U.S. DEPARTMENT OF ENERGY

Office of Inspector General

DOE-OIG-25-30

August 14, 2025

The Department of Energy’s Unclassified Cybersecurity Program – 2024

EVALUATION REPORT

Department of Energy
Washington, DC 20585

August 14, 2025

MEMORANDUM FOR THE SECRETARY

SUBJECT: Evaluation Report: *The Department of Energy's Unclassified Cybersecurity Program – 2024*

The attached report discusses the results of our fiscal year 2024 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. Specifically, programs and sites had taken corrective actions which resulted in the closure of 19 of 63 (30 percent) recommendations made during our prior year audits and evaluations. However, 44 prior year recommendations remained open with weaknesses in areas such as risk management, configuration management, identity and access management, information security continuous monitoring, and security training. We also issued 79 new recommendations throughout the fiscal year. If fully implemented, the open recommendations should enhance the Department's unclassified cybersecurity program. Although management concurred with most of our findings, management at two sites did not concur with four of our recommendations. However, our testing results supported the issuance, and therefore, all issued findings and recommendations will remain open until the described weaknesses have been addressed.

We conducted this evaluation from January 2024 through May 2025 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 and other Office of Inspector General reports released during fiscal year 2024. 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 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.

Sarah Nelson

Sarah Nelson
Assistant Inspector General
for Management
Performing the Duties of the Inspector General
Office of Inspector General

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

DOE OIG HIGHLIGHTS

The Department of Energy's Unclassified Cybersecurity Program – 2024

August 14, 2025

Why We 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 We Found

Our fiscal year 2024 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. While actions were taken to close 19 of 63 (30 percent) recommendations from our prior year audits and evaluations, 44 prior year recommendations remained open. We also issued 79 new recommendations throughout the fiscal year related to various areas of cybersecurity programs.

The weaknesses identified occurred for a variety of reasons. For instance, findings at some Department sites had occurred due to vulnerability management processes that were not fully effective in identifying, addressing, and/or remediating vulnerabilities. We also found that several sites had not fully developed and/or maintained policies and procedures to help facilitate the design and implementation of security controls.

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.

What We Recommend

When fully implemented, the 123 recommendations made during fiscal year 2024 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 take action to implement the latest Federal cybersecurity requirements and enhancements to assist in ensuring adequate protection of the Department's data and information systems at risk to emerging threats and vulnerabilities.

Table of Contents

Appendices

Background and Objective

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 in coordination with representatives from the Office of Management and Budget (OMB) and the Council of the Inspectors General on Integrity and Efficiency, with review and feedback provided by several stakeholders, including the Federal Chief Information Officers and Chief Information Security Officers councils. 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 (SCRM)
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 (ISCM)
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 – 2024 Inspector General FISMA Reporting 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 OMB 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 OMB 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 2024 reporting cycle, our review included an evaluation of 20 core metrics and 17 supplemental metrics.

To support our evaluation, we conducted control testing and assessments of various aspects of the unclassified cybersecurity programs at 29 Department locations under the purview of the Administrator for the National Nuclear Security Administration, the Under Secretary for Science and Innovation, the Office of Environmental Management, the Office of the Chief Information Officer, the Office of the Chief Financial Officer, 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 2024.

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 2024 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 risk management, configuration management, information continuous monitoring, and identity and access management. This resulted in the closure of 19 of 63 (30 percent) recommendations made during our prior year audits and evaluations. However, 44 prior year recommendations remained open related to weaknesses in areas such as risk management, configuration management, identity and access management, ISCM, and security training. In addition, we issued 79 new recommendations[1] throughout FY 2024. The Department was able to close three of those recommendations. As a result, 120 recommendations had yet to be fully addressed at the end of the FY. Notably, three sites requested that the OIG not perform follow-up testing on open prior year findings during FY 2024, as corrective actions had not been fully implemented at any of the three sites. As a result, the findings remained open at these sites.

Our FY 2024 FISMA evaluation and other OIG reports, issued throughout the year, identified weaknesses within all five *National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity,* Version 1.1, function areas and each of the related security domains. 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 SCRM. 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 2024 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 assessment, and risk management strategy. Notably, the Department had taken action to address some of our previously identified risk management weaknesses, and we were able to close nine recommendations. However, our FY 2024 work continued to identify risk management concerns across the Department. For instance:

- Eight locations did not always effectively perform risk assessments. We found that one site had not included all relevant risks, such as environmental threats, within a system-specific risk assessment. As a result, the risk assessment may not have accurately reported the likelihood and magnitude of harm from disruption or destruction of the systems and the information that it processes, stores, or transmits. In addition, we identified weaknesses related to site-specific risk assessments performed at numerous other sites. We found that none of the site-specific risk assessments had documented the costs associated with rebuilding a system or network impacted by a ransomware event in accordance with Federal requirements. At the final site evaluated, we determined that risk assessments had not been completed for any of the three systems reviewed.

[1] The total number of new recommendations made during the FY includes those that were issued throughout the FY 2024 FISMA evaluation and those that were issued as a result of other OIG reports, as identified in Appendix 3.

- Two locations reviewed had system governance weaknesses. While a system at one location was managed by two personnel offices, defined roles and responsibilities between the two entities did not exist. As a result, several system-specific control deficiencies had been identified throughout our review. At another location, we found that neither of the two organizations perceived it to be their responsibility to address identified vulnerabilities, resulting in missing updates and patches on workstations.

- At one location, we identified an opportunity for improvement related to the implementation of asset management controls. While all three systems reviewed had information system component inventories, at least one was not current. Specifically, officials indicated that they maintained five separate system component inventories for the system under review. However, we discovered that eight components were not physically present as noted in the inventory.

- We identified nine locations with numerous devices that had unsupported software and/or were not configured with the latest security patches or latest known version of application software across workstations and/or servers. For example, at 1 location, we identified more than 120 critical- and high-risk vulnerabilities related to unsupported software on 58 of 62 (94 percent) workstations tested. At a different location where we performed prior year finding follow-up testing, we continued to find the same types of previously identified vulnerabilities and noted that instances of missing updates and patches increased from those found in the prior year. Specifically, while we found over 510 critical-, high-, and medium-risk vulnerabilities related to missing updates and patches on 10 of 15 (67 percent) of the servers tested in FY 2023, the number of weaknesses increased to 660 of the same type and criticality of vulnerabilities on 17 of 18 (94 percent) servers tested in FY 2024.

The identified weaknesses related to risk management occurred for various reasons. For example, we found that six sites had not developed and implemented processes in accordance with guidelines established by NIST SP 800-37, Revision 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, which requires organizations to conduct security and privacy risk assessments to ensure that each type of risk is fully assessed, such as ransomware threats. Additionally, we found that eight sites had vulnerability management processes that were not fully effective in identifying, addressing, and/or remediating vulnerabilities, including vulnerabilities related to unsupported software and missing patches. For instance, two of the eight sites had patch management deployment tools that were not operating effectively and did not apply patches, as intended. 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 metric work identified several risk management-related activities that had been effectively implemented. For instance, four of six sites reviewed had effectively maintained a comprehensive and accurate inventory of information systems. We also determined that three of the six sites had ensured that information system security risks were adequately managed at the organizational, mission/business process, and information system level. Further, one site reviewed had achieved the “optimized” maturity level for using an information security architecture to provide a disciplined and structured methodology for managing risk, including risk from the organization’s supply chain.

Supply Chain Risk Management

The SCRM 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. Cybersecurity SCRM is a systematic process for managing exposure to cybersecurity risk throughout supply chains and developing appropriate response strategies, policies, processes, and procedures. In FY 2024, we evaluated the Department’s progress in developing and implementing related supply chain requirements through our FISMA metric work and identified weaknesses within this area. For example:

- Three locations had not made adequate progress in ensuring products, system components, systems, and services of external providers were consistent with their organization’s cybersecurity and supply chain requirements. These locations had not defined, communicated, and/or implemented related SCRM policies, procedures, and processes. As a result, all three locations were rated at the “ad-hoc” maturity level.

- We identified three different locations that had not implemented processes to ensure that counterfeit components are detected and prevented from being introduced into their organization’s systems. While one of the three locations had developed and communicated related policies and procedures, it had not provided component authenticity or anti-counterfeit training. Therefore, the location had only achieved a “defined” maturity-level rating. The remaining two locations had not taken any steps in strengthening measures related to component authenticity and anti-counterfeit operations and, as such, were rated at the “ad-hoc” maturity level.

Some sites assessed indicated that the weaknesses identified occurred, in part, because they relied on the Department’s Cybersecurity SCRM program. For example, two sites noted that they were still in the process of onboarding into this program. Without effective Cybersecurity SCRM controls, organizations may not be effectively managing cybersecurity risks associated with external parties, such as identifying, assessing, and mitigating counterfeit items. However, to the Department’s credit, we determined that three sites assessed had effectively implemented products, system components, systems, and services of external providers consistently with their 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 four security domains that relate to cybersecurity controls found in NIST SP 800-53, Revision 5—configuration management, identity and access management, data protection and privacy, and security training security domains. Our FY 2024 evaluation identified weaknesses related to the Department’s implementation of all the security domains included in the Protect cybersecurity function.

However, to the Department's credit, actions were taken to address some of the weaknesses within this function area. As a result, we were able to close five prior year recommendations related to configuration management. In addition, we were also able to close five recommendations related to identity and access management.

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. Although the Department took actions to address some known configuration management weaknesses, we continued to identify control deficiencies related to this security domain. For instance:

- At two locations, we found that vulnerability remediation processes were not fully aligned with NIST vulnerability management requirements. The defined processes at both locations disclosed that vulnerabilities should be remediated based on discovery date. For example, at one location, site officials noted that the site's policy was written to follow the requirements set within its program office's Cybersecurity Program Plan, which contradicted NIST direction that organizations prioritize remediation activities based on the release date of the security relevant software and firmware updates. As a result, we identified vulnerabilities related to missing security updates and unsupported software at both locations. Without effective vulnerability management practices, servers and workstations that are missing security patches for known vulnerabilities or are running unsupported software are at risk for computer viruses and other malicious attacks that could give attackers control of the workstations, servers, or even the entire network.

- Our testing at four locations identified firewall rule deficiencies. Of the firewalls examined, we determined that multiple rules were overly permissive or granted unnecessary access. For example, at 1 site, we identified 66 rules that were overly permissive or granted unnecessary access to a specific application.

- We identified system integrity weaknesses at four locations. We determined that three of the four locations accepted malicious input data, which in some cases could have been used to launch attacks against legitimate application users and result in unauthorized access to applications. At one of the three locations, the malicious input data could also have been used to obtain unauthorized access to data within a certain application through legitimate users' web browsers. The fourth location had vulnerabilities that could have been used to perform unauthorized actions against users of a certain application.
- One site continued to have weaknesses involving default configurations of network systems even though we identified similar weaknesses during our prior year testing. Although improvements were observed, we continued to identify instances of default configurations and passwords in the production environments assessed, including a web server directory listing that was configured to allow anonymous access. We also identified several devices, including multifunction devices and web interfaces, that were configured with default credentials.

- Seven locations did not effectively define and/or implement configuration change control activities. For instance, although one site had established a process to review and approve configuration changes for two systems under review, a third system reviewed did not have adequate processes in place. Specifically, non-routine changes to the system were not approved by an independent and appropriately staffed Change Control Board.

- None of the six sites evaluated during our FISMA metric work had effectively implemented an enterprise-wide configuration management plan. The deficiencies within the plans at each site varied. For instance, at one site, the configuration management plan was not completely integrated within the risk management and continuous monitoring programs. We also determined that four of the six sites evaluated did not effectively use configuration settings or common security configurations for information systems. For example, at one site, we found that tools were used to collect configuration compliance confirmations; however, the data collected was not reviewed in a timely manner.

The identified weaknesses related to configuration management occurred for various reasons. For instance, firewall rule weaknesses occurred because a process to periodically review firewall rules and make the necessary changes, as appropriate, had not been implemented at any of the four sites reviewed. In addition, weaknesses identified involving default configurations of network systems at one site occurred, in part, due to the site inadvertently excluding an internet protocol range from its scanning profiles. Without effective configuration management procedures and practices, unauthorized access to key systems and the disclosure or unauthorized modification of sensitive information could occur. Failure to remedy the underlying causes for the conditions noted could also result in additional systems or components with unknown and undetected security vulnerabilities being introduced into and remaining in the production environment. To the Department's credit, during one of our reviews performed in the FY, we found that six sites had configured firewalls to limit access across their respective networks, implemented a content filter and/or malicious code detection capability, conducted routine vulnerability scans, and established patch management processes.

Identity and Access Management

The identity and access management security domain ensures that 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 actions to close four of the eight recommendations that remained open at the end of FY 2023 and one recommendation that was issued in FY 2024 related to identity and access management. However, our test work continued to identify numerous identity and access management concerns that resulted in the issuance of 21 recommendations. For instance:

- Weaknesses related to authentication management practices existed at two sites. The first location had not configured password parameters for one of its applications and databases in accordance with site policy requirements. At the other site, we identified nine multifunction devices and a remote access controller interface that were configured with default credentials which allowed connections without authentication. We also identified web servers and five file shares that were configured to allow anonymous access to certain directories storing sensitive information.

- Three sites had not effectively implemented account management practices related to non-privileged user access. The first location had not always obtained management approval prior to granting users access to one of its applications and did not consistently grant access in accordance with approved authorization forms. The site also failed to remove application-level access in a timely manner after users were terminated. At another site, we identified two legacy accounts on a database that had not been previously identified by site management. The third site had weaknesses with obtaining the appropriate management approval prior to users gaining access to a tested application and the operating system.

- Officials at four locations had not fully implemented processes related to account management for privileged users. Specifically, officials at one site inappropriately granted privileges to three developers that allowed them to implement changes into the production environment, without obtaining prior approval. This site also granted 10 general users privileged accounts, which gave them the ability to implement changes to one of the site's applications. At another location, we identified two application administrators that had obtained overly permissive access to one of the site's applications, database, and its operating system. A third location granted a user privileged access on the operating system without proper management approvals. At the fourth site, we found that system administrators maintained inappropriate privileges that enabled them to view records in one of the site's databases, including details of individual personnel security files.

- Weaknesses with separation of duties related to certain roles and responsibilities continued to be identified at three sites. For example, although one site had implemented a tool for provisioning, monitoring, and controlling service level accounts, additional work related to the site's separation of duties plan of action and milestones were still required to fully remediate the issue. Another site had not implemented separation of duties between personnel who administer the access control function and those who administer the audit trail. The absence of clear separation of duties in managing audit logs jeopardizes the ability to track and detect unauthorized access, alterations, or deletions of vital records.

- Five of the six sites reviewed during our FISMA metric work had not effectively developed and implemented processes for assigning position risk designations and performing appropriate personnel screening prior to granting access to its systems. For example, one site had not defined how personnel are assigned risk designations or the screening criteria. The site was also unable to provide evidence that personnel had been assigned appropriate risk designations, were appropriately screened prior to being granted system access, and periodically rescreened thereafter.

The identity and access management weaknesses occurred, in part, due to a lack of oversight over authentication management practices. For instance, at one site, the application used had system limitations that could not fully support all password complexity requirements. Although we were informed that the Authorizing Official was aware of the limitations, site officials were unable to provide support that the risk of vulnerability was formally accepted. At another site, weaknesses occurred because of inadequate configuration management and vulnerability management processes. The site's processes did not ensure that anonymous access and default credentials were changed prior to connecting the system to the production network and throughout the system lifecycle, and systems with anonymous access and default credentials on the production network were identified, monitored, and remediated.

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 and adequately respond to privacy-related breaches. Throughout our test work, we identified several weaknesses related to data protection and privacy programs implemented at Department sites. For instance:

- At one location, we identified weaknesses related to transmission confidentiality and integrity; protection of information at rest; and software, firmware, and information integrity. Specifically, a critical system had not always used secure ports, protocols, and services. We also found that the system had not encrypted its data at rest on servers. Further, the systems' administrators had not used automated tools to identify unauthorized changes in software, firmware, and information integrity.

- None of the FISMA metric sites reviewed had effectively implemented security controls to prevent data exfiltration and enhance network defenses. Rather, all the sites reviewed were rated at "consistently implemented" or below, with three sites rated at either a "defined" or ad-hoc" maturity level. For instance, two sites did not analyze qualitative and quantitative performance measures of their data exfiltration and enhanced network defenses. Additionally, three sites either had not implemented all required logging activities or had not defined their data exfiltration protections within formal policies and procedures.

- While our evaluation identified two sites that had effectively implemented security controls such as encryption of data at rest and in transit to protect PII and other agency sensitive data throughout the data lifecycle, we determined that four sites were not effective in this area. We found that three of the four sites lacked defined or implemented policies and procedures. One site also had not been routinely performing security control assessments and lacked assurance regarding whether security controls had been effectively implemented for protecting PII and other agency sensitive data.

- Although one site had effectively developed and implemented a Data Breach Response Plan, we found related weaknesses at the five remaining sites evaluated during our FISMA metric work. Three sites had weaknesses related to measuring the effectiveness of their response plans. Another site had not completed table-top exercises to make improvements to its response plan, nor was it able to provide evidence of system configurations to demonstrate how it would identify individuals affected by a breach, send notice, and provide those individuals with credit monitoring and repair services.

Two sites indicated that the data protection and privacy weaknesses described previously occurred, in part, due to resource constraints. Officials at one site mentioned that competing priorities hindered its ability to generate qualitative and quantitative metrics for its Data Breach Response Plan, while another site noted insufficient funding to implement all cybersecurity requirements. We also determined that one of the two sites lacked effective oversight of its cybersecurity program and had inadequate policies to ensure the confidentiality, integrity, and availability of its systems.

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. During our FY 2024 work, we identified several weaknesses related to the effectiveness of the Department's cybersecurity training and awareness. For example:

- Five locations had not ensured that specialized security training was provided to individuals with significant security responsibilities, as defined within the organization's policies and procedures. Specifically, three locations had only achieved the "defined" maturity level rating, and two locations had been rated at the "ad-hoc" maturity level. At one of the locations, privileged user training weaknesses were identified. Particularly, our test work identified that 13 of 25 sampled privileged users had not completed specialized training within the last year but still had enabled privileged user accounts.

- We determined that two locations had weaknesses related to ensuring that security awareness training was provided to all system users and that it was tailored based on the organizations' mission, risk environment, and types of information systems. At one of the locations, officials did not ensure all system users were provided security and awareness training prior to gaining system access. The same location also could not ensure that all system users had been provided and successfully completed security training on an annual basis. The other location had security awareness training program deficiencies that were associated with the organization not taking actions that would support the program's continuous improvement.

- Three locations assessed had been rated at a maturity level lower than "consistently implemented" when evaluated on whether they used an assessment of the skills, knowledge, and abilities of its workforce to provide tailored awareness and specialized security training within the five functional areas. At one location, for example, the organization disclosed that workforce assessments were only performed on an ad-hoc basis.

To the Department's credit, we determined that six locations reviewed had mandated that users take security awareness training related to identifying and reporting suspicious activities. We also found that five of the six locations had conducted phishing exercises against their user base during the time of our review.

The previously described weaknesses occurred for various reasons. For instance, although one location had active privileged users that were delinquent in their specialized privileged user training, the organization noted that the cybersecurity team did not have the authority to disable user accounts. As a result, the organization did not track or take actions against users that became delinquent in specialized training. At another location, the identified weaknesses occurred due to the organization not adequately monitoring information security and privacy training activities. In addition, we noted that issues related to role-based training occurred because the location's policy had not identified the appropriate individuals that should have been required to take privileged user training.

Without an adequate security awareness and training program, 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 2024, we identified various weaknesses related to the implementation of the Detect cybersecurity function.

Information Security Continuous Monitoring

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

- We identified audit logging weaknesses at three locations. We determined that one site had not implemented audit logging capabilities to log user activity and suspicious or unusual events within a certain financial application. While the other two sites had developed certain logging capabilities within the systems reviewed, one site had not documented the types of events that the system was capable of auditing. The other site's system audit logs did not capture enough data to determine whether system changes were authorized or what the change entailed.

- Three sites had weaknesses related to system security control assessment plans and/or the assessments performed on the systems reviewed. One of the sites had not adequately assessed all controls for an application reviewed and its operating environment because the site had not developed control assessment plans to support the assessment and monitoring activities. While another site had developed security control assessment plans for two systems evaluated, the plans were not approved by the Authorizing Official prior to conducting the assessments. We also found that the same site had only tested a small fraction of the required controls and control enhancements implemented for the two systems reviewed. For example, the site had only reviewed 18 percent of the controls and control enhancements implemented for one of the systems reviewed, although the system was classified as a Federal Information Processing Standard 199 "high" system. The third site had not performed a security control assessment on one of its systems since 2019.

- Eight sites did not effectively implement ongoing system authorizations. For instance, although required to support ongoing authorizations, we determined that three sites did not perform the required continuous monitoring activities to fully evaluate third-party providers' information technology environments for security changes or threats.

- Three sites reviewed had SSP deficiencies. While all three sites had developed SSPs for each of the systems reviewed, weaknesses were identified that related to the content within the SSPs. For example, an SSP at one site had not been updated since 2017 and, therefore, listed numerous outdated security control requirements.

- Our assessment of a system at one site concluded that the system was not reauthorized to operate on the required 3-year cycle. We determined that the system was last authorized to operate in 2014, and while the reauthorization process was initiated in FY 2017, it had not been completed, in part, due to a decision to retire the system. However, the system remained in operation with many weaknesses going unaddressed.

In addition to the deficiencies previously outlined, we assessed the Department at a "defined" maturity level for this function area based on our FISMA metric work. Although one of the six sites reviewed achieved an "optimized" maturity level for implementing effective processes for collecting and analyzing ISCM performance measures and reporting findings, we identified many ineffective ISCM related processes, policies, and/or strategies throughout our evaluation. For instance, we determined that all six sites evaluated did not effectively use policies and strategies that addressed ISCM requirements and activities. In one instance, while the site had developed an ISCM strategy, it had not been fully published and disseminated across the site to ensure consistent implementation. Additionally, all six sites had ineffective processes for performing one or more of the following continuous monitoring activities—ongoing information system assessments, granting system authorizations, developing and maintaining system security plans, and monitoring system security controls.

The weaknesses identified occurred, in part, because site policies and procedures were not fully developed and/or maintained to help facilitate the design and implementation of security controls at numerous sites. For example, at three sites, we determined that processes were not developed or implemented in accordance with guidelines established by NIST SP 800-37, Revision 2, related to managing security risks and continuous monitoring activities of systems. In addition, we noted that one site inherited the application under review from a Federal contractor. As a result, the site had not developed audit log policies for the application that included defined audit events; audit review, analysis, and reporting activities; and audit retention responsibilities and requirements.

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 relevant to response planning, communications, analysis, mitigation, and improvements. Throughout our test work, we identified weaknesses related to these cybersecurity control activities.

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 detection, analysis, handling, and information sharing. Our FISMA cybersecurity metric work and other OIG reviews performed throughout FY 2024 identified various weaknesses related to the Department's readiness and incident response capabilities. For instance, during our FISMA metric work, we determined that five of six sites reviewed did not effectively ensure that the incident response team's structures/models, stakeholders, roles and responsibilities, levels of authority, and dependencies were defined, communicated, and implemented across the organization. Similarly, we reported deficiencies during other OIG reviews that related to incident response training, testing, and exercises. Without effective design and implementation of incident response controls, members of the incident response team and stakeholders may not be able to maintain control of networks, systems, and applications, in accordance with security standards. In addition, improving user awareness regarding incidents through training should reduce the frequency of incidents.

To the Department's credit, we observed that certain processes related to incident response were effectively implemented at some sites evaluated. Specifically, three sites had achieved the "managed and measurable" maturity level for their use of an incident response plan. The same three sites also effectively implemented incident response information sharing activities and processes for incident handling. In addition, one site effectively implemented a process for incident detection and analysis. Another site achieved the "optimized" maturity level for its defined, communicated, and implemented incident response roles and responsibilities within the incident response team and organizational stakeholders.

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 2024, we identified deficiencies within 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. We noted during our FISMA metrics evaluation that several sites had achieved a "consistently implemented" maturity level rating for some of their system contingency planning processes. However, none of the sites reviewed had implemented processes necessary to achieve a "managed and measurable" maturity level or higher for any of the contingency planning FISMA metric questions evaluated in FY 2024. In fact, four of the six sites evaluated had multiple "ad-hoc" ratings within this domain. As a result, we assessed the Department at the "defined" maturity level for contingency planning. Additionally, our other OIG reviews reported similar results. For example, during one of our reviews, we evaluated one of the Department's high-value assets and determined that a system-level contingency plan had not been developed and tested. We also reported concerns related to the lack of an alternate storage site for the same system which is significant given the importance of the system to the Department's operations.

CYBERSECURITY REQUIREMENTS CHALLENGES

As noted in the OIG's Special Report, *Management Challenges at the Department of Energy — Fiscal Year 2025* (DOE-OIG-25-05, November 2024), cybersecurity is a critical aspect of the Department's overall security posture and one of the Department's highest risks. Cybersecurity attacks could lead to devastating consequences in the event of a cyber breach, including loss of life, property damage, and disruption of the essential services and critical functions upon which society relies. Despite these known challenges, the Department continued to fall behind in implementing the latest Federal cybersecurity requirements and enhancements.

This is illustrated, in part, by the Department's lack of progress in implementing NIST SP 800-53, Revision 5[2] requirements. Similar to the results reported in our prior year FISMA evaluation, we found that four of the six sites reviewed had not yet fully implemented the requirements of NIST SP 800-53, Revision 5. In particular, 82 of 101 systems at the 4 sites were still operating under the outdated NIST 800-53, Revision 4, *Security and Privacy Controls for*

[2] NIST SP 800-53, Revision 5, was published in September 2020; therefore, Revision 4 of the publication was withdrawn from use September 23, 2021. According to OMB Circular A-130, agencies are expected to meet the requirements of, and be in compliance with, NIST standards and guidelines within 1 year of their respective publication dates, unless otherwise directed by the OMB.

Federal Information Systems and Organizations. Of those 82 systems, at least 57 (70 percent) systems processed controlled unclassified information, including at least 46 systems that processed PII.

The sites that continued utilizing outdated requirements indicated various reasons for their noncompliance. For instance, officials expressed resource constraints, prioritization of other known weaknesses, and/or a commitment to other process improvements as reasons for noncompliance. Delayed implementation of Federal cybersecurity requirements, such as NIST 800-53, Revision 5, continues to leave the Department's data and information systems at risk to emerging threats and vulnerabilities.

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 risks underscore 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 for computer viruses and other malicious attacks. These attacks could have resulted in the attacker obtaining control and/or gaining 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.

Similar to our findings reported in previous years, we also continued to identify deficiencies related to developing, updating, and/or implementing policies and procedures. Without defined and effectively implemented governance structures, cybersecurity-related activities are at risk of not being effectively managed and monitored. For example, because of audit logging deficiencies that we identified in FY 2024, several Department sites were at an elevated risk for not detecting and responding promptly to unusual activity. Failure to detect such events could severely impact the Department's information and its systems by being exposed to activities that result in compromise, loss, modification, or non-availability.

During FY 2024, the Department informed the OIG of steps taken to strengthen its cybersecurity program. For instance, it developed the *Department's Cybersecurity Strategy* and updated its cybersecurity program requirements within Department Order 205.1D, *Department of Energy Cybersecurity Program*. The Department also updated its privacy program requirements within Department Order 206.1A, *Department of Energy Privacy Program*, which solidified privacy as a direct contributor to the Department's management of risk. According to the Department, both Department Orders establish requirements for protection of information and awareness training completion by both Federal employees and contractors. In addition, leadership engaged in promoting collaborations within the Department on activities and issues relating to cybersecurity. Further, the Department partnered with other Federal agencies to support key initiatives. For example, the officials participated in the Cybersecurity and Infrastructure Security Agency's Federal Attack Surface Testing program and Secure Cloud Business Applications project. The Department also made advancements related to cyber operations, such as launching the

Enterprise Cybersecurity Collaboration Office to improve compliance with FISMA and associated OMB-mandated metrics. These positive actions assisted the Department in prioritizing compliance with Executive Order 14028, expanding the implementation of security and privacy controls, and adoption of zero trust architecture principles across the enterprise to meet security goals and requirements outlined in OMB Memorandum M-22-09, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*. The Department also indicated that multifactor authentication, encryption, endpoint detection and response, and logging activities will continue to be a focus until compliance is achieved.

Recommendations

To address the identified cybersecurity program weaknesses throughout the Department, we made 79 new recommendations[3] in FY 2024. In addition, 44 prior year recommendations remained open. Specific recommendations were made to the Department's programs and sites where weaknesses were identified, including those identified during this evaluation and in other reports issued. During FY 2024, the Department took corrective actions and was able to close 3 newly issued recommendations; therefore, at the end of FY 2024, 120 cybersecurity recommendations remained open and required the attention of Department officials. Corrective actions to address each of the recommendations, if fully implemented, should enhance the Department's unclassified cybersecurity program.

Although management at the sites and programs reviewed concurred with most of our findings, management at two sites did not concur with four of our recommendations. However, our testing results supported their issuance, and therefore, all issued findings and recommendations will remain open until the described weaknesses have been addressed.

Management Comments

Management concurred with 75 of 79 new recommendations issued in FY 2024 to the programs and sites related to improving the Department's cybersecurity program. However, management nonconcurred with four recommendations and noted that two of the four were recently closed. 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 the 63 cybersecurity program weaknesses previously noted by the OIG, closing out 19. Management's comments are included in Appendix 5.

Office of Inspector General Response

Management's comments and planned corrective actions were responsive to recommendations made during our evaluation. Due to the timing of our test work, we did not validate any noted corrective actions. In addition, and in relation to the four recommendations that management

[3] The total number of new recommendations made during the FY includes those that were issued throughout the FY 2024 FISMA evaluation and those that were issued as a result of other OIG reports, as identified in Appendix 3.

nonconcurred with, we continue to note that our testing results in FY 2024 supported all recommendations issued. Further, we modified certain language in the report to ensure that it was not Controlled Unclassified Information.

Recommendations by Domain Category

The following table summarizes the recommendations made, including those that resulted from our fiscal year (FY) 2024 Federal Information Security Modernization Act of 2014 evaluation, other Office of Inspector General reports issued in FY 2024, and prior year recommendations that remain open. In FY 2024, 123[4] recommendations were made to the Department, nearly double the number issued in FY 2023. These recommendations are categorized by security domain to align with the *National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity* (Version 1.1).

Security Domain Category	FY 2024	FY 2023	FY 2022
Risk Management	30	24	10
Supply Chain Risk Management	0	0	0
Configuration Management	38	23	29
Identity and Access Management	22	8	22
Data Protection and Privacy	2	0	2
Security Training	5	2	1
Information Security Continuous Monitoring	18	3	3
Incident Response	1	0	0
Contingency Planning	6	0	0
Other Recommendations – Uncategorized[5]	1	5	6

[4] In FY 2024, three newly issued recommendations were closed. Therefore, 120 recommendations remained open as of the end of FY 2024.

[5] 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 2024 Metric Results[6]

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:

1. Ad-hoc
2. Defined
3. Consistently implemented
4. Managed and measurable
5. Optimized

Within the context of the maturity model, the Office of Management and Budget asserted that achieving a Level 4, 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	1	4	3
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?	1	3	2	3	4	2
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?	1	2	4	1	4	2

[6] 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 Memorandum M-24-04, *Fiscal Year 2024 Guidance on Federal Information Security and Privacy Management Requirements*, and the *Fiscal Year 2023 – 2024 Inspector General FISMA Metrics*. Due to the sensitivity of the information, we did not include site names.

To what extent has the organization categorized and communicated the importance/priority of information systems in enabling its missions and business functions, including for high value assets?	5	3	4	2	3	2
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?	5	4	4	3	2	3
To what extent does the organization use an information security architecture to provide a disciplined and structured methodology for managing risk, including risk from the organization's supply chain?	5	1	3	3	2	3
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?	5	3	3	2	2	2
Identify – Supply Chain Risk Management						
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?	5	4	1	1	4	1
To what extent does the organization ensure that counterfeit components are detected and prevented from entering the organization's systems?	1	1	3	3	2	3
Protect – Configuration Management						
To what extent have the roles and responsibilities of configuration management stakeholders been defined, communicated, and implemented across the agency, and appropriately resourced?	4	2	2	2	3	3
To what extent does the organization use an enterprise wide configuration management plan that includes, at a minimum, the following components: roles and responsibilities, including establishment of a Change Control Board or related body; configuration management processes, including processes for identifying and managing configuration items during the appropriate phase within an organization's system development life cycle; configuration monitoring;	3	3	3	2	2	3

and applying configuration management requirements to contractor-operated systems?	🟨	🟨	🟨	🟥	🟥	🟨
To what extent does the organization use configuration settings/common secure configurations for its information systems?	3	2	4	1	4	2
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	2	3	2
To what extent has the organization defined and implemented configuration change control activities including: determination of the types of changes that are configuration controlled; review and approval/disapproval of proposed changes with explicit consideration of security impacts and security classification of the system; documentation of configuration change decisions; implementation of approved configuration changes; retaining records of implemented changes; auditing and review of configuration changes; and coordination and oversight of changes by the Change Control Board, as appropriate?	3	3	2	1	3	3
Protect – Identity and Access Management						
To what extent has the organization developed and implemented processes for assigning position risk designations and performing appropriate personnel screening prior to granting access to its systems?	2	4	3	1	3	2
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?	2	3	4	4	4	4
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	2	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
Protect – Data Protection and Privacy						
To what extent has the organization developed and implemented a Data Breach Response Plan, as appropriate, to respond to privacy events?	3	3	1	2	4	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	1	4	2	2	3	4
To what extent has the organization implemented security controls (e.g., endpoint detection and response) to prevent data exfiltration and enhance network defenses?	1	2	3	1	3	3
To what extent does the organization ensure that privacy awareness training is provided to all individuals, including role-based privacy training?	1	2	1	1	3	4
Protect – Security Training						
To what extent does the organization ensure that specialized security training is provided to individuals with significant security responsibilities (as defined in the organization's security policies and procedures and in accordance with 5 Code of Federal Regulation 930.301)?	1	2	2	1	2	4
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	2	1	4	3	2

To what extent does the organization ensure that security awareness training is provided to all system users and is tailored based on its mission, risk environment, and types of information systems? (Note: awareness training topics should include, as appropriate consideration of organizational policies, roles and responsibilities, secure email, browsing, and remote access practices, mobile device security, secure use of social media, phishing, malware, physical security, and security incident reporting.)	3	2	3	1	3	5
Detect – Information Security Continuous Monitoring (ISCM)						
To what extent does the organization use ISCM policies and an ISCM strategy that addresses ISCM requirements and activities at each organizational tier?	3	3	2	2	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	3	3	3	2	2
How mature is the organization's process for collecting and analyzing ISCM performance measures and reporting findings?	5	3	3	1	3	3
Respond – Incident Response						
To what extent does the organization use an incident response plan to provide a formal, focused, and coordinated approach to responding to incidents?	4	2	2	3	4	4
To what extent have incident response team structures/models, stakeholders, and their roles, responsibilities, levels of authority, and dependencies been defined, communicated, and implemented across the organization?	3	2	2	5	3	3
How mature are the organization's processes for incident detection and analysis?	3	2	3	2	3	4
How mature are the organization's processes for incident handling?	4	3	3	1	4	4
To what extent does the organization ensure that incident response information is shared with individuals with significant security responsibilities and reported to external stakeholders in a timely manner?	4	3	3	3	5	4

Recover – Contingency Planning						
To what extent does the organization ensure that the results of business impact analyses are used to guide contingency planning efforts?	**1**	**1**	**3**	**1**	**2**	**1**
To what extent does the organization ensure that information system contingency plans are developed, maintained, and integrated with other continuity plans?	**3**	**1**	**3**	**1**	**2**	**1**
To what extent does the organization perform tests/exercises of its information system contingency planning processes?	**3**	**2**	**2**	**1**	**3**	**1**
To what extent does the organization perform information system backup and storage, including use of alternate storage and processing sites, as appropriate?	**1**	**1**	**3**	**3**	**2**	**3**

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.

Scope

We conducted the evaluation from January 2024 through May 2025 at 29 Department locations primarily under the purview of the Administrator for the National Nuclear Security Administration, Under Secretary for Science and Innovation, Under Secretary for Infrastructure, the Office of Environmental Management, the Office of the Chief Information Officer, the Office of the Chief Financial Officer, and certain staff offices. Of the 29 locations reviewed, 6 were selected 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 and business process application controls for information system work required in support of the audit of *The Department of Energy's Fiscal Year 2024 Consolidated Financial Statements*. In addition, our evaluation involved vulnerability assessment testing on information systems. 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, such as the audit report, *Bonneville Power Administration Needs to Improve Cybersecurity Over Selected Transmission Infrastructure Systems*; the audit report, *The Department of Energy's Ransomware Countermeasures and Response*; and the inspection report, *Cybersecurity Over the Clearance Action Tracking System*. This evaluation was conducted under OIG project number A24TG003.

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.

- 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 reviewing the work of the OIG's contract auditor. The metric reviews were conducted at six locations across various Department programs/elements and performed in accordance with Office of Management and Budget Memorandum M-24-04, *Fiscal Year 2024 Guidance on Federal Information Security and Privacy Management Requirements,* the *FY 2023-2024 Inspectors General FISMA Reporting Metrics,* and the *FY 2024 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.

Our work included analysis and testing of general and application controls for systems, as well as internal and external vulnerability testing of networks, systems, and workstations. To assess the work of OIG contract auditor, 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 July 17, 2025.

Related Reports

Office of Inspector General

- Special Report: *Management Challenges at the Department of Energy – Fiscal Year 2025* (DOE-OIG-25-05, November 2024). Cybersecurity remains a critical aspect of the Department of Energy's overall security posture and is one of the Department's highest risks. While the Department made several cybersecurity-related improvements, we continued to identify numerous weaknesses in cybersecurity within the Department. For instance, the Department continues to encounter challenges implementing Federal mandates, addressing evolving threats, and mitigating shortages in the cyber workforce. Further, the Department's existing governance structure impacts its ability to respond to cybersecurity evolving risks and mandates. In response to these challenges, we reported its initiation of reviews or previously reported results that could substantially benefit the Department. For example, we are in the process of determining whether the Department implemented an effective governance process over information technology and cybersecurity management.

- Evaluation Report: *The Department of Energy's Unclassified Cybersecurity Program – 2023* (DOE-OIG-24-17, May 2024). The Department, including the National Nuclear Security Administration (NNSA), 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. 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.

- Special Report: *Management Challenges at the Department of Energy – Fiscal Year 2024* (DOE-OIG-24-05, November 2023). The Department 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: *The Department of Energy's Unclassified Cybersecurity Program – 2022* (DOE-OIG-23-20, May 2023). The Department, including NNSA, 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: *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 were 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: *The Department of Energy's Unclassified Cybersecurity Program – 2021* (DOE-OIG-22-33, June 2022). The Department, including NNSA, 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.

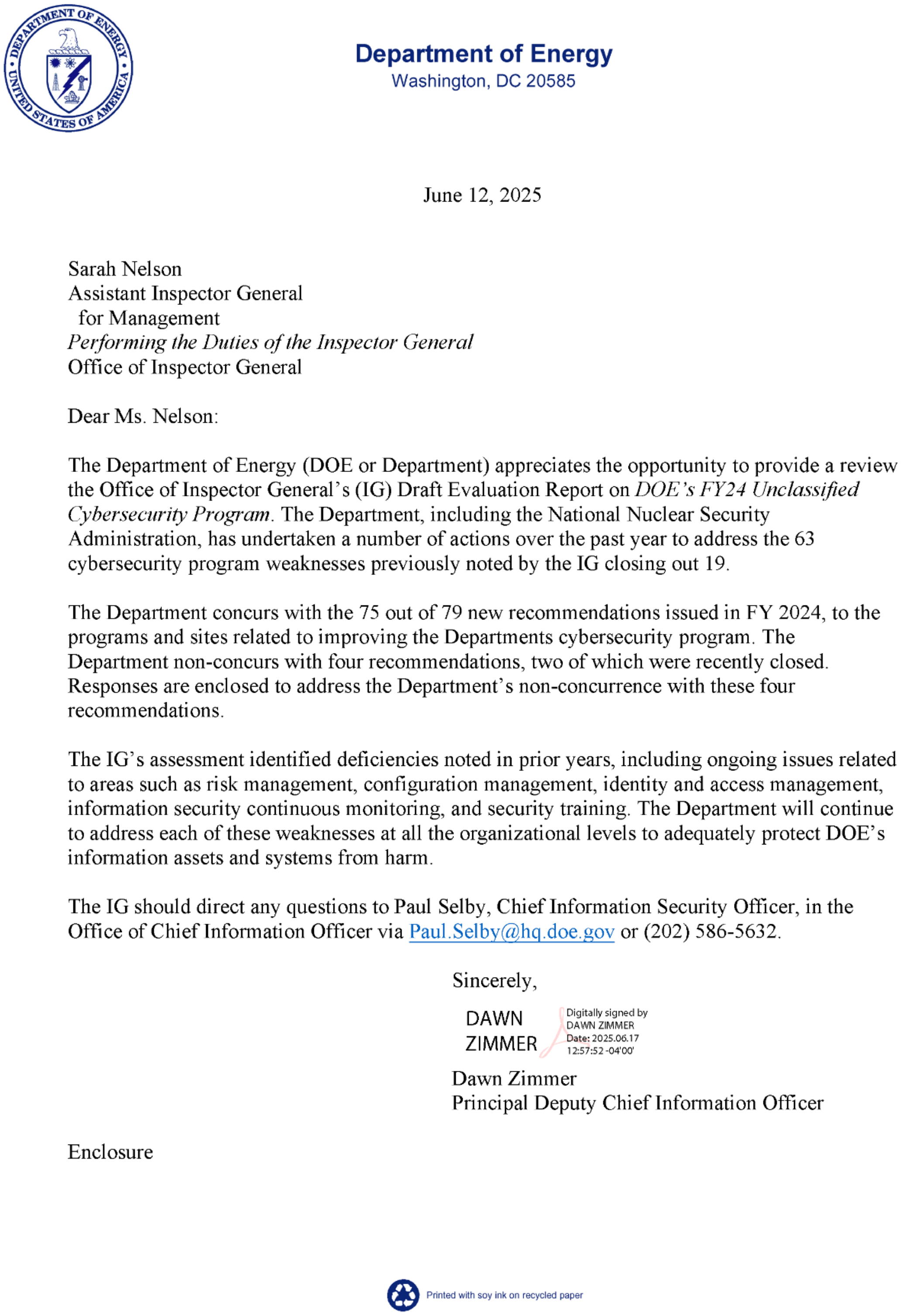
Government Accountability Office

- *Priority Open Recommendations: Department of Energy* (GAO-24-107308, June 2024). The Government Accountability Office (GAO) issued a letter in fiscal year 2024 to provide an update on the overall status of the Department of Energy's implementation of the agency's recommendations and areas where open recommendations should be given high priority. Particularly, as of June 2024, the Department had 203 open recommendations that if fully implemented could significantly improve the agency's operations. Of those open recommendations, 27 were identified as being priority, including 5 that would improve the Department's, including NNSA's, efforts to manage cybersecurity risks. In addition, the GAO recommended that NNSA identify the needed resources to implement foundational cybersecurity practices for the operational technology environment and clarify to management and operating contractors that they are required to monitor subcontractor's cybersecurity measures.

- *CRITICAL INFRASTRUCTURE PROTECTION: Agencies Need to Enhance Oversight of Ransomware Practices and Assess Federal Support* (GAO-24-106221, January 2024). In fiscal year 2024, the GAO issued a report that, in part, identified that the Department had not determined the extent of adoption of the National Institute of Standards and Technology's recommended practices for addressing ransomware. In addition, the GAO reported that the Department did not demonstrate efforts to evaluate the effectiveness of Federal support in helping reduce the risk of ransomware to the energy sector.

Appendix 5

Management Comments



Department of Energy
Washington, DC 20585

June 12, 2025

Sarah Nelson
Assistant Inspector General
for Management
Performing the Duties of the Inspector General
Office of Inspector General

Dear Ms. Nelson:

The Department of Energy (DOE or Department) appreciates the opportunity to provide a review the Office of Inspector General's (IG) Draft Evaluation Report on *DOE's FY24 Unclassified Cybersecurity Program*. The Department, including the National Nuclear Security Administration, has undertaken a number of actions over the past year to address the 63 cybersecurity program weaknesses previously noted by the IG closing out 19.

The Department concurs with the 75 out of 79 new recommendations issued in FY 2024, to the programs and sites related to improving the Departments cybersecurity program. The Department non-concurs with four recommendations, two of which were recently closed. Responses are enclosed to address the Department's non-concurrence with these four recommendations.

The IG's assessment identified deficiencies noted in prior years, including ongoing issues related to areas such as risk management, configuration management, identity and access management, information security continuous monitoring, and security training. 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.

The IG should direct any questions to Paul Selby, Chief Information Security Officer, in the Office of Chief Information Officer via Paul.Selby@hq.doe.gov or (202) 586-5632.

Sincerely,

DAWN
ZIMMER

Digitally signed by
DAWN ZIMMER
Date: 2025.06.17
12:57:52 -04'00'

Dawn Zimmer
Principal Deputy Chief Information Officer

Enclosure

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.

If you have comments, suggestions, and feedback on this report, please reach out at OIG.Reports@hq.doe.gov. Include your name, contact information, and the report number.

For all media-related questions, please send inquiries to OIGpublicaffairs@hq.doe.gov and include your name, contact information, and the report number.