



U.S. DEPARTMENT OF ENERGY

Office of Inspector General

DOE-OIG-27-02

October 8, 2026

Additional Effort Is Needed to Improve the Department of Energy's Unclassified Cybersecurity Program – 2025



EVALUATION REPORT



Department of Energy
Washington, DC 20585

October 8, 2026

MEMORANDUM FOR THE SECRETARY

SUBJECT: Evaluation Report: *Additional Effort Is Needed to Improve the Department of Energy's Unclassified Cybersecurity Program – 2025*

The attached report discusses the results of our fiscal year 2025 *Federal Information Security Modernization Act of 2014* evaluation and summarizes cybersecurity related findings from another Office of Inspector General audit performed for fiscal year 2025. Our work 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. While in many cases programs and sites had taken corrective actions, there were two sites that either consolidated and/or decommissioned their systems, resulting in the closure of outstanding recommendations.

Although management at the sites and programs reviewed concurred with most of our findings, management at two locations nonconcurred with nine of our recommendations. However, our testing results supported the issuance of the findings and recommendations; therefore, all issued findings and recommendations will remain open until the described weaknesses have been addressed.

While this report summarizes findings from this evaluation, which included following up on findings from prior year Office of Inspector General reports and another audit performed for fiscal year 2025, it does not address the status of corrective actions that may have occurred since the findings 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 weaknesses and 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.

A handwritten signature in blue ink, reading "Sarah Nelson", is positioned above the typed name.

Sarah Nelson
Senior Official
Performing the Duties of the Inspector General
Office of Inspector General

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

DOE OIG HIGHLIGHTS

Additional Effort Is Needed to Improve the Department of Energy's Unclassified Cybersecurity Program – 2025

Why We Performed This Evaluation

The *Federal Information Security Modernization Act of 2014* requires 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.

The *Federal Information Security Modernization Act of 2014* mandates 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.

What We Found

Our fiscal year 2025 *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 57 of 120 (48 percent) cybersecurity recommendations from our prior year reviews. However, we determined that 63 recommendations remained open, of which 29 had not been fully addressed for more than 2 years. We also issued 55 new recommendations. Of the 55, 41 were made to address a significant access control deficiency over various financial systems within the Department. This significant deficiency was an audit result described within our report, *The Department of Energy's Fiscal Year 2025 Consolidated Financial Statements* (DOE-OIG-26-03, December 2025).

The weaknesses occurred for a variety of reasons. For instance, deficiencies related to access controls occurred, in part, due to management not responding to changes in risks or identifying risks associated with inappropriate or unnecessary access to systems.

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 unauthorized modification.

What We Recommend

If fully implemented, the 118 recommendations that remain open 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 and one of its highest risks, the Department should take action to implement the latest Federal cybersecurity requirements to ensure adequate protection of the Department's data and information systems.

Table of Contents

Background and Objective	1
Results of Review	3
Additional Effort Is Needed to Improve the Department's Unclassified Cybersecurity Program.....	3
Govern	4
Identify	5
Protect	7
Detect	11
Respond	12
Recover	14
Cybersecurity Requirements Challenges	14
Risks to Information and Systems	15
Recommendations	16
Management Comments and OIG Response	17
Appendices	
1. Recommendations by Domain Category	18
2. <i>Federal Information Security Modernization Act of 2014</i> Fiscal Year 2025 Metrics Results.....	19
3. Objective, Scope, and Methodology	24
4. Related Reports.....	27
5. Management Comments.....	30

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 6 cybersecurity functions and 10 security domains that are aligned with the *National Institute of Standards and Technology* (NIST) *Cybersecurity Framework* (CSF) 2.0.

Table 1: Cybersecurity Functions and Domains

Cybersecurity Functions		Security Domains
Govern	The organization’s cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored.	Cybersecurity Governance
		Cybersecurity Supply Chain Risk Management (C-SCRM)
Identify	The organization’s current cybersecurity risks are understood.	Risk and Asset Management
Protect	Safeguards to manage the organization's cybersecurity risks are used.	Configuration Management
		Identity and Access Management
		Data Protection and Privacy
		Security Training
Detect	Possible cybersecurity attacks and compromises are found and analyzed.	Information Security Continuous Monitoring (ISCM)
Respond	Actions regarding a detected cybersecurity incident are taken.	Incident Response
Recover	Assets and operations affected by a cybersecurity incident are restored.	Contingency Planning

Source: NIST CSF 2.0 and *Fiscal Year (FY) 2025 Inspector General FISMA Reporting Metrics, Version 2.0* (IG FISMA Reporting Metrics).

Inspectors General (IGs) 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: IG 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 2025 IG 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. The FY 2025 IG FISMA Reporting Metrics represent a continuation of the multi-year reporting cycle, established in FY 2022. Specifically, a set of core metrics¹ are to be evaluated annually, and the remaining supplemental metrics² are evaluated on a 2-year cycle. For the FY 2025 reporting cycle, our review included an evaluation of 20 core metrics and 5 supplemental metrics.

Additionally, as illustrated in Table 1, the FY 2025 IG FISMA Reporting Metrics were updated to align with NIST CSF 2.0. As such, a new FISMA function (Govern) had been created that included a new domain (Cybersecurity Governance). Also, the Supply Chain Risk Management (C-SCRM) domain moved from the Identify function to the Govern function and was renamed to C-SCRM to better reflect the cybersecurity environment. Further, the Risk Management domain in the Identify function was renamed to Risk and Asset Management.

IGs were also encouraged to evaluate the metrics based on the risk tolerance and threat models of their respective agencies and to focus on the practical security impact of weak control implementations, rather than just evaluating from a compliance standpoint or mere presence or absence of controls. Therefore, in FY 2025, IGs were instructed to consider other data points such as:

- The results of cybersecurity audits, inspections, and evaluations conducted during the review period, to include any system security control reviews, vulnerability scanning, or

¹ Core metrics represent a combination of Administration priorities, high-impact security processes, and essential functions necessary to determine security program effectiveness.

² Supplemental metrics are not considered a core metric but represent important activities conducted by security programs and contribute to the overall evaluation and determination of security program effectiveness. For FY 2025, the supplemental metrics were designed to gauge the maturity of agencies' cybersecurity governance practices and implementation of key components of Zero Trust Architecture.

penetration testing;

- The progress made by agencies in addressing outstanding IG recommendations; and
- Security incidents reported during the review period.

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 Office of the Chief Information Officer, the Office of the Chief Financial Officer, the Office of Environmental Management, the Office of the Under Secretary for Nuclear Security and National Nuclear Security Administration, the Office of the Under Secretary for Science and Innovation,³ the Office of the Under Secretary of Infrastructure,⁴ 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 2025.

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

ADDITIONAL EFFORT IS NEEDED TO IMPROVE THE DEPARTMENT'S UNCLASSIFIED CYBERSECURITY PROGRAM

Our FY 2025 evaluation determined that the Department had taken actions to address some of the previously identified weaknesses. Specifically, while two sites either consolidated and/or decommissioned their systems, other Department programs and sites had taken corrective actions related to areas such as configuration management, contingency planning, identity and access management, incident response, information security continuous monitoring, risk and asset management, and security training. This resulted in the closure of 57 of 120 (48 percent) recommendations made during prior year audits and evaluations. However, 63 prior year recommendations remained open related to weaknesses in areas such as risk and asset management, configuration management, identity and access management, data protection and privacy, security training, ISCM, and contingency planning. Of the 63 prior year recommendations, we determined that 29 had remained open for more than 2 years. Notably, the OIG agreed not to perform follow-up vulnerability assessment test work on certain open prior year findings at seven sites. The OIG agreed to these conditions due to site officials indicating that corrective actions had not been fully implemented at the time of our test work.

³ As of November 2025, the Office of the Under Secretary for Science and Innovation has been renamed the Office of the Under Secretary for Science.

⁴ As of November 2025, the Office of the Under Secretary for Infrastructure has been renamed the Office of the Under Secretary of Energy. Additionally, the Office of Energy Efficiency and Renewable Energy, which had formerly aligned under the Office of the Under Secretary for Science and Innovation, is now under the purview of the Office of Critical Minerals and Energy Innovation.

Consequently, the findings remained open at these seven sites. Additionally, two other in-scope sites had requested that FY 2025 vulnerability assessment test work be postponed, due to various resource constraints. However, the OIG completed FISMA metric testing for those two sites as planned.

In addition to the prior year recommendations that remained open, we issued 55 new recommendations throughout FY 2025, 41 of which were made to address a significant access control deficiency over various financial systems within the Department. This significant deficiency was an audit result described within our report, *The Department of Energy's Fiscal Year 2025 Consolidated Financial Statements* (DOE-OIG-26-03, December 2025). As a result, 118 recommendations had yet to be fully addressed at the end of the FY.

The combined efforts of our FY 2025 FISMA evaluation, which included following up on findings from prior year OIG reports and *The Department of Energy's Fiscal Year 2025 Consolidated Financial Statements*, identified weaknesses within all six of the NIST CSF 2.0 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.

GOVERN

The Govern cybersecurity function requires that the Department's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored. It includes two information security domains, Cybersecurity Governance and C-SCRM. The Govern cybersecurity function relates to several cybersecurity controls found in NIST Special Publication (SP) 800-53, Revision 5, "Security and Privacy Controls for Information Systems and Organizations," including those that support program management. During our FY 2025 evaluation, we concluded that the Department had not always fully implemented security controls and associated processes related to the Govern cybersecurity function.

Cybersecurity Governance

The Cybersecurity Governance domain focuses on the Department's progress related to organizational context; risk management strategy; roles, responsibilities, and authorities; policy; and oversight. In FY 2025, we evaluated the Department's progress in establishing cybersecurity governance throughout our review of the FISMA metrics. Our results identified related weaknesses at all six sites evaluated during our FISMA metric work. For instance:

- None of the FISMA metric sites reviewed had effectively developed and maintained cybersecurity profiles that were used to understand, tailor, assess, prioritize, and communicate cybersecurity objectives. Specifically, five sites had not fully defined and implemented processes to develop and maintain cybersecurity profiles. With respect to the remaining site, it had developed and maintained current and target profiles requirements, performed gap analyses, and developed a high-level project plan. However, at the time of our review, the site had not implemented any of these efforts.

- While one site reviewed had effectively used a cybersecurity risk management strategy to support operational risk decisions, we determined that the remaining five sites were not effective in this area. Particularly, we found that three sites had not developed a risk management strategy that included all of the required components. Although one of the three locations had developed risk management procedures and processes, it had not developed a strategy that fully aligned with NIST requirements. Additionally, two sites had not collected or evaluated qualitative and quantitative measures to aid in the improvement of their implemented cybersecurity risk management strategies.
- All six sites had not effectively established cybersecurity roles, responsibilities, and authorities that fostered accountability, performance assessments, and continuous improvement. Although four had consistently implemented related processes, two had weaknesses with existing policies and procedures. For example, one of the sites had not demonstrated consistent completion of performance plans for individuals with significant cybersecurity duties.

A few sites assessed indicated that some of the weaknesses identified occurred, in part, because they had not aligned policies and processes to the NIST CSF 2.0 requirements, published in February 2024. For instance, three sites thought that NIST CSF 2.0 did not apply to them for various reasons and, therefore, they had not defined and implemented processes to develop and maintain target profiles. Without strong oversight, sites face increased security control failures due to ineffective risk management roles, policies and practices, and allocation of resources.

Cybersecurity Supply Chain Risk Management

The C-SCRM domain evaluates systematic processes for managing exposure to cybersecurity risk throughout supply chains and developing appropriate response strategies, policies, processes, and procedures. To the Department's credit, four of six FISMA metric sites assessed in FY 2025 had achieved the "Optimized" maturity level by analyzing, in a near-real time basis, the impact of material changes to C-SCRM assurance requirements on their relationships with external providers and ensuring that acquisition tools, methods, and processes were updated as soon as possible. However, the remaining two sites had not effectively ensured that products, system components, systems, and services of external providers were consistent with the organization's cybersecurity and supply chain requirements. Specifically, one site had not fully implemented site-specific performance measures related to reporting and monitoring activities for C-SCRM. The other site had not implemented qualitative and quantitative measures over the C-SCRM program.

IDENTIFY

The Identify cybersecurity function requires that the Department's current cybersecurity risks are understood, such as assets (e.g., data, hardware, software, systems, facilities, services, and people), suppliers, and other related cybersecurity risks. Additionally, it includes the identification of improvement opportunities for the organization's policies, plans, processes, procedures, and practices that support cybersecurity risk management. As such, the Identify function has one information security domain—Risk and Asset Management. The Identify cybersecurity function relates to several cybersecurity controls found in NIST SP 800-53,

Revision 5, including those that support risk assessments, asset inventories, and asset usages. During our FY 2025 evaluation, we concluded that the Department had not remediated many prior year weaknesses that related to risk and asset management, which included some that had not been fully addressed for over 2 years. Furthermore, our evaluation identified additional weaknesses within the Identify function.

Risk and Asset Management

The Risk and Asset Management domain focuses on the Department's progress as it relates to asset management, risk assessment, and improvement capabilities. The Department had taken corrective actions to close five recommendations identified in prior year reports that related to risk and asset management. However, based on our FY 2025 evaluation results, it continues to have challenges closing open recommendations under this domain. Specifically, we identified 23 recommendations associated with findings from prior year reviews that had not been fully remediated and, therefore, had remained open. Of the 23 recommendations that remained open, we determined that 13 had been open for more than 2 years. Furthermore, our FY 2025 FISMA metric work also identified risk and asset management weaknesses at the six sites reviewed. For instance:

- All six sites evaluated had not effectively developed or maintained asset inventories. The weaknesses varied depending on whether the reviewed inventory focused on information systems, hardware, software, or data assets. For instance, none of the FISMA metric sites reviewed had designed or implemented defined policies, procedures, processes, and roles and responsibilities for developing and maintaining a comprehensive and accurate inventory of their data and corresponding metadata. Additionally, while all six sites had used standard data elements/taxonomy to develop and maintain an up-to-date inventory of hardware assets, none of the sites were able to achieve the "Consistently Implemented" maturity level, for various reasons. For example, two sites had established processes for reviewing and updating their hardware asset inventory; however, neither site had maintained evidence of the reviews. Another site had established a hardware inventory but had not defined policies of maintaining and reviewing the established inventory on a set frequency to ensure the inventory was complete and accurate.
- While one site had consistently implemented a process that ensured information system security risks were adequately managed, the remaining sites had weaknesses that related to defining and/or implementing related policies and procedures. Three sites developed related policies, procedures, and processes; however, two of the three sites had deficiencies that affected the implementation of their risk registers, and all three had differing risk assessments weaknesses. Specifically, one site had not documented a risk assessment for the system that we selected to be reviewed. In addition, the second site had not periodically updated its risk assessment to prioritize threats and vulnerabilities or provide an overall assessment of risk to facilitate security control implementation to mitigate risks. Finally, the third location had not updated its risk assessment since 2018 and continues to conduct risk assessments based on the outdated requirements in NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems*

and Organizations, despite Revision 5 being issued in September 2020. The other two locations reviewed had not fully developed or received approval for related draft policies and procedures.

- None of the FISMA metric sites reviewed had effectively used technology/automation to provide a centralized, enterprise-wide (portfolio) view of cybersecurity risk management activities across the organization. Although two locations had not fully implemented an automated enterprise-wide solution, and one had not fully integrated all necessary sources of cybersecurity risk information within its established solution, all three sites had established plans for the implementation of their solutions. The remaining three sites did not have plans to utilize an automated solution to view cybersecurity risks.

The weaknesses related to risk and asset management occurred for several reasons. For example, three locations had not allocated resources to develop and implement inventories for their data and corresponding metadata. Site officials at all three locations noted that they believed the requirements set within NIST CSF 2.0 did not apply to them because they were not under contractual obligation to comply with NIST CSF 2.0 at the time of the assessment. Another location was delayed in receiving funding to implement tools to support its data management system. Without maintaining a comprehensive and accurate inventory of data and metadata, the risk of data mismanagement is elevated, which can lead to loss, inaccuracies, and security vulnerabilities that may result in unauthorized access to protected or sensitive data.

PROTECT

The Protect cybersecurity function requires the Department to implement safeguards to manage the organization's cybersecurity risks. It supports the ability for organizations to secure assets from adverse cybersecurity events by preventing or lowering the likelihood and impact of such events. Therefore, 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. Our FY 2025 evaluation concluded that the Department had not remediated 30 prior year weaknesses within the Protect function, which included some that had not been fully addressed for over 2 years. Additionally, our evaluation continued to identify weaknesses within all the security domains included in this cybersecurity function.

Configuration Management

The Configuration Management security domain focuses on the Department's progress related to areas such as use of secure configurations, vulnerability management, and flaw remediation activities. To its credit, the Department had taken actions to address and close 14 recommendations from prior year assessments that related to configuration management. In addition, two recommendations were closed due to a site's consolidation and the disposition of associated systems. Despite this success, the Department continues to have challenges closing open recommendations under this domain. Specifically, we identified 22 recommendations associated with findings from prior year reviews that had not been fully remediated and, therefore, had remained open. Of the 22 recommendations that remained open, we determined

that nine had been open for more than 2 years. Furthermore, our FY 2025 work continued to identify configuration management weaknesses across the Department. For example:

- We identified three locations that had firewall configuration management weaknesses. While one location had developed a firewall management procedure to configure, monitor, and maintain firewalls, our testing determined that corrective actions related to the review process of existing and new firewall rules had yet to be fully implemented. The other two locations had firewall rules that were unused, no longer necessary, or granted overly permissive or unnecessary access to the rule's destination group.
- Numerous devices had unsupported software and/or were not configured with the latest security patches across workstations, servers, and/or applications at three sites. For instance, at one site, we identified 833 critical- and high-risk vulnerabilities through credentialed and uncredentialed scanning across workstations, servers, and a system application. The two other sites where we performed prior year finding follow-up testing had taken some notable actions to assist in addressing these weaknesses; however, our results indicated that these weaknesses remained to be substantial. For example, at one of these locations, we identified 448 critical- and high-risk vulnerabilities related to missing updates and patches on 49 of 50 (98 percent) workstations tested.
- One program office did not require sites under its purview to prioritize remediation activities, in accordance with NIST requirements. Specifically, three locations did not have vulnerability and patch management remediation procedures that supported the NIST requirement to prioritize remediation activities based on the release date of the security relevant software and firmware updates. Rather, all three locations noted that the remediation time period began at the date of discovery, which follow the requirements set with the program office's cybersecurity program plan.
- One location had system integrity weaknesses related to used web applications. In particular, during our credentialed and uncredentialed scanning, we determined that vulnerabilities existed on two web applications that could be used to obtain unauthorized access to data and functionality. For instance, one of the web applications did not verify whether the user submitting a request for data or functionality was authorized to perform the requested action.
- None of the six sites evaluated during our FISMA metric work had effective flaw remediation processes. Four sites had weaknesses related to fully defining their vulnerability and patch management processes and/or the implementation of such policies and procedures. The two remaining sites had neither provided evidence of qualitative and quantitative performance measures on the effectiveness of their flaw remediation processes nor centrally managed their flaw remediation processes.
- Five of the six sites evaluated during our FISMA metric work had not effectively used configuration settings and/or common secure configurations for information systems. Four sites had weaknesses in either fully defining and/or implementing related policies and procedures. For instance, one site did not have a complete process implemented to

consistently maintain security configurations. The fifth site had not established related policies and procedures, established a process for performing baseline scanning, or established a process for managing and approving configuration baseline deviations or false positives.

The identified configuration management weaknesses occurred for various reasons. For instance, firewall rule weaknesses occurred because a process to periodically review the firewall rules and make the necessary changes, as appropriate, had not been fully implemented at any of the three sites reviewed. In other instances, vulnerabilities related to unsupported software and missing security updates had occurred because the reviewed sites did not have vulnerability and patch management processes that were operating effectively.

Without effective configuration management procedures and practices for systems in the production environment, unauthorized network access to key systems or denial of service could occur. Failure to remedy the underlying cause of the conditions previously noted could also result in additional, unnecessary network access and risk to systems, applications, components, and sensitive data.

Identity and Access Management

The Identity and Access Management domain ensures that organizations limit access to physical and logical assets by identifying and managing authorized users, services, and hardware. Notably, the Department had taken actions to address and close 10 of our recommendations issued in prior years that related to identity and access management. In addition, seven recommendations were closed due to a site's decommissioning of its systems. However, we identified four recommendations associated with findings from prior year reviews that had not been fully remediated and, therefore, had remained open. Of the four recommendations that remained open, we determined that three had been open for more than 2 years. Additionally, our FY 2025 test work continued to identify weaknesses within this domain. For instance:

- Seven locations reviewed during our audit, *The Department of Energy's Fiscal Year 2025 Consolidated Financial Statements*, had numerous access management deficiencies over various financial systems within the Department. For example, we determined that six of the sites had not fully implemented the principles of least privilege and separation of duties. In addition, six sites had varying access review deficiencies. Given the many deficiencies identified across various financial systems within the Department, a significant deficiency related to access controls was reported within *The Department of Energy's Fiscal Year 2025 Consolidated Financial Statements* (DOE-OIG-26-03, December 2025).
- While one of the six FISMA metric sites reviewed was determined to be effective at implementing phishing-resistant multifactor authentication (MFA) mechanisms for both privileged and non-privileged users, the remaining sites were determined to have various related weaknesses. To one site's credit, it had effectively implemented MFA mechanisms for non-privileged users. However, the same site did not implement MFA for privileged users across all endpoints. In another instance, a site was not fully tracking

MFA compliance for both privileged and non-privileged users and was also not able to provide authentication configuration settings to support how users access physical, network, and system assets.

- None of the six FISMA metric sites evaluated had effectively ensured that privileged accounts were provisioned, managed, and reviewed, in accordance with principles of least privilege. For example, four sites had weaknesses with either their defined or implemented privileged accounts management processes.

Many of the weaknesses related to identity and access management occurred because management had not consistently designed, implemented, or operated controls to ensure compliance with standards for effective internal control systems and internal policies. For instance, most of the deficiencies related to least privileged and separation of duties occurred, in part, because management had not fully assessed the risk associated with approving permissions that exceeded what was necessary for an individual's assigned role and responsibilities.

Without effective controls over account management processes, information systems and their data are at increased risk of becoming compromised. For instance, an unauthorized user could gain access to sensitive information and transactions, which could lead to unauthorized disclosure, modification, or destruction. This could also have a significant downstream impact on the reliability of data and disrupt normal business operations.

Data Protection and Privacy

The Data Protection and Privacy domain focuses on the extent to which agencies protect the confidentiality, integrity, and availability of information, such as personally identifiable information (PII) and other sensitive information. Based on our FY 2025 review results, we identified two recommendations associated with weaknesses described within a prior year review that had not been fully remediated and, therefore, had remained open. Also, our FY 2025 FISMA metric work continued to find data protection and privacy weaknesses at the six sites reviewed. For instance, we determined that all six sites had not effectively implemented security controls to protect the confidentiality, integrity, and availability of PII and other agency sensitive data, as appropriate, throughout the data lifecycle. For example, two of the sites were found to have data encryption-related deficiencies. Similarly, all six sites did not effectively implement security controls to prevent data exfiltration and enhance network defenses. While two sites had consistently implemented related security controls, they had weaknesses associated with qualitative and quantitative measures on the performance of their overall data protection and privacy strategy. The remaining sites had various deficiencies that related to the implementation of or development of defined policies and procedures regarding data exfiltration and network defenses.

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

Security Training

The Security Training domain aims to ensure that the Department has implemented an effective cybersecurity training and awareness program so that personnel can successfully perform cybersecurity-related tasks. While the Department had taken action to address and close three recommendations in FY 2025 that related to this domain, the Department continues to have challenges in this area. Specifically, we identified two recommendations associated with findings from prior reviews that had not been fully remediated. Both of these recommendations have remained open for more than 2 years. Additionally, our FY 2025 FISMA metric work continued to identify security training-related weaknesses. Specifically, all six sites reviewed did not effectively utilize an assessment of the skills, knowledge, and abilities of their workforce to provide specialized security training within all six cybersecurity functions. For instance, three sites did not assess and/or define processes for assessing the skills, knowledge, and abilities of their workforce. Although the three other sites had provided evidence that some action had been taken in this area, weaknesses persisted. For example, while we determined that one site performs workforce assessments, it did not assess its current workforce's skills and abilities for the site to provide specialized training. Rather, the assessment was performed to identify resource needs.

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 ensures that possible cybersecurity attacks and compromises are found and analyzed. This function enables the timely discovery and analysis of anomalies, indicators of compromise, and other potentially adverse events that may indicate that cybersecurity attacks and incidents are occurring. It also supports successful incident response and recovery activities. As such, the Detect function 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. During our FY 2025 evaluation, we concluded that the Department had not remediated several ISCM-related weaknesses that were identified in prior year reviews. Also, our evaluation identified additional weaknesses within the Detect function.

Information and Security Continuous Monitoring

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. Notably, the Department had taken action to address and close eight recommendations related to previously identified ISCM weaknesses. In addition, two recommendations were closed due to a site's decommissioning of its system. However, the Department continues to have challenges closing open recommendations under this domain. Specifically, we identified eight recommendations associated with findings from prior year reviews that had not been fully remediated and,

therefore, had remained open. Of the eight recommendations that remained open, we determined that two had been open for more than 2 years. Furthermore, our FY 2025 FISMA metric work continued to find ISCM weaknesses at the six sites reviewed. For instance:

- None of the six sites effectively used ISCM policies and strategies that addressed requirements and activities at each organizational tier. Specifically, while one site followed its enterprise cybersecurity program plan requirements, it had not developed and documented ISCM policies, nor had it established a minimum frequency for monitoring implemented controls. In addition, four sites had weaknesses in the development of their ISCM policies or the timing of their security controls assessments. The sixth site had not implemented quantitative and qualitative data collection and reporting to measure the effectiveness of its ISCM program.
- Three sites consistently implemented monitoring and measuring activities for the integrity and security posture of all owned and associated assets. However, while one site has implemented an automated inventory collection process, it continued to maintain a manual process to track cyber asset inventory. The two other sites either did not automate inventory collection, endpoint monitoring, and unauthorized device detection or did not have a defined process for performing manual reviews for non-automated technologies. Furthermore, the remaining three sites had weaknesses in the development, management, and implementation of their related defined processes.
- None of the six sites had effectively performed ongoing information system assessments to grant system authorizations. Specifically, we found that one site had not implemented automated analysis tools or manual expert analysis to assist with ongoing authorization. In addition, three sites had weaknesses related to the frequency in which security assessments were performed and documented. For example, at one location, a Security Assessment Report was last performed on a particular system and documented in 2018 while another location's 2020 Security Assessment Report was not fully completed or approved. Furthermore, while one site had documented continuous monitoring procedures and strategies, it did not implement ongoing security control assessments, system authorizations, and system security plan maintenance activities. The last site had not fully established authorization boundaries, implemented associated security controls, or fully documented and maintained related policies and procedures.

Without an effective ISCM program, it leaves the Department vulnerable to undetected cyberattacks and data breach risks. Without real-time visibility, security gaps remain open, and critical systems are exposed to evolving threats between periodic assessments.

RESPOND

The Respond cybersecurity function requires the Department to take actions regarding a detected cybersecurity incident and, therefore, includes one security domain—Incident Response. The Respond cybersecurity function relates to incident response cybersecurity controls found in NIST SP 800-53, Revision 5, including categories related to management, analysis, mitigation,

and reporting of incidents. During our FY 2025 evaluation, we concluded that the Department, generally, had less weaknesses in this function than others; however, improvements could still be made.

Incident Response

The Incident Response domain puts an emphasis on activities that support incident detection, analysis, handling, and reporting. Although the Department had taken action to address and close one related recommendation from a previous OIG review, our FY 2025 FISMA metric work continued to identify weaknesses within this domain. For instance:

- All six sites reviewed did not effectively implement processes related to incident handling. While three sites had consistently implemented related processes, none had implemented quantitative and/or qualitative performance measures over the effectiveness of its incident handling policies and procedures. Two other sites had developed formal incident handling policies and procedures; however, both sites had deficiencies that involved defining- and/or implementing-related strategies. For example, one of the two sites had developed a containment strategy, but it did not include the effectiveness of the strategy or the duration of the solution for the strategy. The final site had not fully designed or implemented policies, procedures, and processes for incident handling. While the location provided a policy that relayed some incident response activities (e.g., incident investigation procedures), impact classifications, and roles and responsibilities, the site was unable to provide evidence to support developed containment strategies for various types of major incidents, eradication processes, and processes for recovery system operations.
- None of the six sites reviewed had effectively implemented processes related to incident detection and analysis. While one site had consistently implemented related policies and procedures, it had not met event logging (EL) requirement EL2 (Intermediate) of OMB Memorandum M-21-31, *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents*.⁵ Four sites had not transitioned to EL1 (Basic) audit logging requirements. The sixth site did not implement software that would ensure file integrity.

Failure to fully design and implement policies, procedures, and processes related to incident handling activities elevates the risk of data loss or theft, unauthorized access and modification to data or systems, the disruption of services, and overall business impacts, such as financial losses. In addition, without fully defined and effective incident handling processes, stakeholders may not be fully aware of their roles and responsibilities when an incident occurs, which could lead to prolonging the response to an incident and increased damages.

⁵ OMB Memorandum M-21-31 established a maturity model to guide the implementation of requirements across four EL tiers: EL0 (Not Effective), EL1 (Basic), EL2 (Intermediate), and EL3 (Advanced).

RECOVER

The Recover cybersecurity function requires that assets and operations affected by a cybersecurity incident are restored. It supports the timely restoration of normal operations to reduce the effects of cybersecurity incidents and enables appropriate communication during recovery efforts. As such, it 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 executed restoration activities and the coordination of the restoration activities. During our FY 2025 evaluation, we identified deficiencies with the design and/or implementation of cybersecurity controls within this function.

Contingency Planning

The Contingency Planning security domain includes an emphasis on ensuring that the Department develops business impact analyses (BIAs) to guide contingency planning efforts. It also focuses on ensuring that contingency plans are tested to ensure recovery and limit disruption, after a cybersecurity incident occurs. To its credit, the Department had taken action and closed four of six recommendations from our prior year reviews that related to contingency planning. However, two recommendations from a prior year review had not been fully remediated and, therefore, had remained open. Furthermore, our FY 2025 FISMA metric work continued to find contingency planning weaknesses at the six sites reviewed. For instance:

- Although two sites had consistently implemented BIAs to guide contingency planning efforts, the remaining four sites had various weaknesses with the implementation of their defined related policies and procedures. For example, despite one site's policy requiring BIAs for all systems, it did not perform one for the system we reviewed during our test work. Additionally, the same site and another site had not fully integrated system-level BIAs into their organizational-level BIAs.
- All six sites were not fully effective in performing tests/exercises of their information system contingency plan (ISCP) processes. In particular, three sites had not used automated mechanisms to test contingency plans. Additionally, the same three sites did not coordinate ISCP testing with external stakeholders. The remaining sites had not consistently implemented existing ISCP-related policies or consistently documented support of existing policies being implemented. For example, one site had not consistently documented performed tabletop exercises or any improvements made to the ISCP, as a result of those exercises.

Without effectively designed and implemented contingency planning cybersecurity controls, the availability of Department assets and operations affected by a cybersecurity incident are at an elevated risk.

CYBERSECURITY REQUIREMENTS CHALLENGES

The OIG's special report, *Management Challenges at the Department of Energy – FY 2026* (DOE-OIG-26-05, December 2025), emphasizes that cybersecurity is a critical aspect of the Department's overall security posture and one of its highest risks. While the usual attacks by

adversaries remain persistent challenges, threats are increasingly coming from state-sponsored military and intelligence organizations, terrorist groups, and international crime organizations. Protecting and enhancing the security of the Department's information technology and operational technology assets, including critical infrastructure and high-value assets, is crucial to fulfilling the Department's unique mission set. Despite these known challenges, the Department continues to encounter challenges implementing Federal mandates, addressing evolving threats, and mitigating shortages in the cyber workforce.

This is illustrated, in part, by the Department's lack of progress in implementing NIST SP 800-53, Revision 5,⁶ and NIST CSF 2.0 requirements. Similar to the results reported in our prior year FISMA evaluation, our FY 2025 FISMA evaluation found that the Department continued to struggle with implementing the revised NIST SP 800-53 requirements. In particular, we found that four of the six FISMA metric sites evaluated had not yet fully implemented the requirements of NIST 800-53, Revision 5. Specifically, we identified 21 of 42 systems at the 4 sites still operating under the outdated NIST 800-53, Revision 4, requirements. Of those 21 systems, 9 systems processed controlled unclassified information, including 7 systems that processed PII. Due to the confidentiality impact value for controlled unclassified information being no lower than moderate, systems containing such information are required to have implemented controls that align with NIST 800-53, Revision 5, or a successor standard, in accordance with Department Order 471.7, *Controlled Unclassified Information*. Additionally, despite NIST CSF 2.0 being published in February 2024, our metric work found that multiple sites had not fully implemented the requirements set within NIST CSF 2.0. As a result, we identified weaknesses in various areas, such as the development and maintenance of data and metadata inventories.

The sites that continued to utilize outdated requirements indicated various reasons for their noncompliance. For example, site officials at one site indicated that they were contractually obligated to align with NIST SP 800-53, Revision 4, rather than the requirement's latest revision. In another instance, three sites had not fully implemented NIST CSF 2.0, in part, due to Department Order 205.1D, *Department of Energy Cybersecurity Program*, not explicitly requiring adherence to NIST CSF 2.0. Delayed implementation of Federal cybersecurity requirements, such as NIST 800-53, Revision 5, and NIST CSF 2.0 continues to leave the Department's data and information systems at risk to emerging threats and vulnerabilities.

RISKS 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 unauthorized 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, weaknesses were identified across the Department within all 10 security domains. Failure to design and implement effective cybersecurity controls could leave the

⁶ NIST SP 800-53, Revision 5, was published in September 2020; therefore, Revision 4 of the publication was withdrawn from use on 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 OMB.

Department's confidentiality, integrity, and availability of systems and sensitive information unprotected with significant implications to operations, assets, and/or the welfare of individuals and the Nation.

Similar to findings reported in previous years, 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. Without defined and effectively implemented governance structures through policies and procedures, cybersecurity-related activities are at risk of not being effectively managed and monitored. For example, the sites that we identified in FY 2025 as having asset inventory deficiencies were at an elevated risk of data mismanagement. Absent of related defined and implemented policies and procedures, the Department could be more exposed to loss, inaccuracies, and security vulnerabilities that may result in unauthorized access to protected or sensitive data.

To its credit, during FY 2025, the Department informed the OIG of steps taken to strengthen its cybersecurity program. For instance, the Department continued to prioritize adoption of a Zero Trust Architecture across the enterprise to meet security goals and comply with Federal mandates. Department offices and National Laboratories refined Zero Trust Architecture implementation plans, to include documenting current and target-state maturity for all high-value assets and high-impact systems in line with OMB Memorandum M-24-14, *Administration Cybersecurity Priorities for the FY 2026 Budget*. Additionally, in FY 2025, the Department awarded 13 projects intended to drive innovation and modernize cyber defenses, while also completing 13 projects funded in previous fiscal years. These completed projects were related to various initiatives in areas such as risk and asset management, identity and access management, configuration management, data protection and privacy, and ISCM. Other Department initiatives include identifying areas where they can share capabilities in terms of cybersecurity/IT tools to reduce duplication of effort. For instance, Office of Science officials stated that they regularly coordinate with the Office of the Chief Information Officer, which includes updates on their shared cloud authority to operate and joint enterprise license agreement efforts with the National Nuclear Security Administration. Finally, the Department is also tracking its progress toward implementation of OMB Memorandum M-21-30, *Protecting Critical Software Through Enhanced Security Measures*, OMB Memorandum M-21-31 and improving audit logging, inventory of operational technology assets, information technology inventory, multi-factor authentication, and end-point detection and response capabilities.

Recommendations

To address the identified cybersecurity program weaknesses throughout the Department, we made 55 new recommendations in FY 2025. In addition, 63 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 our report, *The Department of Energy's Fiscal Year 2025 Consolidated Financial Statements*. During FY 2025, we found that the Department had taken actions to close 57 recommendations; therefore, at the end of FY 2025, 118 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.

While management at the sites and programs reviewed concurred with most of our findings, management at two sites nonconcurred with nine 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 and OIG Response

Management concurred with 46 of 55 new recommendations issued in FY 2025 to the programs and sites related to improving the Department's cybersecurity program. However, management nonconcurred with nine recommendations and noted that two of the nine 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 undertaken to address the 120 cybersecurity program weaknesses previously noted by the OIG, closing out 57. Management's comments are included in Appendix 5.

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

Recommendations by Domain Category

The following table (Table 3) illustrates the number of Office of Inspector General recommendations issued to the Department throughout the last 4 years. These recommendations were then categorized by security domain to align with the *National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) 2.0*. Table 3 also provides a summary of recommendations to include those that resulted from our fiscal year (FY) 2025 *Federal Information Security Modernization Act of 2014* evaluation, audit of *The Department of Energy's Fiscal Year 2025 Consolidated Financial Statements*, and prior year recommendations that remain open. In FY 2025, 118 cyber-related recommendations remained open for management within the Department of Energy to address. Although the Department made some noticeable progress in remediating deficiencies within the domains of Configuration Management and Information Security Continuous Monitoring, a significant deficiency was identified within the Identity and Access Management domain. As a result, 45 of 118 (38 percent) recommendations contributed to identity and access management issues.

Table 3: Current and Prior Year Recommendations

Security Domain Category	FY 2025	FY 2024	FY 2023	FY 2022
Cybersecurity Governance ⁷	0	Not Applicable	Not Applicable	Not Applicable
Cybersecurity Supply Chain Risk Management ⁸	0	0	0	0
Risk and Asset Management ⁹	30	30	24	10
Configuration Management	28	38	23	29
Identity and Access Management	45	22	8	22
Data Protection and Privacy	2	2	0	2
Security Training	2	5	2	1
Information Security Continuous Monitoring	8	18	3	3
Incident Response	1	1	0	0
Contingency Planning	2	6	0	0
Other Recommendations - Uncategorized	0	1	5	6
Total Recommendations	118	123¹⁰	65	73

⁷ In the *FY 2025 Inspector General FISMA Reporting Metrics*, a new function area (Govern) was created to align with the *National Institute of Standards and Technology Cybersecurity Framework 2.0*. As a result, a new domain (Cybersecurity Governance) was established.

⁸ In the *FY 2025 Inspector General FISMA Reporting Metrics*, the supply chain risk management domain moved from the Identify function to the Govern function and was renamed to Cybersecurity Supply Chain Risk Management.

⁹ In the *FY 2025 Inspector General FISMA Reporting Metrics*, the Risk Management domain was renamed to the Risk and Asset Management domain.

¹⁰ In FY 2024, three newly issued recommendations were closed during the FY. Specifically, 2 of the 30 recommendations in the Risk and Asset Management domain were closed, while 1 of the 22 recommendations in the Identity and Access Management domain was closed. Therefore, 120 recommendations remained open at the end of FY 2024.

Federal Information Security Modernization Act of 2014 Fiscal Year 2025 Metrics Results¹¹

Inspectors General are required to assess the effectiveness of information security programs on a maturity model spectrum, in which the foundational levels ensure that the 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, “Managed and Measurable,” or above, represents an effective level of security. The following table (Table 4) presents the results of our security metrics for each of the six locations reviewed.

Table 4: Fiscal Year 2025 Metrics Results

Metrics	A	B	C	D	E	F
Govern – Cybersecurity Governance						
To what extent does the organization develop and maintain cybersecurity profiles that are used to understand, tailor, assess, prioritize, and communicate its cybersecurity objectives?						
	1	2	1	1	1	1
To what extent does the organization use a cybersecurity risk management strategy to support operational risk decisions?						
	3	2	1	1	4	3
To what extent do cybersecurity roles, responsibilities, and authorities foster accountability, performance assessment, and continuous improvement?						
	3	2	3	3	3	2

¹¹ The metrics results relayed here only include sites tested by the Office of Inspector General’s contract auditor. 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-25-04, *Fiscal Year 2025 Guidance on Federal Information Security and Privacy Management Requirements*, and the *Fiscal Year 2025 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics, Version 2.0*.

Appendix 2

Metrics	A	B	C	D	E	F
Govern – Cybersecurity 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	5	3	3	5	5
Identify – Risk and Asset 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?						
	3	2	3	1	2	2
To what extent does the organization use standard data elements/taxonomy to develop and maintain an up-to-date inventory of hardware assets (e.g., Government-furnished equipment, internet of things, and bring your own device mobile devices) connected to the organization’s network with the detailed information necessary for tracking and reporting?						
	2	2	2	2	2	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?						
	3	2	3	1	2	2
To what extent does the organization develop and maintain inventories of data and corresponding metadata for designated data types, as appropriate throughout the data lifecycle?						
	1	1	1	1	1	1
To what extent does the organization ensure that information system security risks are adequately managed?						
	2	2	1	1	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?						
	2	2	1	2	1	1

Metrics	A	B	C	D	E	F
Protect – Configuration Management						
To what extent does the organization use configuration settings/common secure configurations for its information systems?						
	2	2	2	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?						
	3	2	3	2	2	2
Protect – Identity and Access Management						
To what extent has the organization implemented phishing-resistant multifactor authentication mechanisms (e.g., personally identifiable verification, Fast Identity Online 2, or web authentication) for non-privileged users to access the organization’s physical and logical assets (organization-defined entry/exit points), networks, and systems, including for remote access?						
	4	3	3	2	4	3
To what extent has the organization implemented phishing-resistant multifactor authentication mechanisms (e.g., personal identification verification, Fast Identity Online 2, or web authentication) for privileged users to access the organization’s physical and logical assets (organization-defined entry/exit points), networks, and systems, including for remote access?						
	2	3	3	2	4	2
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?						
	3	2	2	1	2	2
Protect – Data Protection and Privacy						
To what extent has the organization implemented the following security controls to protect the confidentiality, integrity, and availability of its personal 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						

Appendix 2

Metrics	A	B	C	D	E	F
- Backups of data are created, protected, maintained, and tested - Access to personal email, external file sharing and storage sites, and personal communication applications are blocked, as appropriate						
	2	2	2	2	2	2
To what extent has the organization implemented security controls (e.g., data loss prevention, intrusion detection and prevention system, cloud access security broker, user and entity behavior analytic tools, security information and event management and endpoint detection and response) to prevent data exfiltration and enhance network defenses?						
	3	2	2	2	2	3
Protect – Security Training						
To what extent does the organization use an assessment of the skills, knowledge, and abilities of its workforce to provide specialized security training within the functional areas (Govern, Identify, Protect, Detect, Respond, and Recover)?						
	2	2	1	1	2	1
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?						
	2	2	2	1	2	3
To what extent does the organization monitor and measure the integrity and security posture of all owned and associated assets?						
	3	3	2	2	3	2
To what extent does the organization perform ongoing (continuous monitoring) information system assessments to grant system authorizations, including developing and maintaining system security plans, and monitoring system security controls?						
	2	2	2	1	2	3
Respond – Incident Response						
To what extent has the organization implemented processes related to incident detection and analysis?						
	3	2	2	2	2	2
To what extent has the organization implemented processes related to incident handling?						
	3	2	3	2	3	1

Metrics	A	B	C	D	E	F
Recover – Contingency Planning						
To what extent does the organization ensure that the results of business impact analyses are used to guide contingency planning efforts?						
	2	3	2	2	3	2
To what extent does the organization perform tests/exercises of its information system contingency planning processes?						
	3	3	2	2	3	2

Objective, Scope, and Methodology

Objective

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

Scope

We conducted the evaluation from January 2025 through May 2026 at 29 Department locations under purview of the Office of the Chief Information Officer, the Office of the Chief Financial Officer, the Office of Environmental Management, the Office of the Under Secretary for Nuclear Security and National Nuclear Security Administration, the Office of the Under Secretary for Science and Innovation,¹² the Office of the Under Secretary of Infrastructure,¹³ and certain staff offices. Of the 29 locations reviewed, 6 were 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, *The Department of Energy’s Fiscal Year 2025 Consolidated Financial Statements*. In addition, our evaluation also 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. This evaluation was conducted under the Office of the Inspector General project number A25TG002.

Methodology

To accomplish our audit 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.

¹² As of November 2025, the Office of the Under Secretary for Science and Innovation has been renamed the Office of the Under Secretary for Science.

¹³ As of November 2025, the Office of the Under Secretary for Infrastructure has been renamed the Office of the Under Secretary of Energy. Additionally, the Office of Energy and Renewable Energy, which had formerly aligned under the Office of the Under Secretary for Science and Innovation, is now under the purview of the Office of Critical Minerals and Energy Innovation.

- 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 initiatives.
- 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 Office of Inspector General, 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 Office of Inspector General'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-25-04, *FY 2025 Guidance on Federal Information Security and Privacy Management Requirements*, *FY 2025 Inspector General FISMA Reporting Metrics, Version 2.0*, and *FY 2025 Inspector General FISMA Metrics Evaluator's Guide, Version 1.0*.
- 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 the OIG contract auditor, we performed procedures that provided 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 been 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 vulnerability scans by confirming the weaknesses disclosed with responsible onsite personnel and performed other procedures to attest 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 September 29, 2026.

Related Reports

Office of Inspector General

- Special Report: [*Management Challenges at the Department of Energy – Fiscal Year 2026*](#) (DOE-OIG-26-05, December 2025). Our fiscal year (FY) 2026 Management Challenges Report identified that the Department of Energy continues to encounter cybersecurity challenges implementing Federal mandates, addressing evolving threats, and mitigating shortages in the cyber workforce. Particularly, our work found that the Department continues to fall behind changing cybersecurity requirements and enhancements. Despite Department directives requiring implementation of the latest Federal cybersecurity guidance, 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. In many cases, officials indicated that while new requirements need to be implemented, they are underfunded or not funded at all.
- Financial Statement Audit: [*The Department of Energy’s Fiscal Year 2025 Consolidated Financial Statements*](#) (DOE-OIG-26-03, December 2025). This audit was performed by the independent public accounting firm KPMG LLP (KPMG) on behalf of the Department’s Office of Inspector General. KPMG audited the consolidated financial statements of the Department, which comprise the consolidated balance sheet as of September 30, 2025, and the related consolidated statements of net cost, changes in net position, and combined statement of budgetary resources for the year then ended, and the related notes to the consolidated financial statements. In part, the audit identified certain deficiencies in internal control that KPMG considered to be a significant deficiency related to access controls over the Department’s various financial systems.
- Evaluation Report: [*The Department of Energy’s Unclassified Cybersecurity Program – 2024*](#) (DOE-OIG-25-30, August 2025). 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 FY related to various areas of cybersecurity programs. Although management concurred with most of our findings, management at two sites nonconcurred with four of our recommendations. When fully implemented, the 123 recommendations made during FY 2024 should help to enhance the Department’s unclassified cybersecurity program. 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 2025*](#) (DOE-OIG-25-05, November 2024). Cybersecurity remains a critical aspect of the Department’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, at the time of the publication of the Special Report, we were 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, 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 FY 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.
- Evaluation Report: [*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.

Government Accountability Office

- [*Information Technology: Agencies Need to Plan for Modernizing Critical Decades-Old Legacy Systems*](#) (GAO-25-107795, July 2025). The Government Accountability Office issued a report in FY 2025 that, in part, identified one of the Department's legacy information technology systems as most in need of modernization across the Federal Government. Specifically, modernization is needed to address ongoing cybersecurity threats and to support the legacy application as it becomes difficult and increasingly expensive to maintain. Additionally, while eight other identified agencies had developed modernization plans for their legacy information technology systems, the Government Accountability Office found that the Department was one of two agencies that did not have a modernization plan.

- [*Priority Open Recommendations: Department of Energy*](#) (GAO-25-108093, April 2025). The Government Accountability Office issued a letter in FY 2025 to provide an update on the overall status of the Department's implementation of recommendations and areas where open recommendations should be given high priority. In particular, as of April 2025, the Department had 257 open recommendations. Of those recommendations, 30 were identified as being priority and noted as having an effect over the Department's mission. These recommendations were summarized into the following six areas: improving contract, project, and program management; addressing nuclear modernization challenges; addressing the Department's environmental and disposal liability; addressing strategic human capital management; enhancing energy reliability, security, and resilience; and addressing insider threats and cybersecurity risks.

Management Comments



Department of Energy
Washington, DC 20585

August 19, 2026

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 of the Office of Inspector General's (IG) Draft Evaluation Report on *DOE's FY25 Unclassified Cybersecurity Program*. The Department, including the National Nuclear Security Administration, has undertaken a number of actions over the past year to address the 120 cybersecurity program weaknesses previously noted by the IG closing out 57.

The Department concurs with the 46 out of 55 new recommendations issued in FY 2025, to the programs and sites related to improving the Department's cybersecurity program. The Department non-concurs with nine recommendations, two of which were recently closed.

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 Robert Knisely, Chief Information Security Officer, in the Office of Chief Information Officer via Robert.Knisely@hq.doe.gov.

Sincerely,

DAWN
ZIMMER

Dawn Zimmer
Chief Information Officer

Digitally signed by DAWN
ZIMMER
Date: 2026.08.20 12:24:37
-04'00'

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.