OFFICE OF INSPECTOR GENERAL

U.S. Department of Energy

SPECIAL REPORT

DOE-OIG-20-21

December 2019

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

Department of Energy
Washington, DC 20585

December 30, 2019

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

FROM: Teri L. Donaldson
Inspector General

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

BACKGROUND

The *Cybersecurity Information Sharing Act of 2015* (Cybersecurity Act) was signed into law on December 18, 2015, to improve the Nation's cybersecurity through enhanced sharing of information related to cybersecurity threats. The law authorized sharing of classified and unclassified cyber threat indicators and defensive measures among Federal agencies and with properly cleared representatives in the private sector. 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 an action, device, procedure, signature, technique, or other measure applied to an information system or information that is stored on, processed by, or transmitted by an information system that detects, prevents, or mitigates a known or suspected cybersecurity threat or security vulnerability.

The Cybersecurity Act required 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 were required to retain, use, and disseminate only information that is directly related to a cybersecurity threat and remove personally identifiable information not directly related to a cyber threat to prevent unauthorized use or disclosure. In addition, the Cybersecurity Act required Inspectors 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 of seven executive agencies to implement the Cybersecurity Act requirements. In support of this joint endeavor, we performed this review to determine the Department of Energy's actions taken to carry out the requirements of the Cybersecurity Act. This report summarizes our findings specific to the Department.

RESULTS OF REVIEW

We determined that the Department had taken the actions necessary to carry out the requirements of the 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. Also, 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 (AIS) over the last 2 years.

Our review did not test the effectiveness of the Department's efforts to implement the Cybersecurity Act; rather, our test work focused on the Department's efforts to comply with the Cybersecurity Act. While progress has been made, Department officials indicated that barriers existed that have or could potentially affect the sharing of cyber threat indicators and defensive measures with Federal entities. In particular, officials identified barriers related to the costs associated with obtaining security clearances, the timeliness of obtaining and adjudicating security clearances, inconsistent communications from the U.S. Department of Homeland Security (DHS), and concerns related to liability protections for threat sources.

Policies and Procedures

The Department collaborated with DHS and the U.S. Department of Justice on the development of Government-wide information sharing policies and procedures, as required by the Cybersecurity Act. Department officials indicated that these documents established the overarching policies and procedures to support automated sharing of cyber threat indicators and defensive measures. The collaborative effort resulted in the development of the following Government-wide policies and procedures:

- 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.*

In addition to the above-mentioned policies and procedures, Department officials stated that internal policies and procedures specific to facilitating and promoting sharing with relevant entities, including the public, if appropriate, had also been developed and implemented. Officials also noted that they used non-Departmental supplemental guidance to enhance the implementation of Cybersecurity Act requirements. The culmination of these documents addressed privacy and civil liberties, development and implementation of near real-time sharing of cyber threat data, incorporation of appropriate security and privacy protections, and provided guidance for receiving and sharing cyber threat indictors.

Classification and Security Clearances

According to Department officials, all cyber threat data had been properly classified and officials were unaware of any breaches related to sharing of classified threat data. We did not evaluate the data to make a determination of whether the shared information was appropriately classified by officials. Specifically, our judgmental sample of 128 shared cyber threat indicators revealed that data was managed in a manner consistent with Department processes related to classification of information. In addition, officials within the Office of the Chief Information Officer stated that, to their knowledge, no shared cyber threat indictors or defensive measures contained classified information.

Further, we were informed that security clearances provided to private sector individuals for the purpose of sharing cyber threat information with the private sector were obtained through one of two methods. The first method required the sponsoring of an individual by the Department. According to an official within the Office of Cybersecurity, Energy Security, and Emergency Response (CESER), there were 39 active private sector security clearances and 8 pending clearances that were Department-sponsored at the time of our review. The Department also had a secondary method of obtaining security clearances for private sector individuals which required the nomination of individuals to DHS. DHS then sponsored the individual and the request for a clearance through its Private Sector Clearance Program for Critical Infrastructure. When nominating individuals through the DHS process, the Department was required to provide a justification or "need-to-know" for these individuals.

Information Sharing

The Department continued to share cyber threat indicators using the AIS capability – a system managed by DHS to promote sharing of cyber threat information. AIS enabled the Department to utilize actionable cyber threat data as it became available. Specifically, in response to a request for information, a Department official reported that DHS relayed over 1 million cyber threat indicators and defensive measures in calendar year 2017 and over 3 million indicators and defensive measures in calendar year 2018 via AIS feeds. Receipt of this information could allow the Department's Integrated 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.

Further, a Department official indicated that CESER continues to engage in threat information sharing with private energy sector entities through the Cybersecurity Risk Information Sharing Program (CRISP), among other tools and reports. CRISP 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 CRISP program was developed to enhance collaboration with energy sector partners and facilitate the timely bi-directional sharing of unclassified and classified cyber threat information.

Barriers

Department officials indicated that various barriers had or could have an impact on the sharing of cyber threat indicators and defensive measures. Specifically, officials commented that the cost of security clearances, the length of time to adjudicate a clearance, lack of communication from DHS, and liability protection provisions were considered to be barriers that had or could potentially adversely affect the sharing of cyber threat data. In particular, we noted the following:

- Originally funded by the Office of Management and Budget, CESER officials commented that as of October 2018, costs associated with private sector security clearances were funded through the Department's working capital fund. Specifically, for all security clearances requested by CESER, the cost of the clearances is transferred from CESER-appropriated funds into the working capital fund.

- Officials indicated that there were several challenges related to the security clearance process. For instance, an official indicated that private sector turnover in cybersecurity positions impacts the ability to have a timely clearance process. The official stated that turnover of private-sector employees necessitates initiating the clearance process for the new private sector employee, which, in turn, extends the length of time that it takes to have a private sector security clearance adjudicated. In addition, according to a CESER official, the lack of communication from DHS adversely affects the Department's ability to track Department-nominated DHS security clearance recipients. Specifically, the official stated that the Department is not always notified when a Department-sponsored private sector clearance is approved and does not receive confirmation when Department requests for clearance removals are completed. Further, an official commented that the Department should be receiving a monthly report on security clearances issued and being re-investigated, as well as a list of all DHS-held clearances nominated by the Department. However, the Department had not always received these reports.

- According to Department officials, the lack of protection from private sector suits may adversely affect the sharing of cyber threat indicators and defensive measures by the private sector. Specifically, Department officials stated that the Cybersecurity Act does not adequately incentivize entities in the private sector to share cyber threat indictors with Federal entities other than the Department of Homeland Security.

Attachments

cc: Chief of Staff

OBJECTIVE, SCOPE, AND METHODOLOGY

OBJECTIVE

The objective of this review was to determine the Department of Energy's actions taken to carry out the requirements of the *Cybersecurity Information Sharing Act of 2015*.

SCOPE

The review was performed between March and December 2019 at Department Headquarters in Washington, DC. The *Cybersecurity Information Sharing Act of 2015* 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 actions taken to meet the requirements of the *Cybersecurity Information Sharing Act of 2015*. The review was conducted under Office of Inspector General project number A19TG021.

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 Department's 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 Information Sharing Act of 2015*;
- Assessed the process for determining how the Department accounts for the number of security clearances authorized for sharing cyber threat indicators and defensive measures with the private sector;
- Determined whether a sample of shared information that was not directly related to a cybersecurity threat contained personal data or information related to privacy and civil liberties of a specific individual; and
- Identified barriers that potentially affected the sharing of cyber threat indicators and defensive measures among Federal entities.

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-18-13, January 2018). The Department of Energy had taken actions to carry out the requirements of the *Cybersecurity Information Sharing Act of 2015*; however, we identified several opportunities for improvement. Specifically, while the Department had taken actions related to: (1) development of policies and procedures; (2) sharing and use of cyber threat indicators and defensive measures; and (3) management and accounting of private sector security clearances for individuals responsible for sharing threat information, we noted that challenges existed that could have an impact on the sharing of cyber threat information in accordance with the *Cybersecurity Information Sharing Act of 2015*.

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 Information Sharing Act of 2015* provisions relevant to the removal of personal information from cyber threat indictors and defensive measures. No recommendations for improvement were made in this report.

Office of the Inspector General of the Intelligence Community

- *Joint Report on the Implementation of the Cybersecurity Information Sharing Act of 2015* (Audit Report AUD-2017-005, December 2017). The joint report summarizes the results of Inspectors General reviews related to implementation of the *Cybersecurity Information Sharing Act of 2015*. 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. Each Office of Inspector General independently obtained the required assessments on its agency's implementation of the *Cybersecurity Information Sharing Act of 2015* requirements, and the results were compiled into this report. The report disclosed various levels of progress among the agencies that participated.

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.