OFFICE OF INSPECTOR GENERAL

U.S. Department of Energy

SPECIAL REPORT

DOE-OIG-18-13 January 2018

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

Department of Energy
Washington, DC 20585

January 5, 2018

MEMORANDUM FOR THE SECRETARY

FROM: April G. Stephenson
Principal Deputy 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 appropriate private sector entities. Classified cyber threat indicators may also be shared outside the government but only with a strictly limited audience. A cyber threat indicator is information, such as an internet protocol address, necessary to describe or identify malicious cyber activities. A defensive measure is an action, device, or other mechanism applied to an information system to detect, prevent, or mitigate a known or suspected cybersecurity threat.

The Cybersecurity Act required agencies to develop processes and procedures to facilitate and promote the timely sharing of cyber threat information. It addressed sharing of cyber threat indicators and defensive measures both within the Federal Government and with private entities, as well as the potential impact on privacy and civil liberties. 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. We participated in a joint review led by the Office of the Inspector General of the Intelligence Community to summarize the efforts taken by six agencies, including the Department of Energy. To support the joint report, we performed this audit to determine whether the Department had taken actions consistent with the requirements of the Cybersecurity Act. This report summarizes our findings specific to the Department.

RESULTS OF AUDIT

We determined that the Department had taken actions to carry out the requirements of the Cybersecurity Act; 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 Act. Furthermore, although we did not test the effectiveness of the Department's efforts to implement the Cybersecurity Act, we did identify several opportunities for improvement related to managing the cyber information sharing process.

Policies and Procedures

We found that the Department collaborated with the Department of Homeland Security (DHS) and the Department of Justice during 2016 on the development of Government-wide information sharing policies and procedures, as required by the Cybersecurity Act. Department officials indicated that they primarily relied on the Government-wide policies and procedures to support automated sharing of cyber threat indicators and defensive measures. To their credit, although the Cybersecurity Act did not require the Department to create a separate policy, officials were in the process of developing agency specific policies.

During our review, we evaluated the *U.S. Department of Energy's Instruction for Automated Indicators Sharing of Unclassified Information (Draft).* The instruction, once finalized, will establish the requirement for sharing unclassified cybersecurity threat information with appropriate entities to prevent or mitigate adverse effects from cybersecurity threats. In addition, we noted that the Department's draft policy will outline the roles and responsibilities for sharing threat indicators in its possession. Based on our preliminary review, we believe that finalization and implementation of the policy will augment existing government-wide policies and procedures and further enhance the Department's implementation of the Cybersecurity Act.

Information Sharing

We found that the Department began sharing limited information with other Federal agencies during fiscal year 2016 in conjunction with DHS. In addition, the Department continued to share information with private energy sector organizations through an existing program administered by the Electricity Information Sharing and Analysis Center, a division of the North American Electricity Reliability Corporation. In particular, we identified the following:

- The Department's Office of the Chief Information Officer initially began receiving cyber threat indicators from other Federal agencies and the private sector using the Automated Indicator Sharing capability – a system managed by DHS to promote real-time sharing of cyber threat information. Later in 2016, the Department began a pilot program at one of its sites using Automated Indicator Sharing for bi-directional sharing of cyber threat indicators with DHS. DHS shared the information with other Federal agencies and the private sector, as appropriate. Department officials reported that the Department shared 79,966 cyber threat indicators with DHS in 2016 through the Automated Indicator Sharing system. However, the Department's pilot program provided only limited information.

Because only limited information was shared, we determined that the Department may not have been sharing certain cyber threat indicators with other organizations that could have been used to enhance their cybersecurity posture. For instance, we noted that information related to the actual or potential harm caused by an incident, including a description of the information exfiltrated as a result of a particular cybersecurity threat, may not have been shared as envisioned by the Cybersecurity Act. In addition, officials stated they had not shared defensive measures through Automated Indicator Sharing because each site and/or organization should determine how best to defend their environments. Management agreed that only one site was sharing information, but commented that the location was sharing all of the information it had available. While we agree that this is a positive step, we believe that additional information sharing could further enhance the Department's implementation of the Cybersecurity Act.

- The Department's Office of Electricity Delivery and Energy Reliability continued to share cyber threat indicators and defensive measures with private energy sector entities through the existing Cybersecurity Risk Information Sharing Program administered by the Electricity Information Sharing and Analysis Center. The Cybersecurity Risk Information Sharing Program is a public-private partnership, cofounded by the Department and the Electricity Information Sharing and Analysis Center, to enhance collaboration with energy sector partners to facilitate the timely bi-directional sharing of unclassified and classified threat information. In 2014, the Electricity Information Sharing and Analysis Center took the lead in managing the Cybersecurity Risk Information Sharing Program in collaboration with the Pacific Northwest National Laboratory. Office of Electricity Delivery and Energy Reliability officials commented that, at the time of our review, the collaboration had 28 participating utilities accounting for about 75 percent of the Nation's electric customers.

Private Sector Security Clearances

We identified potential opportunities for improvement with the Department's process for accounting for private sector clearances. We found that security clearances provided to private sector individuals for the purpose of sharing cyber threat information were obtained through one of two methods. The first method required the Department to sponsor the individual for a security clearance, which officials reported was used for a very limited number of private sector clearances. The second method required the Department to nominate individuals to DHS for clearances, which then sponsored those clearances through its Private Sector Clearance Program for Critical Infrastructure.

Office of Electricity Delivery and Energy Reliability officials informed the Office of Inspector General that the Department's only responsibility related to the DHS-sponsored clearances was to provide the justification, or "need-to-know," when nominating a private sector individual for a security clearance. According to the Office of Electricity Delivery and Energy Reliability officials, it was the private sector employee's responsibility to let DHS know if there was a change in employment status requiring the clearance to be terminated. Management also commented that clearance holders receive training that included requirements for individuals to report on various changes such as a change in job status. We noted, however, that the

Department's process document, *Nomination Process Document for Private Sector Clearance Program for Critical Energy Infrastructure*, indicated that responsibilities within the Department included identification of status/employment changes for clearance holders within the private energy sector. While management indicated that the document is only a best practice and we did not test the effectiveness of the clearance termination process, we are concerned that private sector clearances may not be terminated in the future when they are no longer needed, as required by Executive Order 12968, *Access to Classified Information*.

Barriers Affecting Sharing

Department officials indicated that cultural barriers within Federal agencies and the energy sector had an impact on the sharing of cyber threat indicators and defensive measures within the energy sector. The cultural barriers – such as the reluctance to release information deemed organizationally specific, liability concerns, or the general resistance to change – are an ongoing challenge that needs to be addressed. In addition, Office of the Chief Information Officer and Office of Electricity Delivery and Energy Reliability officials commented there was a general lack of openness by both government and private sector entities concerning cyber threat details, which hindered the positive impact such information could provide. For instance, officials commented that all participants in the program were happy to receive cyber threat indicators from other organizations; however, most organizations, including some within the Department, were reluctant to share information with others. As such, the challenge going forward will be to develop relationships that will drive active participation and contribution from all organizations.

SUGGESTED ACTIONS

To improve activities related to the Department's implementation of the Cybersecurity Act, we suggest that the Chief Information Officer:

1. Finalize the Department's policies and procedures for sharing cyber threat indicators and defensive measures while continuing to follow existing Government-wide policies and procedures; and

2. Based on results of the information sharing pilot program, proceed with the implementation of the Department's timeline for sharing cyber threat indicators and defensive measures across the entire Department by the second quarter of fiscal year 2019.

In addition, we suggest that the Assistant Secretary for the Office of Electricity Delivery and Energy Reliability:

3. Develop and implement a process, as appropriate, to ensure that the Department notifies DHS of status/employment changes for clearance holders within energy private sector entities.

Attachments

cc: Deputy Secretary
Chief of Staff
Chief Information Officer
Assistant Secretary for the Office of Electricity Delivery and Energy Reliability

OBJECTIVE, SCOPE, AND METHODOLOGY

OBJECTIVE

To determine whether the Department of Energy had taken actions consistent with the requirements of the *Cybersecurity Information Sharing Act of 2015*.

SCOPE

This audit was performed between April 2017 and January 2018 at Department Headquarters in Washington, DC. The review was limited to evaluating the Department's actions taken to meet the requirements of the *Cybersecurity Information Sharing Act of 2015*. The audit was conducted under Office of Inspector General project number A17TG022.

METHODOLOGY

To accomplish the objective, we:

- Reviewed applicable laws and regulations;
- Reviewed applicable standards and guidance issued by the Department, including the Department's Office of the Chief Information Officer and Office of Electricity Delivery and Energy Reliability;
- Reviewed prior reports issued by the Office of Inspector General and Government Accountability Office;
- Held discussions with officials and personnel from Department Headquarters, including representatives from the Office of the Chief Information Officer and the Office of Electricity Delivery and Energy Reliability;
- Reviewed cyber threat indicators and defensive measures shared with other Federal agencies and the private sector;
- Reviewed documents related to the use and dissemination of cyber threat indicators; and
- Interviewed personnel responsible for the classification of cyber threat indicators and defensive measures.

We conducted this audit in accordance with generally accepted Government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe the evidence obtained provides a reasonable basis for our findings and conclusion based on our objective. Accordingly, we assessed significant internal controls and compliance with laws and regulations to the extent necessary to satisfy the audit objective. In particular, we assessed the Department's implementation of the *GPRA Modernization Act of*

2010 and determined that it had established performance measures and/or goals related to improving cybersecurity in the energy sector through effective government-industry collaboration. Because our review was limited, it would not have necessarily disclosed all internal control deficiencies that may have existed at the time of our audit. We did not rely on computer-processed data to satisfy our objective.

Management waived an exit conference on December 22, 2017.

PRIOR REPORT

- Summary Report on the *Department of Energy's Implementation of Selected Controls as Defined in the Cybersecurity Act of 2015* (DOE-OIG-16-14, August 2016). The *Cybersecurity Act of 2015* required the Office of Inspector General to report on various aspects of the Department of Energy's national security systems and information systems containing personally identifiable information. We found that the Department had generally developed and implemented controls related to a number of areas covered by the *Cybersecurity Act of 2015*. However, based on the information reported by the Department, we also noted areas highlighted by the Act where the Department had not fully implemented certain types of controls.

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) 253-2162.