program – 2023

The attached report discusses the results of our fiscal year 2023 Federal Information Security Modernization Act of 2014 evaluation. Our evaluation determined that the Department of Energy, including the National Nuclear Security Administration, had taken actions to address some of the previously identified weaknesses related to its unclassified cybersecurity program. Department programs and sites had taken corrective actions which resulted in the closure of 45 of 73 (62 percent) recommendations made during our prior year audits and evaluations. We also issued 39 new recommendations throughout fiscal year 2023, many of which were similar in type to the deficiencies identified in our previous reports (Appendix 1). If fully implemented, the 67 open recommendations should enhance the Department's unclassified cybersecurity program. Management concurred with the findings and recommendations and indicated that corrective actions had been taken or were planned. As noted in the Office of Inspector General's Special Report, *Management Challenges at the Department of Energy — Fiscal Year 2024* (DOE-OIG-24-05, November 2023), the weaknesses we identified, as well as a myriad of other challenges, emphasized the Department's need to conduct analyses and take enterprise-wide actions necessary to improve its cybersecurity posture.

We conducted this evaluation from February 2023 through March 2024 in accordance with the Council of the Inspectors General on Integrity and Efficiency's *Quality Standards for Inspection and Evaluation* (December 2020). This report summarizes findings from this evaluation, notices of findings and recommendations, and other audits released during fiscal year 2023. This report does not address the status of corrective actions that may have occurred since the reports were issued. 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 program and site 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 appreciated 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-24-17

Department of Energy
Office of Inspector General

The Department of Energy's Unclassified Cybersecurity Program – 2023
(DOE-OIG-24-17)

WHY THE OIG PERFORMED THIS EVALUATION

The Federal Information Security Modernization Act of 2014 requires Federal agencies to develop, implement, and manage agency-wide information security programs. Agencies are also required to provide acceptable levels of security for the information and systems that support their operations and assets.

The Federal Information Security Modernization Act of 2014 also mandates that the Office of Inspector General conduct an independent evaluation to determine whether the Department of Energy's unclassified cybersecurity program adequately protected its data and information systems in accordance with Federal and Department requirements.

What Did the OIG Find?

Our fiscal year 2023 Federal Information Security Modernization Act of 2014 evaluation determined that the Department, including the National Nuclear Security Administration, had taken actions to address some of the previously identified weaknesses related to its unclassified cybersecurity program. Actions were taken to close 45 of 73 (62 percent) recommendations from our prior year audits and evaluations. We also issued 39 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, findings at some Department sites related to configuration and vulnerability management practices revealed vulnerabilities that could have allowed malicious attacks that could have disrupted normal business operations or have negative impacts on system and data reliability. 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.

What Is the Path Forward?

When fully implemented, our recommendations should help to enhance the Department's unclassified cybersecurity program. The Department should emphasize closing findings in a timely manner, especially those findings repeated from prior years. As cybersecurity remains an ongoing challenge, it is important that the Department identify the root cause for ongoing cybersecurity issues and take corrective actions.

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. As part of that evaluation, the OIG is required to assess the Department's cybersecurity program according to FISMA security 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. As noted in Table 1, the metrics are focused on five cybersecurity functions and nine security domains and are aligned with the *National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity*.

Table 1: Cybersecurity Functions and Domains

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 Fiscal Year (FY) 2023 FISMA security metrics.

Inspectors General are required to assess the effectiveness of information security programs on a maturity model spectrum, in which the foundational levels ensure that agencies develop sound policies and procedures, and the advanced levels capture the extent that agencies institutionalize those policies and procedures. The five maturity model levels are "ad hoc," "defined," "consistently implemented," "managed and measurable," and "optimized." Descriptions of these levels are included in Table 2. Within the context of the maturity model, the Office of Management and Budget asserted that achieving a "managed and measurable" level, or above, represents an effective level of security.

Table 2: Inspector General Evaluation Maturity Levels

Maturity Level	Maturity Level Description
Level 1: Ad Hoc	Policies, procedures, and strategies are not formalized; activities are performed in an ad-hoc, reactive manner.
Level 2: Defined	Policies, procedures, and strategies are formalized and documented but not consistently implemented.
Level 3: Consistently Implemented	Policies, procedures, and strategies are consistently implemented, but quantitative and qualitative effectiveness measures are lacking.
Level 4: Managed and Measurable	Quantitative and qualitative measures on the effectiveness of policies, procedures, and strategies are collected across the organization and used to assess them and make necessary changes.
Level 5: Optimized	Policies, procedures, and strategies are fully institutionalized, repeatable, self-generating, and regularly updated based on a changing threat and technology landscape and business/mission needs.

Source: *FY 2023 – 2024 Inspector General FISMA Reporting Metrics*.

In 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. Specifically, a set of core metrics are evaluated annually, and the remaining metrics are evaluated on a 2-year cycle.

For the FY 2023 and FY 2024 cycles, metrics were updated to determine an agency's progress in implementing these requirements. Specifically, eight core metrics related to hardware and software asset management, configuration settings, flaw remediation, third-party security, account management, incident detection and analysis, and data exfiltration and enhanced network defenses were updated. The scope of our review included an evaluation of the core metrics and supplemental metrics for FY 2023.

To support our evaluation, we conducted control testing and assessments of various aspects of the unclassified cybersecurity programs at 28 Department locations under the purview of the Administrator for the National Nuclear Security Administration, Under Secretary for Science and Innovation, the Office of Environmental Management, and certain staff offices. Our evaluation 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 cybersecurity metric work performed at six Department locations during FY 2023.

Report Objective

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

Results of Review

Our FY 2023 evaluation determined that the Department had taken actions to address some of the previously identified weaknesses. Specifically, Department programs and sites had taken corrective actions related to areas such as configuration management, audit logging and monitoring, and identity and access management. This resulted in the closure of 45 of 73 (62 percent) recommendations made during our prior year audits and evaluations. We also issued 39 new recommendations throughout FY 2023, many of which were similar in type to the deficiencies identified in our previous reports (Appendix 1). Our FY 2023 evaluation identified weaknesses in three 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, and information security continuous monitoring (ISCM). Further, we identified opportunities for improvement during our FISMA cybersecurity 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 supporting asset management, governance, and risk assessment. During our FY 2023 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 FY 2023 work identified several risk management concerns across the Department. For instance:

- One location did not always effectively implement security controls related to asset management. The site had not always documented or maintained an all-inclusive information system component inventory for its general support system. For example, we identified 310 servers that were not included in the component inventory. As noted by NIST, a complete information system component inventory identifies system-specific information that is required for proper component accountability and security. We also determined that the site did not have a security architecture documented that was reflective of the current operating environment. The architecture document was last updated in 2015 and still referred to NIST SP 800-53, Revision 3, *Recommended Security*

Controls for Federal Information Systems and Organizations, even though Revision 5 was established in September 2020. The document also referenced the use of Windows servers that had reached end-of-life support in 2015 and 2020.

- We identified an opportunity for improvement at one location related to the approval of control assessments and results. We found that although control assessment plans were developed and control assessments were performed annually, the plans were not reviewed and approved by the Authorizing Official prior to conducting the assessment, as required by NIST. The Authorizing Official's review and approval of control assessment plans help to ensure that plans are consistent with security and privacy objectives, support continuous monitoring and near real-time risk management, and are cost-effective.

- As noted in our recent report, *Security over Cloud Computing Technologies at Select Department of Energy Locations* (DOE-OIG-23-18, March 2023), five locations had numerous weaknesses related to authorizing, monitoring, and assessing cloud-based services. In particular, two locations used cloud-based systems without appropriate approval, and three locations had not conducted complete system authorizations for cloud systems. We also found that three locations had not conducted required continuous security monitoring of cloud services that were authorized through the Federal Risk and Authorization Management Program. Further, we identified that significant amounts of information were stored in unapproved cloud storage accounts. We also determined that the Department did not have an accurate inventory of cloud-based systems used across the enterprise and that programs and sites generally used many more cloud computing systems than they reported. Specifically, at the beginning of our review, the Department was aware of 103 cloud-based systems at the 5 locations reviewed. However, during our test work, we determined that these locations operated a total of 227 cloud-based systems.

- We identified six locations with numerous devices that were running unsupported software across workstations and/or servers. We found that these devices were not configured with the latest known versions of application software. For example, at 1 location, we identified over 350 critical vulnerabilities related to unsupported software on 77 of 151 (51 percent) workstations tested. We also found another location with critical vulnerabilities related to unsupported software on all 16 servers tested.

- Six locations were operating workstations and servers that had missing critical- and high-risk vulnerability security patches or updates. We found that 417 of 619 (67 percent) workstations and 437 of 634 (69 percent) servers tested were operating with missing patches or updates that had not been applied within each location's established timeframes. For example, at 1 location, 122 workstations tested had missing patches that could have addressed over 1,600 critical- and high-risk vulnerabilities. The same location also had missing critical- or high-risk patches or updates on 389 of 531 (73 percent) servers tested. 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.

The identified weaknesses related to risk management occurred for various reasons. For example, we found that policies and procedures were not fully developed or lacked sufficient detail to ensure security controls were appropriately designed and implemented across the risk management domain area. Additionally, some locations reviewed had not issued enterprise-level policies and procedures to ensure the Department's cloud systems inventory was complete and accurate, nor had they always modified continuous monitoring processes to utilize all available information to ensure cloud systems were operating within the site's risk tolerance, including keeping the Authorizing Official aware of any system changes.

At six locations, vulnerability management processes were not always fully effective in addressing known vulnerabilities, including vulnerabilities related to unsupported software and missing patches. Without adequate risk management controls, the Department may be unable to effectively prioritize cybersecurity activities and manage the likelihood that an event will occur.

To the Department's credit, our FISMA cybersecurity work identified that many of the six sites had effectively implemented metrics related to risk management at their respective sites. Specifically, five of six sites reviewed had effectively maintained a comprehensive and accurate inventory of information systems. These sites had also effectively used standard data elements to develop and maintain an up-to-date inventory of hardware assets connected to their organization's network that included detailed information necessary for tracking and reporting. Further, five of the sites reviewed had sufficiently communicated information about cybersecurity risks in a timely and effective manner to appropriate internal and external stakeholders.

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 identified an opportunity for improvement related to supply chain risk management at one site reviewed. In particular, the site had not implemented controls to document, monitor, and maintain valid provenance of organizational defined systems, system components, and associated data. A site official stated that coordination efforts were underway to establish the origin, ownership, location, and changes to systems, components, and data. Additionally, site officials stated that the requirement to have the assessment plans approved by the Authorizing Official prior to the assessment is a new NIST 800-53, Revision 5, requirement that did not exist under NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*. The site is in the process of updating its security plan accreditations to NIST SP 800-53, Revision 5, and will address this new NIST update once implemented. 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. To the Department's credit, four locations reviewed during our FISMA cybersecurity metric testing adequately implemented policies and procedures to manage supply chain risk management activities at all organizational tiers. The sites also ensured that products, system components, systems, and services of external providers were consistent with the organization's cybersecurity and supply chain requirements.

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 2023 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 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 11 prior year recommendations. However, we found that configuration management weaknesses continued to exist. For instance:

- At 1 location, we identified 17 servers and 5 printers that were running services with web management interfaces configured with accounts set to default passwords or did not have a password set. We also identified a server message block share that was configured to allow anonymous read/write access. Attackers could exploit these vulnerabilities to obtain unauthorized access to the servers and printers, reconfigure or install malicious firmware on the affected devices, cause a denial of service preventing valid users from using the services and printers, or use the server message block share to spread malware.

- 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, 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. Follow-up testing to determine the status of the recommendations will be conducted in FY 2024. The applications reviewed at the other two locations accepted malicious input data and trusted a user-supplied parameter for executing protected functions within the application, which could have allowed an attacker to add unauthorized data to other users' data sets.

- 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 continued to exist even though they were first identified during our FY 2021 evaluation.

- One location had not developed, documented, or maintained baseline configurations for its financial management system. The location also had not reviewed and updated established baseline configurations and settings for its general support system. We found that security baselines were not reviewed and updated every 6 months, as required, thereby exposing the systems to vulnerabilities that otherwise could have been mitigated. We also found that the site did not always document deviations from configuration settings and associated approvals. Further, site personnel did not always document the review, approval, security impact, and/or implementation of configuration changes. For example, 5 of 16 (31 percent) configuration changes tested did not document the necessary requirements to implement the change. In another instance, one of the changes was an emergency change that did not have documentation of an implementation plan, a configuration change decision, lessons learned, or coordination with the site's change authority.

- At one location, we identified 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. This issue was first identified during our FY 2022 evaluation and still had not been corrected at the time of our FY 2023 review.

Our FISMA metric work also determined that five of the six sites reviewed had effectively adopted the Trusted Internet Connection 3.0 program to assist in protecting their networks. Further, five sites effectively used a vulnerability disclosure policy as part of vulnerability management programs for internet-accessible Federal systems. However, we concluded that while two sites had effectively implemented flaw remediation processes, including asset discovery, vulnerability scanning, analysis, and patch management to manage software vulnerabilities on all network addressable internet protocol assets, the remaining four sites had not implemented all elements necessary to be considered effective. Two of the four sites had achieved a "consistently implemented" maturity level for this metric, but some requirements had not yet been applied at these sites to meet a "managed and measurable" maturity level. For example, one of these sites was still in the process of implementing an automated methodology to manage its flaw remediation process, and another site was not centrally managing its flaw remediation process and had not established qualitative and quantitative performance measures to monitor the effectiveness of its flaw remediation processes.

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. Two 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. Neither site ensured that anonymous access and default credentials were changed prior to connecting systems to the production network and throughout the system lifecycle. Additionally, both sites' vulnerability management processes did not ensure that systems with anonymous access and default credentials on the production network were identified, monitored, and remediated.

One location had not ensured implementation of configuration management policies and procedures. While policies and procedures existed, they were not always fully implemented or did not address all necessary requirements to ensure an effective configuration management program. At another location, weaknesses occurred because Federal oversight officials and system managers had not recognized the system as a Federal information system. As a result, 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 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. The Department had taken action to close 18 prior year recommendations related to identity and access management; however, weaknesses continued to exist. For instance:

- Contrary to NIST requirements and site policies, we found weaknesses related to access reviews of standard and/or privileged accounts at two locations. For example, one 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. Follow-up testing to determine the status of the recommendations will be conducted in FY 2024. At another location, user access reviews excluded administrators within the "wheel" group who had root access and administrative accounts on one of the Linux database servers. We also noted discrepancies related to the data used for conducting account reviews. In particular, the application user access listing did not match the system-generated listing observed and erroneously included two administrative accounts. We found that this site also failed to remove four database administrator accounts, as requested by the system owner as part of a previous review performed in March 2022. 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 account management and separation of duties controls for the tested application. Specifically, one database administrator who was granted system administrator ("root" level) access to the financial servers was also assigned an "Admin" role; three Linux system administrators were assigned an "Admin" role; and two users with disabled and terminated accounts were not removed from the "Admin" role of the tested application.

- Weaknesses with separation of duties related to certain roles and responsibilities continued to be identified at two sites. 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. The site also 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, separation of duties and least privilege processes did not make certain that access rights within systems and applications were configured and documented to ensure certain key tasks were separated. We also found that system owners had not identified key tasks and considered how those tasks would be audited to identify when potential conflicts occurred.

In addition, our FISMA metric work determined that all six sites reviewed had effectively implemented phishing-resistant multifactor authentication mechanisms for privileged users to access their organization's networks and systems, including for remote access. However, these sites had not implemented all requirements necessary to ensure that privileged accounts were provisioned, managed, and reviewed in accordance with the principles of least privilege and separation of duties. While three of these sites had achieved a "consistently implemented" level, we identified two sites that had not reviewed account permissions to validate appropriateness of continued access. Additionally, a third site had not conducted periodic access reviews of privileged accounts at all.

The identity and access management weaknesses occurred, in part, because some officials were unaware of current account management requirements. For instance, at one site, we noted that although the site had an automated mechanism capable of identifying administrative accounts for its Windows servers, the process for identifying similar accounts for Linux was performed manually. This led to officials inadvertently excluding certain Linux administrative accounts from its semiannual review process. We also found that there was no formalized process in place to validate the removal of terminated user accounts.

Further, two locations did not ensure that appropriate separation of duties controls were established to address related risks. Officials at one of the 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. At another location, officials relied on a manual separation of duties process wherein the system owner was expected to recognize potentially conflicting roles and tasks and prevent unauthorized group membership that would violate role separation.

Data Protection and Privacy

The data protection and privacy security domain focuses on the extent to which agencies protect personally identifiable information (PII) and other sensitive information and have controls in place to prevent data exfiltration. Throughout our test work, we identified weaknesses related to data protection and privacy programs implemented at Department sites. We identified an

opportunity for improvement at one location which indicated that the site had not performed privacy risk assessments for all applications processing PII. Specifically, the site had not developed an overall or individual application privacy risk assessment for its general support system. According to a site official, an overarching privacy risk assessment for the general support system had not been prepared due to the complex nature of the information residing on applications. To minimize the complications, the site decided to document privacy risk assessments for individual applications within the general support system that processed PII; however, efforts were not completed by the established target date of February 2023.

Our FISMA cybersecurity metric work identified that one site had effectively developed a privacy program for the protection of PII that is collected, used, maintained, shared, and disposed of by information systems. Another site had achieved a "consistently implemented" rating. However, four of the six sites had only achieved a "defined" maturity level for this metric. Further, while one site had implemented appropriate security controls to protect PII and other sensitive agency data throughout the data lifecycle, the other five sites had not implemented all requirements necessary to achieve a "managed and measurable" maturity level rating. Three of these sites had achieved a "consistently implemented" rating, and the remaining sites were rated as "defined." Finally, we determined that one of the sites reviewed had effectively implemented security controls to prevent data exfiltration and to enhance network defenses. Of the remaining five sites, four were rated at a "consistently implemented" maturity rating, and one was rated as "ad-hoc." Without adequate data protection and privacy cybersecurity controls, PII 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. Site officials also had not identified which roles and associated access levels should be subject to role-based training.

To the Department's credit, we determined, as part of our FISMA cybersecurity metric work, that four locations reviewed adequately assessed the overall skills, knowledge, and abilities of their workforces and addressed any identified gaps through training and/or talent acquisition. However, we found that two of the sites reviewed had not implemented all requirements needed to achieve a "consistently implemented" maturity level for this metric. For instance, we noted that one site had not conducted a recent and full workforce assessment. Another site was not able to demonstrate that the organization was periodically updating its workforce assessment and making progress towards addressing the identified gaps in knowledge, skills, and abilities through training or hiring of additional staff.

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.

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 2023, 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. For instance:

- One location had not fully implemented its cybersecurity program plan requirements to retain application, database, and system logs for at least 1 year to support after-the-fact investigations of security incidents and meet regulatory and site retention requirements. The latest retrievable audit event had a retention period of only 52 days. Without effective audit log retention controls, investigations of security incidents and other activities related to the data were at risk.

- Our assessment of one site's selected system security plans concluded that all required controls were not fully documented and may not have been effectively implemented. In particular, the site had not fully described its implementation of required NIST moderate baseline controls to ensure that security plans were consistent with its enterprise architecture and operating as intended. At the same site, a cybersecurity oversight structure had not been fully implemented to ensure that the required controls were operating effectively.

We also noted an opportunity for improvement at another site related to ISCM activities. Specifically, we determined that the site did not operate its unclassified environment under an ongoing authority to operate or ongoing authorization in accordance with best practices. As noted in NIST SP 800-37, Revision 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy,* a strategically designed, well-managed, organization-wide continuous monitoring program can be used to maintain a system's authorization to operate and keep required system information and data up to date on an ongoing basis.

The weaknesses identified occurred, in part, because site officials did not ensure that the configuration supporting application event log collection and 1-year retention was appropriately implemented. In addition, we noted that Federal and contractor officials at one site had not continuously monitored systems and applications to ensure that reviews were conducted of the required security controls for configuration management, contingency planning, security assessments, data security, and planning.

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 2023, we identified 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. Based on our FISMA cybersecurity metric work, we identified opportunities to improve the Department's process for incident detection and analysis. Specifically, five of the sites reviewed had not implemented all requirements necessary to capture event logging at the intermediate level. While four of these sites had achieved a "consistently implemented" rating for this metric, one of these sites had not fully implemented basic event logging capabilities in accordance with Federal requirements. Additionally, our review determined that one of the sites had not implemented mature policies and procedures for the incident response tools and methodologies employed at their location. Another site had not identified and implemented performance measures to evaluate the effectiveness of the incident response technologies at that location.

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 2023, we identified concerns with 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 FISMA cybersecurity metric work found that while three sites had achieved a "consistently implemented" maturity level rating related to their information system contingency planning processes, none of the sites reviewed had implemented all requirements necessary to achieve a "managed and measurable" maturity level. Additionally, our separate test work at one location found that officials had not adequately tested contingency plans to ensure that the site could recover essential operating functions in the event of a significant disruption. Although site policy required annual tabletop and functional exercises to be conducted, officials stated they had not ever tested the contingency plan for one system, and a test of another contingency plan had not been completed since 2020. We also noted an opportunity for improvement at this site related to the effectiveness of its contingency plans. In particular, the site has an opportunity to ensure that its contingency plans address how to maintain essential missions and business functions in the event of an information system disruption or failure; include processes to coordinate response activities with internal and external stakeholders; and ensure plans are approved and signed by key personnel.

Governance Challenges

In the OIG's Special Report, *Management Challenges at the Department of Energy — Fiscal Year 2024* (DOE-OIG-24-05, November 2023), we noted that the Department continues to experience many challenges related to the implementation of an effective cybersecurity program. Specifically, the Department's governance structure has caused the agency to fall behind changing cybersecurity requirements and enhancements. Despite Department directives requiring implementation of the latest Federal cybersecurity guidance published by NIST, various contractors performing work on behalf of the Department and at Department-owned facilities continue to implement and assess their cybersecurity environments against outdated requirements.

As part of our FISMA cybersecurity metric test work, we assessed the Department's progress in implementing NIST SP 800-53, Revision 5. NIST issued Revision 5 in September 2020. Prior to the issuance of Revision 5, all Federal programs were required to be compliant with NIST 800-53, Revision 4. Although NIST updated its guidance more than 3 years ago, we identified that five of six Department sites reviewed had not yet fully implemented NIST SP 800-53, Revision 5. At these sites, we identified 70 information systems still operating under the outdated NIST 800-53, Revision 4. At least 56 of the systems processed controlled unclassified information, including 22 systems that processed PII. One of the sites reviewed had not implemented a process to determine which of its 10 systems were used to process controlled unclassified information and PII.

Some of the sites reported that the revised guidance had not been implemented due to resource constraints and other commitments to process improvements. One of these sites indicated that it is working toward full implementation of NIST SP 800-53, Revision 5. Additionally, two of the sites indicated that they had plans of action and milestones in place to move their systems into compliance with NIST, SP 800-53, Revision 5, with implementation at one site expected to be completed by September 2024. Delayed implementation of these requirements could put sensitive information at risk. Further, the inability of Department locations to implement Federal

requirements in a timely manner could go beyond NIST direction and include critical requirements conveyed through the Cybersecurity and Infrastructure Security Agency, Executive Orders, and other mechanisms.

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, findings related to configuration and vulnerability management practices at some Department sites revealed vulnerabilities that could have allowed malicious attacks. These attacks could have resulted in unauthorized access to key systems, applications, and sensitive data, which could disrupt normal business operations or have negative impacts on system and data reliability. In addition, untimely patch management processes could result in additional systems or components with known and detected security vulnerabilities remaining unresolved in the production environment. Web application attacks could also disrupt normal business operations or have a negative impact on application and data reliability.

We also 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 2023 evaluation, 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, the Department indicated that during FY 2023 it continued to make progress toward improving the Department's cybersecurity posture through a risk-based approach. For example, the Department indicated that it had provided extensive cybersecurity related training to Authorizing Officials, and information system security officers focused on Department-related policies and procedures to safeguard information and information systems. The Department also noted that it is revising its cybersecurity policy, including incorporating new applicable laws, regulations, and mandates. The updated Department Order was scheduled for publication by February 2024; however, it was not completed at the time of our review. While these are positive steps, our test work determined that additional action is necessary to further strengthen the Department's unclassified cybersecurity program. Further, while we are not making a formal recommendation in this report, we concluded that the Department could benefit from identifying the root causes related to common areas of weaknesses such as risk management, configuration management, and identity and access management, and taking necessary corrective actions (see Appendix 1).

Recommendations

To address the cybersecurity weaknesses identified throughout the Department, we made 67 recommendations in FY 2023 (including 28 repeat recommendations 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 2023, 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 recommendations issued this year to programs and sites related to improving the Department's 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 also commented that a number of actions had been taken to address cybersecurity program weaknesses previously noted by the OIG.

Management's comments are included in Appendix 6.

Office of Inspector General Response

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

Appendix 1

Recommendations by Domain Category

The following table summarizes the Office of Inspector General's recommendations by security domain according to the *National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity* and *FY 2023 – 2024 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics*. Notably, most of the recommendations are relevant to security domains included within the Identify and Protect cybersecurity function areas.

Security Domain Category	Fiscal Year 2023	Fiscal Year 2022	Fiscal Year 2021
Risk Management[1]	24	10	15
Supply Chain Risk Management	0	0	0
Configuration Management	24	29	25
Identity and Access Management	9	22	11
Data Protection and Privacy	0	2	3
Security Training	2	1	0
Information Security Continuous Monitoring	3	3	3
Incident Response	0	0	0
Contingency Planning	0	0	1
Other Recommendations – Uncategorized[2]	5	6	3
Total Recommendations	**67**	**73**	**61**

[1] In the fiscal year 2022 report, six of the Risk Management recommendations were categorized under Configuration Management.

[2] These recommendations were issued in Office of Inspector General cybersecurity-related reports but are not specific to a domain category.

Appendix 2

Federal Information Security Modernization Act of 2014 Fiscal Year 2023 Metric Results[3]

Inspectors General are required to assess the effectiveness of information security programs on a maturity model spectrum, in which the foundational levels ensure that agencies develop sound policies and procedures, and the advanced levels capture the extent that agencies institutionalize those policies and procedures. The five maturity model levels are "ad-hoc," "defined," "consistently implemented," "managed and measurable," and "optimized." Within the context of the maturity model, the Office of Management and Budget asserted that achieving a Level 4 ("managed and measurable"), or above, represents an effective level of security. The following table presents the results of our security metrics testing for each of the six locations reviewed.

Metrics	A	B	C	D	E	F
Identify – Risk Management						
To what extent does the organization maintain a comprehensive and accurate inventory of its information systems (including cloud systems, public facing websites, and third-party systems), and system interconnections?	**4**	**4**	**4**	**2**	**4**	**4**
To what extent does the organization use standard data elements/taxonomy to develop and maintain an up-to-date inventory of hardware assets (including Government-furnished equipment and Bring Your Own Device mobile devices) connected to the organization's network with the detailed information necessary for tracking and reporting?	**5**	**4**	**4**	**3**	**4**	**4**
To what extent does the organization use standard data elements/taxonomy to develop and maintain an up-to-date inventory of the software and associated licenses used within the organization with the detailed information necessary for tracking and reporting?	**5**	**4**	**3**	**3**	**4**	**4**
To what extent does the organization ensure that information system security risks are adequately managed at the organizational, mission/business process, and information system levels?	**4**	**4**	**5**	**2**	**2**	**3**

[3] The metric results relayed here only include the sites tested by the Office of Inspector General's contract auditor, KPMG LLP. The metric reviews were conducted at six locations across various Department of Energy programs/elements and performed in accordance with Office of Management and Budget M-23-03, *Fiscal Year 2023 Guidance on Federal Information Security and Privacy Management Requirements*, and the *FY 2023 IG FISMA Metrics Evaluator's Guide*. Due to the sensitivity of the information, we did not include site names.

Appendix 2

Metrics	A	B	C	D	E	F
To what extent have the roles and responsibilities of internal and external stakeholders involved in cybersecurity risk management processes been defined, communicated, implemented, and appropriately resourced across the organization?	4	5	5	3	3	3
To what extent has the organization ensured that plans of action and milestones are used for effectively mitigating security weaknesses?	4	3	3	2	4	4
To what extent does the organization ensure that information about cybersecurity risks is communicated in a timely and effective manner to appropriate internal and external stakeholders?	4	4	5	4	3	4
To what extent does the organization use technology/automation to provide a centralized, enterprise-wide (portfolio) view of cybersecurity risk management activities across the organization, including risk control and remediation activities, dependencies, risk scores/levels, and management dashboards?	2	3	4	3	2	2
Identify – Supply Chain Risk Management (SCRM)						
To what extent does the organization use an organization-wide SCRM strategy to manage the supply chain risks associated with the development, acquisition, maintenance, and disposal of systems, system components, and system services?	4	5	4	1	4	3
To what extent does the organization use SCRM policies and procedures to manage SCRM activities at all organizational tiers?	4	5	4	1	4	3
To what extent does the organization ensure that products, system components, systems, and services of external providers are consistent with the organization's cybersecurity and supply chain requirements?	4	5	4	1	4	2
Protect – Configuration Management						
To what extent does the organization use baseline configurations for its information systems and maintain inventories of related components at a level of granularity necessary for tracking and reporting?	4	5	4	2	3	4

Appendix 2

Metrics	A	B	C	D	E	F
To what extent does the organization use configuration settings/common secure configurations for its information systems?	2	4	4	3	3	4
To what extent does the organization use flaw remediation processes, including asset discovery, vulnerability scanning, analysis, and patch management, to manage software vulnerabilities on all network addressable internet protocol-assets?	2	4	4	1	3	3
To what extent has the organization adopted the Trusted Internet Connection 3.0 program to assist in protecting its network?	5	5	5	1	5	5
To what extent does the organization use a vulnerability disclosure policy as part of its vulnerability management program for internet-accessible Federal systems?	3	4	4	4	4	4
Protect – Identity and Access Management						
To what extent have the roles and responsibilities of identity, credential, and access management (ICAM) stakeholders been defined, communicated, and implemented across the agency, and appropriately resourced?	2	4	4	1	3	2
To what extent does the organization use a comprehensive ICAM policy, strategy, process, and technology solution roadmap to guide its ICAM processes and activities?	3	4	3	1	3	3
To what extent does the organization ensure that access agreements, including nondisclosure agreements, acceptable use agreements, and rules of behavior, as appropriate, for individuals (both privileged and non-privileged users) that access its systems are completed and maintained?	4	3	4	4	4	3
To what extent has the organization implemented phishing-resistant multifactor authentication mechanisms (e.g., personal identity verification, Fast IDentity Online 2 (FIDO2), or web authentication) for non-privileged users to access the organization's facilities [organization-defined entry/exit points], networks, and systems, including for remote access?	3	4	4	4	4	4

Appendix 2

Metrics	A	B	C	D	E	F
To what extent has the organization implemented phishing-resistant multifactor authentication mechanisms (e.g., personal identity verification, Fast IDentity Online 2 (FIDO2), or web authentication) for privileged users to access the organization's facilities [organization-defined entry/exit points], networks, and systems, including for remote access?	4	4	4	4	4	4
To what extent does the organization ensure that privileged accounts are provisioned, managed, and reviewed in accordance with the principles of least privilege and separation of duties? Specifically, this includes processes for periodic review and adjustment of privileged user accounts and permissions, inventorying and validating the scope and number of privileged accounts, and ensuring that privileged user account activities are logged and periodically reviewed.	2	2	3	1	3	3
To what extent does the organization ensure that appropriate configuration/connection requirements are maintained for remote access connections? This includes the use of appropriate cryptographic modules, system time-outs, and the monitoring and control of remote access sessions.	4	4	4	3	4	4
Protect – Data Protection and Privacy						
To what extent has the organization developed a privacy program for the protection of personally identifiable information that is collected, used, maintained, shared, and disposed of by information systems?	2	4	2	2	2	3
To what extent has the organization implemented the following security controls to protect its personally identifiable information and other agency sensitive data, as appropriate, throughout the data lifecycle? • Encryption of data at rest • Encryption of data in transit • Limitation of transfer to removable media • Sanitization of digital media prior to disposal or reuse	2	4	3	2	3	3

Appendix 2

Metrics	A	B	C	D	E	F
To what extent has the organization implemented security controls (e.g., endpoint detection and response) to prevent data exfiltration and enhance network defenses?	4	3	3	1	3	3
Protect – Security Training						
To what extent have the roles and responsibilities of security awareness and training program stakeholders been defined, communicated, and implemented across the agency, and appropriately resourced? This includes the roles and responsibilities for the effective establishment and maintenance of an organization-wide security awareness and training program as well as the awareness and training-related roles and responsibilities of system users and those with significant security responsibilities.	2	4	4	2	3	3
To what extent does the organization use an assessment of the skills, knowledge, and abilities of its workforce to provide tailored awareness and specialized security training within the functional areas of identify, protect, detect, respond, and recover?	4	4	4	4	2	2
To what extent does the organization use a security awareness and training strategy/plan that leverages its skills assessment and is adapted to its mission and risk environment? Note: The strategy/plan should include the following components: • The structure of the awareness and training program • Priorities • Funding • The goals of the program • Target audiences • Types of courses/material for each audience • Use of technologies (such as email advisories, intranet updates/wiki pages/social media, web-based training, phishing simulation tools) • Frequency of training • Deployment methods	2	4	5	1	4	4

Appendix 2

Metrics	A	B	C	D	E	F
Detect – Information Security Continuous Monitoring						
To what extent does the organization use information security continuous monitoring (ISCM) policies and an ISCM strategy that addresses ISCM requirements and activities at each organizational tier?	**3**	**4**	**5**	**4**	**3**	**3**
To what extent have ISCM stakeholders and their roles, responsibilities, levels of authority, and dependencies been defined, communicated, and implemented across the organization?	**4**	**5**	**4**	**4**	**3**	**3**
How mature are the organization's processes for performing ongoing information system assessments, granting system authorizations, such as developing and maintaining system security plans, and monitoring system security controls?	**3**	**5**	**4**	**4**	**2**	**3**
Respond – Incident Response						
How mature are the organization's processes for incident detection and analysis?	**3**	**4**	**3**	**2**	**3**	**3**
How mature are the organization's processes for incident handling?	**4**	**4**	**4**	**1**	**4**	**3**
To what extent does the organization collaborate with stakeholders to ensure onsite, technical assistance/surge capabilities can be leveraged for quickly responding to incidents, including through contracts/agreements, as appropriate, for incident response support?	**4**	**4**	**4**	**2**	**4**	**4**
To what extent does the organization use the following technology to support its incident response program? • Web application protections, such as web application firewalls • Event and incident management, such as intrusion detection and prevention tools, and incident tracking and reporting tools • Aggregation and analysis, such as security information and event management products • Malware detection, such as antivirus and antispam software technologies • Information management, such as data loss prevention • File integrity and endpoint and server security tools	**4**	**4**	**4**	**1**	**4**	**3**

Appendix 2

Metrics	A	B	C	D	E	F
Recover – Contingency Planning						
To what extent have roles and responsibilities of stakeholders involved in information systems contingency planning been defined, communicated, and implemented across the organization, including appropriate delegations of authority?	4	2	4	1	3	3
To what extent does the organization ensure that the results of business impact analyses are used to guide contingency planning efforts?	2	4	4	1	2	4
To what extent does the organization perform tests/exercises of its information system contingency planning processes?	3	2	3	1	2	3
To what level does the organization ensure that information on the planning and performance of recovery activities is communicated to internal stakeholders and executive management teams and used to make risk-based decisions?	3	2	4	1	3	3

Appendix 3

Commonly Used Terms

Department of Energy	Department
Federal Information Security Modernization Act of 2014	FISMA
Fiscal Year	FY
Identity, Credential, and Access Management	ICAM
Information Security Continuous Monitoring	ISCM
National Institute of Standards and Technology	NIST
Office of Inspector General	OIG
Personally Identifiable Information	PII
Special Publication	SP

Appendix 4

Objective, Scope, and Methodology

Objective

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

Scope

We conducted the evaluation from February 2023 through March 2024 at 28 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 28 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 Department of Homeland Security, 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.

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 A23TG002.

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-23-03, *Fiscal Year 2023 Guidance on Federal Information Security and Privacy Management Requirements* and the *FY 2023 IG FISMA Metrics Evaluator's 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.

Management officials waived an exit conference on May 6, 2024.

Appendix 5

Related Reports

Office of Inspector General

- Special Report on *Management Challenges at the Department of Energy — Fiscal Year 2024* (DOE-OIG-24-05, November 2023). The Department of Energy continues to experience many challenges related to the implementation of an effective cybersecurity program. Specifically, the Department lacks a centralized organizational structure, or a federated mechanism, to oversee enterprise-level risks facing the Department, and to obtain, process, and correlate real-time cyber data. In addition, the Department's governance structure has caused the agency to fall behind changing cybersecurity requirements and enhancements. Despite Department directives requiring implementation of the latest Federal cybersecurity guidance published by the National Institute of Standards and Technology, various contractors performing work on behalf of the Department and at Department-owned facilities continue to implement and assess their cybersecurity environments against outdated requirements.

- Evaluation Report on *The Department of Energy's Unclassified Cybersecurity Program – 2022* (DOE-OIG-23-20, May 2023). 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. Specifically, 38 of 61 (62 percent) recommendations from our prior year evaluations remained open. 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.

- Audit Report on *Security over Cloud Computing Technologies at Select Department of Energy Locations* (DOE-OIG-23-18, March 2023). Although the Department had implemented security measures over many of its cloud-based technologies and services, additional efforts are necessary. We found weaknesses with the Department's processes to authorize, monitor, assess, control, and inventory cloud-based services used by its programs and sites. Without improvements, the Department may not be adequately protected from the risks posed by the use of systems outside its physical network boundaries, such as unauthorized access and data exfiltration.

- Evaluation Report on *The Department of Energy's Unclassified Cybersecurity Program – 2021* (DOE-OIG-22-33, June 2022). The Department, 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.

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)
- *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 24, 2024

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-2023"

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 - 2023*." 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 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. Paul Selby, Deputy Chief Information Officer for Cybersecurity, at (202)-586-4386.

Printed with soy ink on recycled paper

FEEDBACK

The Office of Inspector General has a continuing interest in improving the usefulness of its products. We aim to make our reports as responsive as possible and ask you to consider sharing your thoughts with us.

Please send your comments, suggestions, and feedback to OIG.Reports@hq.doe.gov and include your name, contact information, and the report number. You may also mail comments to us:

Office of Inspector General (IG-12)
Department of Energy
Washington, DC 20585

If you want to discuss this report or your comments with a member of the Office of Inspector General staff, please contact our office at 202–586–1818. For media-related inquiries, please call 202–586–7406.