Office of Inspector General

OFFICE OF CYBER ASSESSMENTS AND DATA ANALYTICS

EVALUATION REPORT

THE DEPARTMENT OF ENERGY'S IMPLEMENTATION OF THE CYBERSECURITY INFORMATION SHARING ACT OF 2015

DOE-OIG-24-09
DECEMBER 2023

Department of Energy
Washington, DC 20585

December 20, 2023

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

SUBJECT: Evaluation Report on The Department of Energy's Implementation of the Cybersecurity Information Sharing Act of 2015

The attached report summarizes the results of our evaluation of the Department of Energy's implementation efforts during calendar years 2021 and 2022 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 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, to implement Cybersecurity Act requirements related to policies and procedures, information sharing, and barriers. Our evaluation determined that the Department had taken the actions necessary to implement the requirements of the Cybersecurity Act despite a barrier related to the quality of cyber threat indicators shared by the Office of the Director of National Intelligence. Considering the Department's continued implementation of the Cybersecurity Act, we did not make formal recommendations for improvement.

We conducted this evaluation from March 2023 through November 2023 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.

Kshemendra Paul
Assistant Inspector General
for Cyber Assessments and Data Analytics
Office of Inspector General

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

Department of Energy
Office of Inspector General

The Department of Energy's Implementation of the Cybersecurity Information Sharing Act of 2015
(DOE-OIG-24-09)

WHY THE OIG 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. 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 of Energy, to implement Cybersecurity Act requirements related to policies and procedures, information sharing, and barriers.

What Did the OIG Find?

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 or classify 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 energy sector. The Department also continued to share and receive cyber threat indicators using Automated Indicator Sharing capabilities, resulting in almost 33,000 cyber threat indicators and defensive measures being shared with the U.S. Department of Homeland Security. Over 475,000 indicators and defensive measures were also received from the U.S. Department of Homeland Security during calendar years 2021 and 2022.

What Is the Impact?

Although the barrier related to the classification of cyber threat information greatly improved since our 2021 evaluation, Department officials noted another barrier related to the quality of cyber threat indicators received from the Office of the Director of National Intelligence. While Department officials noted these barriers, we did not identify any impact to the sharing of threat indicators and defensive measures during calendar years 2021 and 2022.

What Is the Path Forward?

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

Table of Contents

Background and Objective

Background

The Cybersecurity Information Sharing Act of 2015 (Cybersecurity Act) was signed into law in December 2015 to improve the Nation's cybersecurity posture through enhanced information sharing related to cybersecurity threats. The law authorizes sharing of classified and unclassified cyber threat indicators and defensive measures among Federal agencies and with properly cleared private sector representatives. A cyber threat indicator is information that is necessary to describe or identify malicious reconnaissance, including anomalous patterns of communications that appear to be transmitted for the purpose of gathering technical information related to a cybersecurity threat or security vulnerability. A defensive measure is any tool, technique, or procedure applied to an information system or its information to detect, prevent, or mitigate a known or suspected cybersecurity threat or vulnerability.

The Cybersecurity Act requires agencies to develop processes and procedures to facilitate and promote the timely sharing of cyber threat information. To address privacy and civil liberty concerns, Federal agencies must only retain, use, and disseminate information that is directly related to a cybersecurity threat, and all unrelated personally identifiable information must be removed to prevent unauthorized use or disclosure. In addition, the Cybersecurity Act 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. 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 of Energy, to implement Cybersecurity Act requirements related to policies and procedures, information sharing, and barriers. This report summarizes the results of our review of the Department's implementation efforts in conjunction with the Office of the Inspector General of the Intelligence Community.

Report Objective

We conducted this evaluation to determine the Department's actions taken during calendar years (CYs) 2021 and 2022 to implement the requirements of the Cybersecurity Act.

Results of Review

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 or classify information related to a cybersecurity threat. In addition, we found that the Department had authorized security clearances for the purpose of sharing threat indicators and defensive measures with the private sector representatives. During CYs 2021 and 2022, the Department continued to use the Automated Indicator Sharing capabilities to share and receive cyber threat indicators and defensive measures with the U.S. Department of Homeland Security (DHS).

Our test work focused on the Department's compliance with the Cybersecurity Act and did not test the effectiveness of its implementation efforts. Although the barrier noted in our previous evaluation related to the classification of cyber threat information has greatly improved, Department officials identified a new barrier with the use of the Intelligence Community Analysis and Signature Tool (ICOAST)[1] to receive cyber threat information. Specifically, officials asserted that ICOAST contained poor quality indicators of compromise, including inconsistent or inaccurate data tagging. However, we noted that this barrier did not impact the sharing of threat indicators and defensive measures during the period under review.

Policies and Procedures

The Department had implemented policies, procedures, and guidelines for sharing cyber threat indicators such as Department Order 205.1C, *Department of Energy Cybersecurity Program*, and the *Federal Multilateral Information Sharing Agreement* (January 2019). In addition, our review found that the Department did not use, but was aware of, the following four policy and procedure documents maintained by DHS to support automated information sharing:

- *Sharing of Cyber Threat Indicators and Defensive Measures by the Federal Government under the Cybersecurity Information Sharing Act of 2015*;
- *Final Procedures Related to the Receipt of Cyber Threat Indicators and Defensive Measures by the Federal Government*;
- *Guidance to Assist Non-Federal Entities to Share Cyber Threat Indictors and Defensive Measures with Federal Entities under the Cybersecurity Information Sharing Act of 2015*; and
- *Privacy and Civil Liberties Final Guidelines: Cybersecurity Information Sharing Act of 2015.*

[1] ICOAST was deployed by the Office of the Director of National Intelligence's Intelligence Community Security Coordination Center in April 2017 to increase cybersecurity threat intelligence sharing, including indicators of compromise and malware signatures.

The four documents above were not required to be implemented; however, we found that the Department used various policies, procedures, and guidelines for sharing cyber threat information, which we determined to be sufficient and compliant with the intent of the Cybersecurity Act.

Classification and Security Clearances

Similar to our prior report on *The Department of Energy's Implementation of the Cybersecurity Information Sharing Act of 2015* (DOE-OIG-22-22, January 2022), Department officials indicated that there was no classified threat information shared with the private sector representatives. Our prior report also noted that security clearances were not issued to private sector representatives. However, the Department has since authorized security clearances for the purpose of sharing threat indicators and defensive measures with the private sector representatives during the period under review. In particular, the Department had 32 active security clearances in CY 2021 and 67 active security clearances in CY 2022. The Department's Office of Cybersecurity, Energy Security, and Emergency Response oversees the private sector clearance program. Officials from the Office of Cybersecurity, Energy Security, and Emergency Response indicated that the number of security clearances was managed by using reports from the Department's Central Personnel Clearance Index and by coordinating directly with the Department's Office of Departmental Personnel Security. The Department also has guidelines that describe its process for identifying, selecting, and sponsoring security clearances for private sector representatives.

Information Sharing

The Department continued to share and receive cyber threat indicators using Automated Indicator Sharing capabilities—cyber threat feeds managed by DHS to promote sharing of cyber threat information. Specifically, the Department used Analyst1[2] for sharing and receiving cyber threat information with both DHS's Automated Indicator Sharing and Cyber Information Sharing and Collaboration Program feeds during CYs 2021 and 2022. Department officials noted that threat indicators from Analyst1 are correlated with the Department's network traffic and logging capabilities to determine if sites should be notified of potential or actual threats. Further, Department officials stated that while trending analysis was historically not effective in Analyst1, a new version includes a dashboard feature that allows for trend and pattern analysis of the data.

Based on information provided by the Department, we found that almost 33,000 cyber threat indicators and defensive measures had been shared with DHS during CYs 2021 and 2022. Similarly, we determined that the Department received over 475,000 cyber threat indicators and defensive measures from DHS in CYs 2021 and 2022. In particular, 428,391 were received in 2021 and 46,670 were received in 2022. A Department official stated that the significant decrease from 2021 to 2022 was a result of DHS improving its process of curating, prioritizing, and focusing the threat indicators it shares with Federal partners.

[2] Analyst1 is a threat intelligence platform that helps organizations collect, validate, analyze, and manage data on potential cybersecurity threats. It consolidates data from different sources and in different formats, applies advanced analytics to identify anomalies and patterns, and prioritizes potential threats based on severity and potential impact.

In addition, the Office of Cybersecurity, Energy Security, and Emergency Response continued to engage in threat information sharing with private sector representatives by using the Cybersecurity Risk Information Sharing Program and Analysis of Risks in the Energy Sector reports. The Cybersecurity Risk Information Sharing Program is a public-private partnership initially developed by the Department and now managed by the Electricity Information Sharing and Analysis Center. The program was developed to enhance collaboration with energy sector partners and facilitate near real-time delivery of relevant and actionable cyber threat information. The Analysis of Risks in the Energy Sector reports help energy sector entities evaluate the risk to their systems from identified threat vectors and provide additional context and details to ensure indicators are actionable.

Barrier

Although the barrier related to the classification of cyber threat information greatly improved since our 2021 evaluation, Department officials noted another barrier related to difficulties using ICOAST to receive cyber threat information. Specifically, officials asserted that ICOAST contained poor quality indicators of compromise, including inconsistent or inaccurate data tagging. While Department officials noted these barriers, we did not identify any impact to the sharing of threat indicators and defensive measures during CYs 2021 and 2022.

Recommendations

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

Appendix 1

Commonly Used Terms

Calendar Years	CYs
Cybersecurity Information Sharing Act of 2015	Cybersecurity Act
Department of Energy	Department
Intelligence Community Analysis and Signature Tool	ICOAST
U.S. Department of Homeland Security	DHS

Appendix 2

Objective, Scope, and Methodology

Objective

We conducted this evaluation to determine the Department of Energy's actions taken during calendar years 2021 and 2022 to implement the requirements of the Cybersecurity Information Sharing Act of 2015 (Cybersecurity Act)

Scope

The review was performed remotely from March 2023 through November 2023 with Department Headquarters in Washington, DC, and selected field sites. The Cybersecurity Act requires Inspectors General to report to Congress at least every 2 years concerning their agency's implementation status. As such, a joint assessment was performed by seven Inspectors General in consultation with the Office of the Inspector General of the Intelligence Community. Our review was limited to evaluating the Department's implementation efforts to meet the Cybersecurity Act requirements related to policies and procedures, information sharing, and barriers during calendar years 2021 and 2022. The evaluation was conducted under Office of Inspector General Project Number S23TG004.

Methodology

To accomplish our objective, we:

- Researched and reviewed Federal regulations and Department policies and procedures related to sharing cyber threat indicators within the Federal Government;
- Reviewed relevant reports issued by the Office of Inspector General, the U.S. Government Accountability Office, and the Office of the Inspector General of the Intelligence Community;
- Conducted interviews with personnel associated with the Department's implementation of the Cybersecurity Act; and
- Reviewed the Department's processes for sharing cyber threat indicators and defensive measures with other Federal agencies and the private sector representatives.

We conducted our evaluation in accordance with the *Quality Standards for Inspection and Evaluation* (December 2020) as put forth by the Council of the Inspectors General on Integrity and Efficiency. We believe that the work performed provides a reasonable basis for our conclusions.

Management officials from the National Nuclear Security Administration; Office of Science; Office of the Chief Information Officer; Office of Cybersecurity, Energy Security, and Emergency Response; and Office of Intelligence and Counterintelligence waived an exit conference on November 20, November 27, November 30, December 4, and December 7, 2023, respectively.

Appendix 3

Related Reports

Office of Inspector General

- Evaluation Report on *The Department of Energy's Implementation of the Cybersecurity Information Sharing Act of 2015* (DOE-OIG-22-22, January 2022). The Department of Energy had taken the actions necessary to implement the requirements of the Cybersecurity Information Sharing Act of 2015. 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 or classify information related to a cybersecurity threat. In addition, we found that the Department had not authorized security clearances for the purpose of sharing threat indicators and defensive measures with the private sector. Based on the information provided by the Department, we identified that over 7 million data items containing threat indicators and defensive measures had been shared with the U.S. Department of Homeland Security, and over 1,100 threat indicators were shared with private sector entities through the Cybersecurity Risk Information Sharing Program during calendar years 2019 and 2020.

Office of the Inspector General of the Intelligence Community

- *Unclassified Joint Report on the Implementation of the Cybersecurity Information Sharing Act of 2015* (AUD-2021-002-U, December 2021). The joint report summarized the results of Inspectors General reviews related to the implementation of the Cybersecurity Information Sharing Act of 2015 during calendar years 2019 and 2020. The effort was led by the Inspector General of the Intelligence Community in coordination with the U.S. Departments of Commerce, Defense, Energy, Homeland Security, Justice, and the Treasury. The Offices of Inspectors General determined that the sharing of cyber threat indicators and defensive measures had improved over the past 2 years, and efforts were underway to expand accessibility to information.

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.

Please send your comments, suggestions, and feedback to OIG.Reports@hq.doe.gov and include your name, contact information, and the report number. You may also mail comments to us:

Office of Inspector General (IG-12)
Department of Energy
Washington, DC 20585

If you want to discuss this report or your comments with a member of the Office of Inspector General staff, please contact our office at 202–586–1818. For media-related inquiries, please call 202–586–7406.