U.S. DEPARTMENT OF ENERGY

Office of Inspector General

DOE-OIG-26-36

May 28, 2026

The Department of Energy's Cybersecurity and Information Technology Governance Program

AUDIT REPORT

On May 28, 2026, the Department of Energy Office of Inspector General issued audit report DOE-OIG-26-36, *The Department of Energy's Cybersecurity and Information Technology Governance Program*. Due to the audit report containing controlled unclassified information, it was not released publicly. However, in the interest of transparency, we prepared a highlights document to convey key summary facts from our work that is free of controlled information.

Department of Energy
Washington, DC 20585

May 28, 2026

MEMORANDUM FOR THE SECRETARY

SUBJECT: Audit Report: *The Department of Energy's Cybersecurity and Information Technology Governance Program*

We contracted with KPMG LLP (KPMG) to audit the Department of Energy's cybersecurity and information technology governance program. KPMG's review considered select internal controls' compliance with Office of Management and Budget, National Institute of Standards and Technology, and Department requirements related to cybersecurity and information technology governance practices.

KPMG made 11 recommendations to the Department to address the report's findings related to areas such as outdated contracts, policies, and/or requirements to include standard terms and conditions for prime and subcontractors. In addition, the Department had not fully implemented an enterprise data strategy, risk monitoring program, or comprehensive enterprise information system inventory to include those with personally identifiable information. Further, improvements were needed for ensuring compliance with Federal requirements, developing a comprehensive workforce assessment, and verifying the completeness and accuracy over requests for data. Management concurred with the recommendations and planned to take corrective actions. Management's responses are included within Appendix VI of the report.

KPMG was responsible for the attached audit report April 14, 2026, and the conclusions expressed therein. The Office of Inspector General monitored audit progress and reviewed the audit report and related documentation. This review disclosed no instances where KPMG did not comply, in all material respects, with generally accepted government auditing standards. The Office of Inspector General did not express an independent opinion on the Department's cybersecurity and information technology governance program.

We appreciated the cooperation and assistance received during this audit.

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-26-36

DOE OIG HIGHLIGHTS

The Department of Energy's Cybersecurity and Information Technology Governance Program

Why the Audit Was Performed

This audit, performed by KPMG LLP (KPMG) on behalf of the Department of Energy Office of Inspector General (OIG), examined the Department's cybersecurity and information technology (IT) governance program.

The audit's objective was to determine whether the Department developed and implemented a governance structure over its cybersecurity and IT activities.

In contracting with an independent audit firm and drawing from the results of the audit, auditing standards require the OIG to review the work performed. Accordingly, the OIG oversaw the audit and reviewed the results. Our review disclosed no instances where KPMG did not comply, in all material respects, with generally accepted government auditing standards.

What the Audit Found

KPMG identified eight areas for improvement to the Department's cybersecurity and IT governance program. Specifically, KPMG identified findings related to areas such as outdated contracts, policies, and/or requirements to include standard terms and conditions for prime and subcontractors. In addition, the Department had not fully implemented an enterprise data strategy, risk monitoring program, or comprehensive enterprise information system inventory to include those with personally identifiable information. Further, improvements were needed for ensuring compliance with Federal requirements, developing a comprehensive workforce assessment, and verifying the completeness and accuracy over various requests for data from Department elements.

What the Audit Recommends

KPMG made 11 recommendations to the Department to address the report's 8 areas for improvement. These areas include enterprise-level approaches for ensuring the most recent Federal cybersecurity and IT governance requirements are more timely implemented and contractually required, enterprise-level areas, such as a data strategy, risk monitoring, and systems inventories, are either formalized and/or completed, and data call information is verified for completeness and accuracy.

How the Department Responded

The Department concurred with each of the 11 recommendations and planned to take corrective actions.

DOE-OIG-26-36