



U.S. DEPARTMENT OF ENERGY

Office of Inspector General

DOE-OIG-26-51

September 28, 2026

Improvements Needed to Reduce Risk of Unauthorized Access to Highly Sensitive Data and Personally Identifiable Information



MANAGEMENT ALERT

On September 28, 2026, the Department of Energy Office of Inspector General issued Management Alert, *Improvements Needed to Reduce Risk of Unauthorized Access to Highly Sensitive Data and Personally Identifiable Information*, report DOE-OIG-26-51. Due to the management alert report containing controlled unclassified information, it was not released publicly. However, in the interest of transparency, we prepared a cover memo document to convey key summary facts from our work that is free of controlled information.



Department of Energy
Washington, DC 20585

September 28, 2026

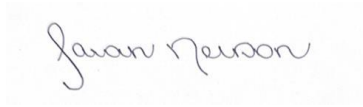
MEMORANDUM FOR A DEPARTMENT OF ENERGY ELEMENT'S LEADERSHIP

SUBJECT: Management Alert: *Improvements Needed to Reduce Risk of Unauthorized Access to Highly Sensitive Data and Personally Identifiable Information*

In November 2025, the Office of Inspector General began reviewing whether a Department of Energy element effectively managed security over a high-value asset information system in accordance with Federal and Department requirements. During our test work, we identified areas of extreme concern. Given the critical nature of this system and the data contained within, coupled with recent changes within the responsible Department element's management team, we are issuing this management alert. This alert provides leadership an opportunity to initiate immediate actions to address risks identified to ensure that continued operation of this information system does not place the Department's resources at higher risk. Specifically, during our testing, we identified vulnerabilities (30 critical, 2 high, and 63 medium) that could result in a higher-than-necessary risk of unauthorized disclosure or changes to sensitive data. This data pertains to current and past individuals employed or otherwise associated with the Department to include members of Congress and other Executive Branch entities. We also found that the Department officials did not consistently apply the concept of least functionality—minimizing the system's risk exposure—to system configurations.

Within our management alert, we have made one recommendation and have included, for context, the four recommendations already issued during the course of our review to help improve the cybersecurity program and mitigate specific vulnerabilities identified. Management concurred with the recommendations. Due to the sensitive nature of the vulnerabilities identified during the review, this management alert was issued as Controlled Unclassified Information. Additional specific information was provided to management as necessary for taking action on those vulnerabilities.

We appreciated the cooperation and assistance that we have received throughout this inspection. We look forward to continuing our review and will provide management with a report detailing the entirety of our results at the conclusion of our inspection.

A handwritten signature in cursive script, appearing to read "Sarah Nelson", is centered within a light gray rectangular box.

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

cc: Chief Information Officer
Chief Information Security Officer

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.