Office of Inspector General

OFFICE OF TECHNOLOGY, FINANCIAL, AND ANALYTICS

EVALUATION REPORT -

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

DOE-OIG-22-22
JANUARY 2022

Department of Energy
Washington, DC 20585

January 13, 2022

Memorandum for the Principal Deputy Assistant Secretary, Office of Cybersecurity, Energy Security, and Emergency Response; Chief Information Officer; and Director, Office of Intelligence and Counterintelligence

Todd Wisniewski

From: Todd Wisniewski
Deputy Assistant Inspector General
for Technology, Financial, and Analytics
Office of Inspector General

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

What We Reviewed and Why

The *Cybersecurity Information Sharing Act of 2015* (*Cybersecurity Act*) was signed into law in December 2015 to improve the Nation's cybersecurity 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. The objective of our evaluation was to determine the Department's implementation efforts during calendar year (CY) 2019 and CY 2020 to implement the requirements of the *Cybersecurity Act*. This report summarizes the results of our review of the Department's implementation efforts.

What We Found

We 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 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 (DHS), and over 1,100 threat indicators were shared with private sector entities through the Cybersecurity Risk Information Sharing Program during CY 2019 and CY 2020.

Our test work focused on the Department's compliance with the *Cybersecurity Act* and did not test the effectiveness of its implementation efforts. We found that while progress had been made since our 2019 evaluation, Department officials indicated that a barrier related to the classification of cyber threat information continued to exist that could potentially affect the timely sharing of threat indicators and defensive measures among Federal entities.

Policies and Procedures

The Department had developed and implemented policies, procedures, and guidelines for sharing cyber threat indicators. Specifically, our review found that although the Department did not utilize policy and procedure documents maintained by DHS to support automated information sharing, an official stated they were aware of the following four DHS documents:

- S*haring 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.*

Although the Department had not utilized the four DHS-maintained documents, the various policies, procedures, and guidelines included in our review for sharing cyber threat information were sufficient and complied with the intent of the *Cybersecurity Act*.

Information Sharing

The Department continued to share threat indicators using Automated Indicator Sharing (AIS) capabilities ─ cyber threat feeds managed by DHS to promote sharing of cyber threat information. Specifically, the Department utilized its Cyber Fed Model and Analyst1 for sharing cyber threat information with DHS' AIS and Cyber Information Sharing and Collaboration Program feeds during CY 2019 and CY 2020. These systems use a machine-to-machine platform that exchanges threat information with DHS' cyber threat feeds. Based on information provided, we found that over 9 million threat indicators and defensive measures were shared by DHS with the Department during CY 2019 and CY 2020. The following table illustrates the total number of threat indicators and defensive measures shared by DHS.

Indicators Shared by DHS with the Department		
Source Data Feeds	**CY 2019**	**CY 2020**
DHS' AIS	920,411	8,183,149
DHS' Cyber Information Sharing and Collaboration Program	9,376	8,528
Total Data Items Downloaded from DHS	**929,787**	**8,191,677**

Similarly, we determined that the Department shared over 7.6 million data items with DHS via AIS during CY 2019 and CY 2020. The Department provided the total number of data items shared with DHS and noted that each may contain one or multiple threat indicators and defensive measures. The following table identifies the total data items shared by the Department with DHS.

Data Items Shared by the Department with DHS[1]		
Source Data Feeds	**CY 2019**	**CY 2020**
DHS' AIS (FEDGOV)	1,786,321	2,086,514
DHS' AIS (Industry)	1,777,037	2,035,974
Total Cyber Threat Indicators Downloaded from DHS	**3,563,358**	**4,122,488**

In addition, the Department's Office of Cybersecurity, Energy Security, and Emergency Response continued to engage in threat information sharing with private sector entities through the Cybersecurity Risk Information Sharing Program. The Cybersecurity Risk Information Sharing Program is a public-private partnership initially developed by the Department and now managed by the North American Electric Reliability Corporation's Electricity Information Sharing and Analysis Center. The program was developed to enhance collaboration with energy sector partners and facilitate the timely bi-directional sharing of cyber threat information.

[1] Uploaded data items are not categorized by individual cyber threat indicators, defensive measures, or specific indicator types.

According to Department officials, all cyber threat sharing during the period under review was at the unclassified or official use only levels, and classified cyber threat information was not shared with private sector entities. Information provided by program officials indicated that the Department shared over 500 unclassified threat indicators with the private sector in CY 2019 and over 600 unclassified threat indicators in CY 2020.

Sharing threat indicators and defensive measures increases the amount of information available for defending systems and networks against cyberattacks. Shared cyber threat information could allow the Department's Integrated Joint Cybersecurity Coordination Center to provide unclassified cybersecurity monitoring, situational awareness, information sharing, reporting, incident response activities, and analysis/dissemination of evolving cybersecurity threats across the Department enterprise on a continuous basis.

Barrier

Department officials indicated that improvements to the implementation of the *Cybersecurity Act* will continue; however, one barrier continues to exist. Specifically, officials indicated that the classification of cyber threat information could potentially affect the sharing of threat indicators and defensive measures. While we noted this barrier, we did not identify any impact to the sharing of threat indicators and defensive measures during CY 2019 and CY 2020.

What We Recommend

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

Attachments

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

Commonly Used Terms

Automated Indicator Sharing	AIS
Calendar Year	CY
Cybersecurity Information Sharing Act of 2015	*Cybersecurity Act*
Department of Energy	Department
U.S. Department of Homeland Security	DHS

Objective, Scope, and Methodology

Objective

The objective of this evaluation was to determine the Department of Energy's actions taken during calendar year 2019 and calendar year 2020 to implement the requirements of the *Cybersecurity Information Sharing Act of 2015* (*Cybersecurity Act*). 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 *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.

Scope

The review was performed remotely from February 2021 through November 2021 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 its implementation status. As such, a joint assessment was performed by multiple 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 requirements of the *Cybersecurity Act* during calendar year 2019 and calendar year 2020. The evaluation was conducted under Office of Inspector General project number S21TG012.

Methodology

To accomplish the 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*;
- Obtained and reviewed a sample of cyber threat information shared with Federal agencies, Federal entities, and private sector entities; and
- Noted a barrier to the sharing of cyber threat indicators and defensive measures among Federal entities and the extent to which those impacted the Department's ability to provide information to its stakeholders.

Management officials waived an exit conference on January 6, 2022.

Related Reports

Office of Inspector General

- Special Report on the *Department of Energy's Implementation of the Cybersecurity Information Sharing Act of 2015* (DOE-OIG-20-21, December 2019). The Department of Energy had taken the actions necessary to carry out the requirements of the *Cybersecurity Information Sharing Act of 2015* (*Cybersecurity Act*). Specifically, we found that policies and procedures related to sharing cyber threat indicators were sufficient and included requirements for the removal of personally identifiable information. In addition, officials we spoke with indicated that the Department had not received any notifications of accidental submission of data determined to be classified. Furthermore, security clearances authorized for the purpose of sharing threat indicators and defensive measures with the private sector were processed in accordance with Federal and Department requirements. We were informed by officials that the Department shared over 3 million cyber threat indicators and defensive measures with other Federal agencies in calendar year 2018 and disseminated over 1.6 million industry indictors to the private sector through automated indictor sharing over the last 2 years.

- Special Report on the *Department of Energy's Implementation of the Cybersecurity Information Sharing Act of 2015* (DOE-OIG-18-13, January 2018). The Department had taken actions to carry out the requirements of the *Cybersecurity Act*. Specifically, the Department had taken actions related to development of policies and procedures; sharing and use of cyber threat indicators and defensive measures; and management and accounting of private sector security clearances for individuals responsible for sharing threat information. However, we noted that challenges existed that could impact the sharing of cyber threat information.

Government Accountability Office

- *Cybersecurity: Federal Agencies Met Legislative Requirements for Protecting Privacy When Sharing Threat Information* (GAO-19-114R, December 2018). According to the Government Accountability Office, the seven designated Federal agencies developed policies, procedures, and guidelines that met the eight *Cybersecurity Act* provisions relevant to the removal of personal information from cyber threat indictors and defensive measures.

Office of the Inspector General of the Intelligence Community

- *Unclassified Joint Report on the Implementation of the Cybersecurity Information Sharing Act of 2015* (AUD-2019-005-U, December 2019). The joint report summarized the results of Inspectors General reviews related to implementation of the *Cybersecurity Act* during calendar years 2017 and 2018. The effort was led by the Inspector General of the Intelligence Community in coordination with the Departments of Commerce, Defense, Energy, Homeland Security, Justice, and the Treasury. The Offices of

Inspectors General determined that sharing of cyber threat indicators and defensive measures had improved over the past 2 years and efforts were underway to expand information accessibility.

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.