



U.S. DEPARTMENT OF ENERGY

# Office of Inspector General

DOE-OIG-26-28

March 30, 2026

## The Department of Energy Took Actions Necessary to Implement the Cybersecurity Information Sharing Act of 2015



EVALUATION REPORT



**Department of Energy**  
Washington, DC 20585

March 30, 2026

MEMORANDUM FOR THE CHIEF INFORMATION OFFICER; THE DIRECTOR, OFFICE OF INTELLIGENCE AND COUNTERINTELLIGENCE; AND THE DIRECTOR, OFFICE OF CYBERSECURITY, ENERGY SECURITY, AND EMERGENCY RESPONSE

SUBJECT: Evaluation Report: *The Department of Energy Took Actions Necessary to Implement the Cybersecurity Information Sharing Act of 2015*

The attached report summarizes the results of our review of the Department of Energy's implementation efforts from calendar year 2023 through calendar year 2024 to fulfill the requirements of the *Cybersecurity Information Sharing Act of 2015* (Cybersecurity Act). The Cybersecurity Act requires agencies to develop processes and procedures to facilitate and promote the timely sharing of cyber threat information. It also requires the Office of Inspector General to report to Congress at least every 2 years. As such, we participated in a joint review led by the Office of the Inspector General of the Intelligence Community to assess efforts by seven executive agencies, including the Department, to implement the Cybersecurity Act requirements related to policies and procedures, information sharing, information classification, authorized clearances, types of cyber threat indicators, actions taken, violations, and barriers. Our evaluation determined that the Department had taken the actions necessary to implement the requirements of the Cybersecurity Act. Considering the Department's continued implementation of the Cybersecurity Act and its successful implementation of mitigating actions, we did not make formal recommendations for improvement. This report contains Controlled Unclassified Information.

We conducted this evaluation from February 2025 through November 2025 in accordance with the Council of the Inspectors General on Integrity and Efficiency's *Quality Standards for Inspection and Evaluation* (December 2020). We appreciated the cooperation and assistance received during this evaluation.

A handwritten signature in cursive script that reads "Sarah Nelson".

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

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

DOE-OIG-26-28

# DOE OIG HIGHLIGHTS

## *The Department of Energy Took Actions Necessary to Implement the Cybersecurity Information Sharing Act of 2015*

---

### Why We Performed This Evaluation

The *Cybersecurity Information Sharing Act of 2015* (Cybersecurity Act) requires agencies to develop processes and procedures to facilitate and promote the timely sharing of cyber threat information. It also requires the Office of Inspector General to report to Congress at least every 2 years on the sufficiency of information sharing policies, procedures, and guidelines.

We participated in a joint review led by the Office of the Inspector General of the Intelligence Community to assess efforts by seven executive agencies, including the Department of Energy, to implement Cybersecurity Act requirements related to policies and procedures, information sharing, and barriers.

### What We Found

Our evaluation determined that the Department had taken the actions necessary to implement the requirements of the Cybersecurity Act. Specifically, we found that policies and procedures related to the sharing of cyber threat indicators were sufficient and included requirements for the removal of personally identifiable information. Officials also indicated that they were unaware of any violations by the Department regarding the failure to remove personally identifiable information related to a cybersecurity threat. In addition, Department officials informed us that security clearances were authorized for the purpose of sharing classified cyber threat indicators and defensive measures with the private sector. The Department also continued to share and receive cyber threat indicators using Automated Indicator Sharing capabilities during the period under review.

Although the barrier related to the quality of cyber threat indicators received from the Office of the Director of National Intelligence was mitigated since our 2023 evaluation, with the discontinued active feed of the Intelligence Community Analysis and Signature Tool, Department officials noted another barrier related to the quality of cyber threat indicators shared with the Department and industry partners. Specifically, information-sharing fatigue from the large quantity of cyber threat indicators was noted as an issue. While Department officials noted this barrier, we did not identify any associated impact to the sharing of threat indicators and defensive measures from calendar year 2023 through calendar year 2024.

### What We Recommend

Due to the Department's continued implementation of the Cybersecurity Act, we did not make formal recommendations for improvement.

## 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](mailto: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](mailto:OIGpublicaffairs@hq.doe.gov) and include your name, contact information, and the report number.