U.S. DEPARTMENT OF ENERGY

Office of Inspector General

DOE-OIG-26-22 March 9, 2026

Weaknesses Identified With the Department of Energy's Unclassified Cybersecurity Program in Fiscal Year 2025

MANAGEMENT LETTER

Department of Energy
Washington, DC 20585

March 9, 2026

MEMORANDUM FOR THE SECRETARY; CHIEF INFORMATION OFFICER; AND VARIOUS DEPARTMENTAL PROGRAM OFFICES

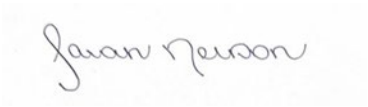
SUBJECT: Management Letter: *Weaknesses Identified With the Department of Energy's Unclassified Cybersecurity Program in Fiscal Year 2025*

Throughout fiscal year 2025, the Office of Inspector General (OIG) conducted cybersecurity reviews to determine whether the Department of Energy's unclassified cybersecurity program was implemented in accordance with Federal and Department requirements. The OIG also engaged its contractor, KPMG LLP, to perform the audit, *The Department of Energy's Fiscal Year 2025 Consolidated Financial Statements*, pursuant to requirements established by the *Government Management Reform Act of 1994*. During the audit, the OIG considered information technology-related controls. In addition, we conducted test work to support the evaluation of the Department's unclassified cybersecurity program in accordance with the *Federal Information Security Modernization Act of 2014*. This included test work specifically designed to satisfy the requirements of the Office of Management and Budget and the Council of Inspectors General on Integrity and Efficiency's *Federal Information Security Modernization Act of 2014* metrics.

In fiscal year 2025, the OIG issued 33 cybersecurity findings (including 13 repeat prior year findings) to Department sites and programs. However, three of those prior year findings, along with their recommendations, are being tracked in other OIG issued reports. Therefore, and as indicated in the attached report, we made 73 recommendations within 30 issued findings that, if fully implemented, should help the Department protect information resources and enhance its overall cybersecurity posture. While management at the sites and programs reviewed concurred with most of the findings, management at two locations did not concur with nine of our issued 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. Additionally, the audit, *The Department of Energy's Fiscal Year 2025 Consolidated Financial Statements*, identified certain access control deficiencies that KPMG LLP considered to be a significant deficiency over various financial systems within the Department. The findings that led to the significant deficiency are included within this report.

Due to the sensitivity of the vulnerabilities identified, portions of the management letter have been marked as Controlled Unclassified Information, including the status of all prior and current year findings.

The OIG would like to thank all participating Department elements for their courtesy and cooperation during the reviews.



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

cc: Deputy Secretary
Chief of Staff

DOE OIG HIGHLIGHTS

Weaknesses Identified With the Department of Energy's Unclassified Cybersecurity Program in Fiscal Year 2025

Why We Performed This Review

During fiscal year (FY) 2025, the Office of Inspector General (OIG) conducted cybersecurity reviews to determine whether the Department of Energy's unclassified cybersecurity program was implemented in accordance with Federal and Department requirements. The OIG also performed the audit, *The Department of Energy's Fiscal Year 2025 Consolidated Financial Statements*, which included test work over controls related to information technology.

The attached report discusses the results of cybersecurity reviews conducted by the OIG in FY 2025 and the results of our *Federal Information Security Modernization Act of 2014* evaluation.

What We Found

The OIG issued 33 cybersecurity findings (including 13 repeat prior year findings) to Department sites and programs related to information technology controls. However, three of those prior year findings, along with their recommendations, are being tracked in other OIG issued reports. Additionally, the audit, *The Department of Energy's Fiscal Year 2025 Consolidated Financial Statements*, identified a significant deficiency related to access controls over various Department financial systems. The findings that led to the significant deficiency are included within this report.

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

To address the issues identified in this report, we have made 73 recommendations that, if fully implemented, should help to enhance the Department's unclassified cybersecurity program. While management at sites and programs reviewed concurred with most of the findings, management at two locations did not concur with nine of our recommendations. However, our test results supported issuance of the findings; therefore, all issued findings and recommendations will remain open until all described weaknesses have been addressed.