U.S. GOVERNMENT ACCOUNTABILITY OFFICE
**441 G St. N.W.**
**Washington, DC 20548**

Accessible Version

December 6, 2018

The Honorable Richard Burr
Chairman
The Honorable Mark R. Warner
Vice Chairman
Select Committee on Intelligence
United States Senate

The Honorable Devin Nunes
Chairman
The Honorable Adam Schiff
Ranking Member
Permanent Select Committee on Intelligence
House of Representatives

**Cybersecurity: Federal Agencies Met Legislative Requirements for Protecting Privacy When Sharing Threat Information**

Federal agencies and our nation's critical infrastructures, such as communications and financial services, are dependent on information technology systems and electronic data to carry out operations and to process, maintain, and report essential information.[1] The security of these systems and data is vital to public confidence and national security, prosperity, and well-being. Yet, cyber-based intrusions and attacks on federal and nonfederal systems have become not only more numerous and diverse, but also more damaging and disruptive. For example, a data breach reported in July 2015 at the Office of Personnel Management affected at least 21.5 million individuals and compromised federal employees' personal information, including Social Security numbers, residency and education history, employment history, financial history, and the fingerprints of approximately 5.6 million individuals.

Due to cyber-based threats to federal systems and critical infrastructure, the persistent nature of information security vulnerabilities, and associated risks, we have continued to designate information security as a government-wide high-risk area in our most recent biennial report to Congress—a designation we have made in each high-risk report since 1997.[2] We expanded this area beyond federal information systems to include the protection of cyber critical infrastructure in 2003 and protecting the privacy of personally identifiable information in 2015.

[1]The term "critical infrastructure," as defined in the Critical Infrastructures Protection Act of 2001, part of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act), refers to systems and assets so vital to the United States that their incapacity or destruction would have a debilitating impact on security, national economic security, national public health or safety, or any combination of these matters. 42 U.S.C.§5195c(e). Federal policy identifies 16 critical infrastructure sectors: chemical; commercial facilities; communications; critical manufacturing; dams; defense industrial base; emergency services; energy; financial services; food and agriculture; government facilities; health care and public health; information technology; nuclear reactors, materials, and waste; transportation systems; and water and wastewater systems.

[2]GAO, *High-Risk Series: Progress on Many High-Risk Areas, While Substantial Efforts Needed on Others,* GAO-17-317, (Washington, D.C.: February 15, 2017).

In December 2015, the President signed the Cybersecurity Information Sharing Act of 2015 (hereafter referred to as CISA or the act) into law to encourage the sharing of cyber threat information between the public and private sectors in a timely manner.[3] The act designated seven federal agencies to coordinate and develop government-wide, publicly available policies, procedures, and guidance to assist federal and nonfederal entities[4] in their efforts to receive and share[5] cyber threat indicators and defensive measures.[6] These seven agencies were the Departments of Homeland Security (DHS), Justice (DOJ), Defense (DOD), Commerce (DOC), Energy (DOE), and the Treasury, and the Office of the Director of National Intelligence (ODNI).

In addition, the act included provisions related to ensuring the protection of privacy and civil liberties during the information sharing activities. It also incorporated language related to limitations on collection and use of personal information. According to the act, the designated agencies were to develop guidelines for the protection of privacy and civil liberties when implementing the CISA provisions.

The act further required that these guidelines on privacy and civil liberties be consistent with the eight fair information practice principles defined in appendix A of the *National Strategy for Trusted Identities in Cyberspace* and other applicable provisions of law.[7] The fair information practice principles are the widely accepted framework of defining principles to be used in the evaluation and consideration of systems, processes, or programs that affect individual privacy.

Beyond the aforementioned requirements, the act included a provision for GAO to review actions taken by the federal government related to the removal of personal information from cyber threat indicators or defensive measures. Accordingly, our specific objective for this work was to determine the extent to which federal agencies have developed policies, procedures, and guidelines for the removal of personal information from cyber threat indicators and defensive measures, pursuant to CISA's provisions.[8]

To fulfill this objective, we gathered and analyzed policies, procedures, and guidelines that the seven designated federal agencies developed in response to requirements established within

[3]Consolidated Appropriations Act, 2016, Pub. L. No. 114-113, div. N (Cybersecurity Act of 2015), Title I (Cybersecurity Information Sharing Act of 2015), 129 Stat. 2242, 2936-56 (2015) (*codified at* 6 U.S.C. §§ 1501-10).

[4]A federal entity is a department or agency of the United States or any component of such department or agency. Nonfederal entities include state and local governments, private sector entities, and academic institutions.

[5] The act established requirements to develop artifacts for the receipt of cyber threat indicators and defensive measures by federal entities and for the sharing of cyber threat indicators and defensive measures by both federal and nonfederal entities. Unless explicitly specified as either receiving or sharing as part of a requirement within the act, this correspondence will collectively refer to these activities as "information sharing".

[6]As defined in CISA, cyber threat indicators include threat-related information such as methods of defeating or causing users to unwittingly enable the defeat of security controls and methods of exploiting cybersecurity vulnerabilities. Defensive measures include any actions, devices, procedures, techniques, or other means that detect, prevent, or mitigate a known or suspected cybersecurity threat or vulnerability.

[7]The White House, *National Strategy for Trusted Identities in Cyberspace,* Appendix A (Washington, D.C.: April 2011).

[8]CISA refers to the removal of "personal information" from cyber threat indicators and defensive measures. For the purposes of this correspondence, we consider personal information to include all information that an individual would consider sensitive and would not want to be released publicly. This information is generally referred to as personally identifiable information (PII) and is similar to, but may not be identical to, personal information.

the act. We compared these documents to requirements established by the eight provisions in the act (identified in table 1 of this report) that relate to the removal of personal information from cyber threat indicators and defensive measures. We also compared the contents of these documents to the eight fair information practice principles (identified in table 2 of this report).

Further, we gathered and analyzed information from the seven designated federal agencies on their use of DHS's Automated Indicator Sharing (AIS) capability—the primary government-wide capability for real-time, automated receipt and sharing of cyber threat indicators and defensive measures that was called for in the act.[9] Specifically, we looked at how each designated agency's relevant policies and guidance incorporated the use of this capability, including for the handling of personal information. In addition, we supplemented our analyses with interviews of responsible security and privacy officials from each of the seven agencies.

We conducted this performance audit from February 2018 to October 2018 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 objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

## Background

CISA encouraged the timely sharing of cyber threat information between the public and private sectors. To facilitate the implementation of provisions related to this information sharing, the act required the seven designated federal agencies to jointly develop publicly available policies, procedures, and guidelines to assist federal and nonfederal entities in sharing information on cyber threat indicators and defensive measures.[10]

Specifically, the act required DHS and DOJ to lead the development of procedures and guidelines to assist federal entities when receiving information on cyber threat indicators or defensive measures from federal and nonfederal entities. The act also required DHS and DOJ to work with DOD and ODNI to develop policies to facilitate the sharing of cyber threat indicators and defensive measures among federal and nonfederal entities. Further, the act required these four agencies to coordinate the development of these artifacts with DOC, DOE and the Treasury. In support of this information sharing, the White House released a memorandum in 2016 stating that all departments and agencies should use DHS's AIS capability for the purpose of sharing cyber threat information.

In addition, the act included specific provisions for the protection of privacy and civil liberties. In this regard, CISA required DHS and DOJ, in coordination with the other five designated federal agencies, to develop government-wide guidelines for the protection of privacy and civil liberties when implementing provisions of the act.

Among other things, the seven designated agencies were to:

[9]The AIS initiative is an automated capability that receives, processes, and disseminates cyber threat indicators and defensive measures in real-time by enabling DHS to receive indicators from federal and nonfederal entities, remove personally identifiable information and other sensitive information not directly related to the cybersecurity threat, and disseminate the cyber threat indicators and defensive measures, as appropriate, to other federal and nonfederal entities.

[10]CISA designated these entities as the appropriate agencies to develop and coordinate regarding the required policies, procedures, and guidance.

- develop privacy and civil liberties guidance governing the receipt, retention, use, and dissemination of cyber threat indicators, consistent with the eight fair information practice principles;

- develop and implement the aforementioned real-time sharing capability in compliance with this privacy and civil liberties guidance; and

- incorporate appropriate security and privacy protections into all other policies, procedures, and guidance for receiving and sharing cyber threat indicators and defensive measures specified in the act.

### Designated Federal Agencies Met Requirements to Develop Policies, Procedures, and Guidelines for Removal of Personal Information

The seven designated federal agencies developed policies, procedures, and guidelines that met the eight CISA provisions relevant to the removal of personal information from cyber threat indicators and defensive measures. Table 1 summarizes these CISA provisions and identifies the government-wide policies, procedures, and guidelines that the designated agencies created to fulfill each provision for the sharing of cyber threat indicators and defensive measures, and the removal of personal information. The table is followed by additional discussion of the provisions and related policies, procedures, and guidance.

**Table 1: Government-wide Policies, Procedures, and Guidelines Created to Fulfill Eight Provisions of the Cybersecurity Information Sharing Act of 2015 Related to the Removal of Personal Information from Cyber Threat Indicators and Defensive Measures**

| CISA section[a] | Requirement | Related policy, procedure, or guidance created by designated agencies |
|---|---|---|
| 103(a) | The Office of the Director of National Intelligence (ODNI), the Department of Defense (DOD), the Department of Justice (DOJ), and the Department of Homeland Security (DHS) are to develop and issue procedures for the timely sharing of cyber threat information to mitigate adverse effects | *Sharing of Cyber Threat Indicators and Defensive Measures by the Federal Government under the Cybersecurity Information Sharing Act of 2015,* February 16, 2016 |
| 103(b) | ODNI, DOD, DOJ, and DHS are to ensure that the secure real-time sharing of cyber threat information excludes personal information not directly related to a cybersecurity threat | *Sharing of Cyber Threat Indicators and Defensive Measures by the Federal Government under the Cybersecurity Information Sharing Act of 2015,* February 16, 2016 |
| 103(c) | Procedures developed shall be issued no later than 60 days after the date of enactment of CISA | *Sharing of Cyber Threat Indicators and Defensive Measures by the Federal Government under the Cybersecurity Information Sharing Act of 2015,* February 16, 2016 |
| 105(a)(1) | DOJ and DHS are to develop interim policies to guide in the receipt of cyber indicators and defensive measures by the federal government | *Interim Procedures Related to the Receipt of Cyber Threat Indicators and Defensive Measures by the Federal Government,* February 16, 2016 |
| 105(a)(2) | DOJ and DHS are to develop final policies to guide in the receipt of cyber indicators and defensive measures by the federal government | *Final Procedures Related to the Receipt of Cyber Threat Indicators and Defensive Measures by the Federal Government,* June 16, 2016 |
| 105(a)(4) | DOJ and DHS are to develop guidance to assist nonfederal entities and promote sharing of cyber | *Guidance to Assist Nonfederal Entities to Share Cyber Threat Indicators and Defensive Measures with Federal Entities under the* |

| CISA section[a] | Requirement | Related policy, procedure, or guidance created by designated agencies |
|---|---|---|
| | threat indicators with federal entities | *Cybersecurity Information Sharing Act of 2015,* February 16, 2016 |
| 105(b)(1) | DOJ and DHS are to develop interim guidelines relating to privacy and civil liberties that governs the receipt, retention, use, and dissemination of cyber threat information and are consistent with fair information practice principles | *Privacy and Civil Liberties Interim Guidelines: Cybersecurity Information Sharing Act of 2015*, February 16, 2016 |
| 105(b)(2) | DOJ and DHS are to develop final guidelines relating to privacy and civil liberties that governs the receipt, retention, use, and dissemination of cyber threat information and are consistent with fair information practice principles | *Privacy and Civil Liberties Final Guidelines: Cybersecurity Information Sharing Act of 2015*, June 16, 2016[b] |

Source: GAO analysis of policies and procedures created by DOD, DOJ, DHS, and ODNI, and in response to CISA.

[a]CISA = Cybersecurity Information Sharing Act of 2015, and can be found at https://www.congress.gov/114/plaws/publ113/PLAW-114publ113.pdf.

[b]In accordance with CISA, DHS and DOJ produced an updated version of this document in June 2018. Changes between the two versions were non-substantial for the purposes of our analysis.

To satisfy subsections 103(a), (b), and (c) of CISA, which called for the development and issuance of procedures for the timely sharing of cyber threat information and defensive measures, DHS, DOJ, ODNI, and DOD, in coordination with the other three agencies designated in the act, developed the procedures in *Sharing of Cyber Threat Indicators and Defensive Measures by the Federal Government under the Cybersecurity Information Sharing Act of 2015*. As required by subsection 103(a), these procedures outline how federal entities are to share classified and unclassified cyber threat indicators and defensive measures in a timely manner and in a way that mitigates adverse effects from cybersecurity threats. For example, the procedures include details on existing government programs that facilitate the sharing of information on cybersecurity threats and the periodic publication of cybersecurity best practices—such as technical security guidelines for federal agency information systems, and recommended practices and references for technical and nontechnical users.

In addition, as required by subsection 103(b), the procedures include information on the existing roles and responsibilities of federal and nonfederal entities when sharing information. The procedures also incorporate requirements related to the security of cyber threat indicators and defensive measures prior to sending them to other entities, in order to assure that federal or nonfederal entities do not share personal information unnecessarily.[11] For example, the guidance includes requirements for notification when a cyber threat indicator or defensive measure is shared in error and for protection against unauthorized access to a cyber threat indicator or defensive measure. Further, as required by subsection 103(c), the designated agencies issued the procedures in less than 60 days after the enactment of the act.

DOJ and DHS met the requirements in sections 105(a)(1) and 105(a)(2) of CISA, which call for the development of policies for the receipt and sharing of cyber threat indicators and defensive measures, including consideration of privacy and civil liberties as a part of the receipt process. Specifically, in coordination with the other five designated federal agencies, these departments developed the interim and final versions of the guidance document, *Procedures Related to the Receipt of Cyber Threat Indicators and Defensive Measures by the Federal Government.* This document describes the processes for receiving, handling, and disseminating cyber threat indicators and defensive measures shared through DHS's AIS, as well as through the

[11]In some cases, personal information directly related to a cybersecurity threat may be shared.

submission of a website form or email.[12] For all federal entities that receive cyber threat indicators and defensive measures, this guidance states and provides context for the statutory requirements for privacy and civil liberties, and for the maintenance of data on the number of cyber threat indicators and defensive measures where personal information concerns were addressed.

DOJ and DHS also addressed the provision in section 105(a)(4) through creation of the *Guidance to Assist Nonfederal Entities to Share Cyber Threat Indicators and Defensive Measures with Federal Entities under the CISA of 2015.* Specifically, the stated intent of this guidance is to assist nonfederal entities in identifying cyber threat information. Further, the guidance explains how to share such information with federal entities through both DHS's AIS and other means authorized by CISA.

In response to requirements in sections 105(b)(1) and 105(b)(2) of CISA, on the development of guidelines for the consideration of privacy and civil liberties when sharing cyber threat indicators, DHS and DOJ, in coordination with the other five designated federal agencies, issued the *Privacy and Civil Liberties Interim Guidelines* and the *Privacy and Civil Liberties Final Guidelines*.[13] These guidance documents govern the receipt, retention, use, and dissemination of cyber threat information. For example, according to the *Final Guidelines*, federal entities should follow requirements to safeguard cyber threat indicators prior to sharing the indicators, including in cases when the shared cyber threat indicators contain specific individuals' personal information or information that identifies specific individuals that is not directly related to a cybersecurity threat.

Beyond the aforementioned provisions, CISA section 105(b) requires that the guidance documents created to fulfill its provisions also address the fair information practice principles as applicable. Table 2 defines the eight fair information practice principles.

**Table 2: Definitions of Fair Information Practice Principles**

| Principle | Definition |
|---|---|
| Transparency | Organizations should be transparent and notify individuals regarding the collection, use, dissemination, and maintenance of personally identifiable information (PII). |
| Individual participation | Organizations should involve the individual in the process of using PII and, to the extent practicable, seek individual consent for the collection, use, dissemination, and maintenance of PII. Organizations should also provide mechanisms for appropriate access, correction, and redress regarding the use of PII. |
| Purpose specification | Organizations should specifically articulate the authority that permits the collection of PII and specifically articulate the purpose or purposes for which the PII is intended to be used. |
| Data minimization | Organizations should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s). |
| Use limitation | Organizations should use PII solely for the purpose(s) specified in the notice. Sharing PII should be for a purpose compatible with the purpose for which the PII was collected. |
| Data quality and integrity | Organizations should, to the extent practicable, ensure that PII is accurate, relevant, timely, and complete. |

[12]The final *Procedures Related to the Receipt of Cyber Threat Indicators and Defensive Measures by the Federal Government* was released in June 2016, replacing the February 2016 interim version.

[13]In accordance with CISA, DHS produced an updated version of this document in June 2018. Changes between the two versions were non-substantial for the purposes of our analysis.

| Principle | Definition |
|---|---|
| Security | Organizations should protect PII (in all media) through appropriate security safeguards. |
| Accountability and auditing | Organizations should be accountable for complying with these principles, providing training to all employees and contractors who use PII, and auditing the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure. |

Source: The White House, *National Strategy for Trusted Identities in Cyberspace* (Washington, D.C.: April 2011).

The *Privacy and Civil Liberties Final Guidelines* fully meets requirements in section 105(b) by addressing all eight fair information practice principles. Specifically, the guidelines do so by establishing or considering the fair information practice principles as the primary guiding principles for all federal entity activities related to the receipt, retention, use, and dissemination of cyber threat indicators, as authorized by CISA. For example:

- *Transparency principle*. The final guidelines state that federal entities are to be transparent about their receipt, retention, use, and dissemination of cyber threat indicators under CISA.

- *Individual participation principle*. The final guidelines state that, given the nature of a cyber threat indicator, an individual whose personal information is directly related to a cybersecurity threat does not have the ability to consent to, or to be involved in, the process used to collect, access, or correct that information.

Each of the other guidance documents refers to the requirements in the *Privacy and Civil Liberties Final Guidelines* as a necessary part of their own requirements.

Finally, DHS's guidance includes other related information on the consideration of the fair information practice principles specifically in support of its implementation of AIS. Specifically, the *Final Procedures Related to the Receipt of Cyber Threat Indicators and Defensive Measures* provides several examples to guide the implementation of fair information practice principles when federal and nonfederal entities use AIS. For example:

- *Purpose specification principle.* The procedures provide guidance to federal entities on using an AIS profile to standardize cyber threat indicator information received while adhering to all relevant privacy and civil liberties requirements.

- *Data minimization principle.* The procedures require nonfederal entity submissions to conform to the defined AIS profile. This ensures that submissions include input fields most directly related to cyber threat indicators. Furthermore, the procedures guide entities to add or delete fields when considering changes to the AIS profile, in compliance with CISA's provisions that are designed to limit the receipt, retention, use, and dissemination of cyber threat indicators containing personal information.

- *Use limitation principle.* The procedures state that failure by federal employees to abide by usage requirements will result in individual sanctions such as loss of access to information and loss of a security clearance.

**Agency Comments**

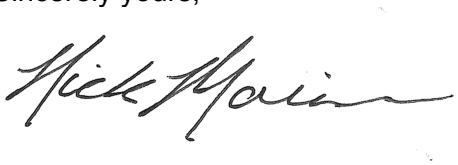
We provided a draft of this report to DHS, DOJ, DOD, DOC, DOE, Treasury, and ODNI for review and comment. DHS, DOJ, and DOD provided technical comments, which we

incorporated into the report as appropriate. The other four agencies stated via email that they had no comments on the draft report.

- - - - -

We are sending copies of this report to the Secretaries of Commerce, Defense, Energy, Homeland Security, and the Treasury; the Attorney General, the Director of National Intelligence, appropriate congressional committees, and other interested parties. In addition, the report is available at no charge on the GAO website at http://www.gao.gov.

If you and your staff have any questions, please contact Nick Marinos at (202) 512-9342 or marinosn@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. Major contributors to this report were Michael Gilmore (assistant director), Shaun Byrnes (analyst-in-charge), Christopher Businsky, Lisa Hardman, James (Andrew) Howard, Richard Sayoc, Priscilla Smith, and Adam Vodraska. Sincerely yours,



Nick Marinos
Director, Cybersecurity & Data Protection Issues
(102626)