OFFICE OF THE INSPECTOR GENERAL OF THE INTELLIGENCE COMMUNITY

Unclassified Joint Report on the Implementation of the Cybersecurity Information Sharing Act of 2015

December 9, 2021 AUD-2021-002-U


INSPECTOR GENERAL
INTELLIGENCE COMMUNITY
INDEPENDENCE • INTEGRITY • PROFESSIONALISM

OFFICE OF THE INSPECTOR GENERAL OF THE INTELLIGENCE COMMUNITY
WASHINGTON, D.C. 20511

MEMORANDUM FOR: See Distribution

SUBJECT: Report No. AUD-2021-002, Joint Report on the Implementation of the Cybersecurity Information Sharing Act of 2015, December 9, 2021

We are providing this summary report for your information and use. Our objective was to provide a joint report on actions taken during calendar years 2019 and 2020 to carry out the requirements of the Cybersecurity Information Sharing Act of 2015.

On December 18, 2015, Congress passed Public Law 114-113, the *Consolidated Appropriations Act, 2016*, which includes Title I – the *Cybersecurity Information Sharing Act of 2015* (the Act). The Act requires the inspectors general of the "appropriate Federal entities," defined as the Departments of Commerce, Defense, Energy, Homeland Security, Justice, and the Treasury, and the Office of the Director of National Intelligence, to jointly report to Congress on the actions taken over the most recent two-year period to carry out the Act. Each of the Offices of Inspector General assessed its agency's implementation of the Act requirements. The Office of the Inspector General of the Intelligence Community compiled the results in this report.

A draft of this report was provided to the Council of Inspectors General on Financial Oversight, and comments were incorporated when preparing this report.

A separate report included For Official Use Only information—*Joint Report on the Implementation of the Cybersecurity Information Sharing Act of 2015* (AUD-2021-002)—and was submitted to the appropriate members of Congress.

We appreciate the courtesies extended to our staffs throughout this review. Please direct questions related to this report to Deborah Carros, Assistant Inspector General for Audit, Office of the Inspector General of the Intelligence Community, at 571-204-8149.

Deborah L. Carros Digitally signed by Deborah L. Carros Date: 2021.12.02 12:50:16 -05'00' 12/2/2021

Deborah L. Carros
Assistant Inspector General for Audit
Office of the Inspector General of the
Intelligence Community

Date

FREDERICK MENY Digitally signed by FREDERICK MENY Date: 2021.12.06 12:52:20 -05'00' 12/6/2021

Frederick J. Meny, Jr.
Assistant Inspector General for Audit and Evaluation
Department of Commerce, Office of Inspector General

Date

MANSFIELD.BRETT.A.1229241709 Digitally signed by MANSFIELD.BRETT.A.1229241709 Date: 2021.12.07 12:14:28 -05'00' 12/7/2021

Brett A. Mansfield
Deputy Inspector General for Audit
Department of Defense, Office of Inspector General

Date

Sarah B. Nelson Digitally signed by Sarah B. Nelson Date: 2021.12.02 14:08:17 -05'00' 12/2/2021

Sarah B. Nelson
Assistant Inspector General for Technology,
Financial, and Analytics
Department of Energy, Office of Inspector General

Date

BRUCE B MILLER II Digitally signed by BRUCE B MILLER II Date: 2021.12.09 06:34:05 -05'00' 12/9/2021

Bruce B. Miller
Deputy Inspector General for Audits
Department of Homeland Security,
Office of Inspector General

Date

12/8/2021

Jason R. Malmstrom
Assistant Inspector General for Audit
Department of Justice, Office of the Inspector General

Date

12/8/2021

Deborah L. Harker
Assistant Inspector General for Audit
Department of the Treasury, Office of Inspector General

Date

Distribution:

Director, National Intelligence
Secretary of Commerce
Secretary of Defense
Secretary of Energy
Secretary of Homeland Security
Attorney General, Department of Justice
Secretary of the Treasury

TABLE OF CONTENTS

REPORT *in* BRIEF

UNCLASSIFIED JOINT REPORT ON THE IMPLEMENTATION OF THE CYBERSECURITY INFORMATION SHARING ACT OF 2015 (AUD-2021-002-U)

WHY WE DID THIS REVIEW

On December 18, 2015, Congress passed Public Law 114-113, the *Consolidated Appropriations Act, 2016*, which includes Title I – the *Cybersecurity Information Sharing Act of 2015* (the Act).[1] The Act creates a framework to facilitate and promote voluntary sharing of cyber threat indicators (CTIs)[2] and defensive measures (DMs)[3] among and between Federal and non-Federal entities.[4]

The Act requires the Inspectors General of the "appropriate Federal entities," defined as the Departments of Commerce, Defense, Energy, Homeland Security, Justice, and the Treasury, and the Office of the Director of National Intelligence (ODNI), "in consultation with the Inspector General of the Intelligence Community and the Council of Inspectors General on Financial Oversight," to jointly report to Congress by December 18—every two years—on the actions taken over the most recent two-year period to carry out the Act (*see* the Background of this report for the specific areas to be addressed in the report).[5] This report meets the joint, biennial reporting requirement.

The Offices of the Inspectors General (OIG) of the Departments of Commerce, Defense, Energy, Homeland Security, Justice, and the Treasury, and Intelligence Community assessed the implementation of the Act for calendar years (CY) 2019 and 2020 for their respective entities.

[1] The *Cybersecurity Information Sharing Act of 2015* is codified at 6 U.S.C. §§ 1501-1510.

[2] According to 6 U.S.C. § 1501(6), CTIs include, but are not limited to, 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.

[3] According to 6 U.S.C. § 1501(7)(A), DM generally means an action, device, procedure, technique, or other measure applied to an information system or information that is stored on, processed by, or transiting an information system that detects, prevents, or mitigates a known or suspected cybersecurity threat or vulnerability.

[4] A Federal entity is a department or agency of the United States or any component of such department or agency. *See* 6 U.S.C. § 1501(8). Non-Federal entities include state, local, and tribal governments; private sector companies; and academic institutions. *See* 6 U.S.C. § 1501(14). Federal entities can share cybersecurity information with one another and with non-Federal entities, and non-Federal entities can share cybersecurity information with one another and with Federal entities. *See generally* 6 U.S.C. § 1502(a).

[5] 6 U.S.C. § 1506(b)(1).

WHAT WE FOUND

The OIGs determined that CTI and DM sharing has improved over the past two years, and efforts are underway to expand accessibility to information. Sharing CTIs and DMs increases the amount of information available for defending systems and networks against cyber attacks. In April 2017, ODNI's Intelligence Community Security Coordination Center (IC SCC) deployed a capability—the Intelligence Community Analysis and Signature Tool (ICOAST)—to increase cybersecurity threat intelligence sharing, including Indicators of Compromise[6] and malware signatures.[7] Additionally, in January 2020, the IC SCC deployed an unclassified version of ICOAST—ICOAST-U. CTIs are integrated into ICOAST through manual entry of information obtained from open, Federal Government, or intelligence sources; automated ingestion of commercial data feeds; or automated machine-to-machine ingestion. Also, the Automated Indicator Sharing (AIS) capability, developed by the Department of Homeland Security in 2016, enables the timely exchange of CTIs and DMs among the private sector; state, local, tribal and territorial governments; and the Federal Government. In CY 2019 and CY 2020, entities continued to share cyber threat information through various reporting means, including email, written reports, websites, and face-to-face communications.

Concerning the specific areas that the Act requires the OIGs assess and report, the auditors determined that the "appropriate Federal entities" continue to implement the Act.[8] Specifically, the OIGs determined that the "appropriate Federal entities" responsible for sharing, receiving, or disseminating cyber threat information:

- Use policies and procedures that are sufficient (with the exception of Commerce and four Department of Defense (DoD) components).
- Properly classify CTIs and DMs when classified information was shared.
- Authorize security clearances for the specific purpose of sharing CTIs or DMs with the private sector, as needed.
- Appropriately disseminate cyber threat information that had been shared by Federal and non-Federal entities, and appropriately used that information.
- Share CTIs and DMs in a timely and adequate manner and with appropriate entities (with the exception of Commerce who only shared CTIs and DMs when required to do so).
- Receive CTIs and DMs in a timely and adequate manner.
- Use the Department of Homeland Security capability—AIS—to receive CTIs or DMs, with the exception of three DoD components and ODNI.

[6] Indicators of Compromise are data or evidence found in system log entries or files that indicate potentially malicious activity on a system or network.

[7] Malware signatures are unique values that indicate the presence of malicious code.

[8] *See* 6 U.S.C. § 1506(b)(2) (identifying the areas to be assessed and reviewed, and included in the biennial report on compliance).

- Did not receive information that was unrelated to a cybersecurity threat that included personal information of a specific individual or information identifying a specific individual.
- Did not receive notices due to a failure to remove information not directly related to a cybersecurity threat that was personal information of a specific individual.
- Did not need to take steps to minimize adverse effects on the privacy and civil liberties of United States persons from activities carried out under the Act because there were no known adverse effects.
- Identified barriers that have hindered sharing CTIs and DMs.

WHAT WE RECOMMEND

This report does not include any constructive findings or recommendations.

BACKGROUND

CYBERSECURITY INFORMATION SHARING ACT OF 2015

On December 18, 2015, Congress passed Public Law 114-113, the *Consolidated Appropriations Act, 2016*, which includes Title I – the *Cybersecurity Information Sharing Act of 2015* (the Act).[9] The Act was established to improve cybersecurity in the United States (U.S.) through enhanced sharing of cyber threat information.[10] The Act creates a framework to facilitate and promote voluntary cyber threat indicator (CTI) [11] and defensive measures (DMs)[12] sharing among and between Federal and non-Federal entities.[13]

The Act required the Department of Homeland Security (DHS) to establish a capability and process for Federal entities to receive cyber threat information from non-Federal entities. The Act designated seven Federal entities—the Departments of Commerce, Defense, Energy, Homeland Security, Justice, and the Treasury, and the Office of the Director of National Intelligence (ODNI)—to coordinate and develop publicly available policies, procedures, and guidance to assist Federal and non-Federal entities in their efforts to receive and share CTIs and DMs.

Other key provisions in the legislation include liability protection for private entities that share cybersecurity information in accordance with established procedures, and the protection of privacy and civil liberties when implementing the Act. Specifically, the Act calls for the removal of information not directly related to a cybersecurity threat that is known at the time of sharing to be personal information of a specific individual or information that identifies a specific individual.[14] The Act does not create any duty to share CTIs or DMs and does not impose a duty to warn or act based on the receipt of shared information. Subject to exceptions, the Act will sunset on September 30, 2025.

OFFICES OF INSPECTORS GENERAL REPORTING REQUIREMENT

Section 1506(b) of the Act requires the Inspectors General of the "appropriate Federal entities," defined as the Departments of Commerce, Defense, Energy, Homeland Security, Justice, and the Treasury, and the ODNI, "in consultation with the Inspector General of the Intelligence Community and the Council of Inspectors General on Financial Oversight," to jointly

[9] *See supra* note 1.

[10] "Cybersecurity threat" is broadly defined to include an action on or through an information system that may result in an unauthorized effort to adversely impact the security, availability, confidentiality, or integrity of an information system. *See* 6 U.S.C. § 1501(5). The term "cyber threat information" is used in this report to refer to both cyber threat indicators and defensive measures.

[11] *See supra* note 2.

[12] *See supra* note 3.

[13] *See supra* note 4.

[14] The Act speaks to the removal of "personal information" from CTIs. *See* 6 U.S.C. §§ 1503(d)(2), 1504(b)(3). This information is commonly referred to as personally identifiable information (PII).

report to Congress by December 18—every two years—on the actions taken over the most recent two-year period to carry out the Act.[15] Section 1506(b) of the Act requires the biennial report to include an assessment that determines:

- The sufficiency of policies and procedures related to sharing CTIs within the Federal Government.
- Whether CTIs and DMs have been properly classified, as well as an accounting of the security clearances authorized for the purpose of sharing CTIs or DMs with the private sector.
- The appropriateness, adequacy, and timeliness of the actions taken to use and disseminate CTIs or DMs shared with the Federal Government.
- Specific aspects of CTIs or DMs that have been shared with the Federal Government, including:
    - The number of CTIs or DMs shared using the capability implemented by the DHS.
    - Instances in which any Federal or non-Federal entity shared information that was not directly related to a cybersecurity threat and contained Personally Identifiable Information (PII).
    - The number of times, according to the Attorney General, that information shared under the Act was used by a Federal entity to prosecute an offense listed in section 1504(d)(5)(A).[16]
    - The effect of sharing CTIs or DMs with the Federal Government on privacy and civil liberties of specific individuals, including the number of notices that were issued with respect to a failure to remove information not directly related to a cybersecurity threat that contained PII.
    - The adequacy of steps taken by the Federal Government to reduce any adverse effect from activities carried out under the Act on the privacy and civil liberties of U.S. persons.
- Barriers affecting the sharing of CTIs or DMs. [17]

[15] *See supra* note 5.

[16] According to 6 U.S.C § 1504(d)(5)(A), cyber threat information provided to the Federal Government may be used by the Federal Government to prosecute a serious threat to a minor or an offense arising out of a specific threat of serious economic harm, including a terrorist act or use of a weapon of mass destruction.

[17] *See supra* note 8.

ENTITIES REVIEWED

The Offices of Inspectors General (OIGs) reviewed their agencies' components responsible for sharing, receiving, or disseminating CTIs and DMs during Calendar Year (CY) 2019 and CY 2020 as follows:

Department of Commerce (Commerce). Commerce has many bureaus within its organizational structure. The Security Operation Centers (SOCs) at the bureaus vary in size and maturity. The Enterprise SOC (ESOC) serves as the focal point for many security operation activities, including cyber threat information sharing. The ESOC maintains the Commerce Threat Intelligence Portal for internal sharing among ESOC and the Commerce bureaus.

Department of Defense (DoD). The following eight DoD components are responsible for sharing cyber threat information with Federal and non-Federal entities. Each DoD component plays a role in sharing cyber threat information based on its mission. Specifically:

- The DoD Cyber Crime Center (DC3) is a DoD cyber center for digital and multimedia forensic services, cyber technical training, vulnerability sharing, and cyber analytics. DC3, the operational focal point for the Defense Industrial Base (DIB) Cybersecurity Program—led by the DoD Office of the Chief Information Officer— analyzes, produces, and distributes cyber products to the DIB, DoD, and Federal Government stakeholders that contain actionable cyber threat information.

- The Defense Intelligence Agency (DIA) is a combat support agency that produces, analyzes, and disseminates military intelligence information to combat and non-combat military missions. The DIA serves as the U.S.'s primary manager and producer of foreign military intelligence and is a central intelligence producer and manager for the Secretary of Defense, the Joint Chiefs of Staff, and the Unified Combatant Commands.

- The Defense Information Systems Agency (DISA) is a combat support agency that plans, engineers, tests, fields, and operates information sharing capabilities for joint warfighters, national-level leaders, and other mission and coalition partners across DoD operations.

- The Defense Counterintelligence and Security Agency (DCSA) provides security and counterintelligence support services to the DoD and law enforcement, Intelligence Community (IC) partners, and cleared contractors. The DCSA performs background investigations for branches of the Government to secure the trustworthiness of the Federal Government's workforce, the integrity of its cleared contractor support, and the nature of its technologies, services, and supply chains.

- The National Geospatial-Intelligence Agency (NGA) is a combat support agency that provides geospatial intelligence for U.S. security. The NGA leads the Federal Government in managing, monitoring, analyzing, and reporting imminent threats to geospatial intelligence.

- The National Reconnaissance Office (NRO) designs, builds, launches, and maintains intelligence satellites. The NRO provides global communications, precision navigation, early warning of missile launches, signals intelligence, and near real-time imagery to the DoD to support the war on terrorism and other continuing operations.

- The National Security Agency (NSA) is a combat support agency that leads the Federal Government in cryptology for signal intelligence and cybersecurity products and services. The NSA enables computer network operations to gain an advantage for the U.S. against its adversaries.

- The U.S. Cyber Command (USCYBERCOM) is a combatant command that defends DoD information networks, provides support to combatant commanders, and strengthens the ability to withstand and respond to cyberattacks. In addition, USCYBERCOM works to improve DoD's capabilities to operate resilient, reliable information and communication networks; counter cyberspace threats; and assure access to cyberspace.

Department of Energy (DOE). Two components within DOE are responsible for sharing cyber threat information. The Integrated Joint Cybersecurity Coordination Center is responsible for sharing CTIs and DMs within DOE and with other Federal entities. The Office of Cybersecurity, Energy Security, and Emergency Response is responsible for sharing CTIs and DMs with the private sector.

DHS. DHS's Cybersecurity and Infrastructure Security Agency leads the national effort to protect critical infrastructure and further cybersecurity by working with partners across all levels of government and in the private sector to promote information sharing. The Cybersecurity and Infrastructure Security Agency manages the Automated Indicator Sharing (AIS) capability, which enables the real-time exchange of CTIs and DMs between government entities and private sector partners to identify and help mitigate cyber threats.

Department of Justice (DOJ). Two components within the DOJ are responsible for sharing cyber threat information. The DOJ Chief Information Officer delegates responsibility for incident response to the Justice Security Operations Center (JSOC). JSOC works with DOJ components to prevent, detect, and respond to cyber attacks and espionage against the Department. JSOC shares CTIs with other Federal entities and the private sector. The National Cyber Investigative Joint Task Force (NCIJTF)—within the Federal Bureau of Investigation (FBI) Cyber Division—serves as a multi-agency national focal point for coordinating, integrating, and sharing cybersecurity threat information with other Federal entities.

Office of the Director of National Intelligence. ODNI and its service provider are responsible for information security services for systems and networks ODNI uses. The following two components within ODNI shared and received cyber threat information with other Federal entities.

- The Intelligence Community Security Coordination Center (IC SCC), a Federal Cybersecurity Center, coordinates the integrated defense of the IC Information Technology Enterprise and IC Information Environment, including continuous coordination and review of cybersecurity related information, events, and incidents to enable correlated enterprise cybersecurity situational awareness across the IC. The

IC SCC coordinates activities for the integrated defense of the IC Information Environment with IC elements, the DoD, and other Federal Government departments and agencies.

- The Cyber Threat Intelligence Integration Center builds understanding of foreign cyber threats to U.S. national interests to inform Federal cyber centers, departments and agencies, and policymaker decision making; integrates network defense, intelligence, and law enforcement communities' information; facilitates information sharing; leads community analysis of cyber threats; and supports interagency planning to develop whole-of-government approaches against cyber adversaries.

Department of the Treasury. Two components within the Department of the Treasury, the Government Security Operations Center (GSOC)[18] and the Office of Cybersecurity and Critical Infrastructure Protection (OCCIP), are responsible for sharing CTIs for Treasury. Treasury's GSOC is a 24-hour, 365-day Treasury-wide incident response and security operations team focused on the detection and mitigation of advanced threats targeted against the Department, its users, and information technology systems. Treasury's GSOC acts as the centralized coordination point for Treasury bureau cyber incidents and is the liaison with the DHS U.S. Computer Emergency Readiness Team and other Federal agency incident response teams. Treasury's OCCIP coordinates Treasury's efforts to enhance the security and resilience of the Financial Services Sector's critical infrastructure and reduce operational risk. OCCIP works closely with financial sector companies, industry groups, and government partners to share information about cybersecurity and physical threats and vulnerabilities; encourage the use of baseline protections and best practices; and respond to and recover from significant incidents.

[18] As of June 2021, GSOC was renamed the Treasury Shared Services Security Operations Center. The report refers to GSOC for consistency since the name change was made after the audit scope period of CY 2019 and CY 2020.

SHARING OF CYBER THREAT INDICATORS AND DEFENSIVE MEASURES HAS IMPROVED OVER THE PAST TWO YEARS AND EFFORTS ARE UNDERWAY TO EXPAND ACCESSIBILITY TO INFORMATION

PROGRESS IN SHARING CYBER THREAT INFORMATION AMONG FEDERAL ENTITIES

In CY 2019 and CY 2020, the Federal entities reviewed made progress enhancing accessibility to cyber threat information for improved information sharing with other Federal entities. Sharing CTIs and DMs increases the amount of information available for defending systems and networks against cyber attacks.

In April 2017, ODNI's IC SCC deployed the Intelligence Community Analysis and Signature Tool (ICOAST) to increase cybersecurity threat intelligence sharing, including Indicators of Compromise[19] and malware signatures.[20] Additionally, in January 2020, the IC SCC deployed an unclassified version of ICOAST—ICOAST-U. An IC SCC official stated that the IC SCC developed an automated process to move indicators from ICOAST-U to populate ICOAST, but the movement of Unclassified//For Official Use Only events and indicators from ICOAST to ICOAST-U requires manual review before loading the information into a weekly transfer. The official stated that the ICOAST and ICOAST-U have similar sharing and population processing through machine to machine transfers, crowdsourcing, and commercial data feeds. Cyber threat indicators are integrated into ICOAST through manual entry of information obtained from open, Federal Government, or intelligence sources; automated ingestion of commercial data feeds; or automated machine-to-machine ingestion. ICOAST users can download DMs into a report for immediate action. ICOAST also produces correlation reports that aggregate technical data, such as Indicators of Compromise, and provide insight to previously unknown threat actors' tactics, techniques, and procedures (TTPs). Six of the Federal entities reviewed—Commerce, DoD (DC3, DCSA, DIA, NGA, NRO, and USCYBERCOM), DOE, DOJ, Treasury, and ODNI—received cyber threat information from ICOAST. Additionally, the DoD (DC3, DISA, NSA, and USCYBERCOM) and DOE shared cyber threat information via DHS's AIS capability. IC SCC officials told Intelligence Community Inspector General (IC IG) auditors that, in 2020, IC SCC and AIS exchanged manual data feeds of cyber threat indicators to prepare for subsequent automated exchanges of indicators, and IC SCC is working with DHS's Cybersecurity and Infrastructure Security Agency to facilitate an interface with AIS and ICOAST in 2021.

Various websites increased the amount of shared cybersecurity information in CY 2019 and CY 2020. IC SCC maintains a website on a top secret network containing various reports on cyber threats, vulnerabilities, and mitigation information. Reports and other products specifically related to cybersecurity that are available on the website include: ICOAST Correlation Reports, Tippers,[21] situational awareness reports, malicious activity reports, monthly activity reports,

[19] *See supra* note 6.

[20] *See supra* note 7.

[21] IC SCC Tippers contain time-sensitive technical information on a variety of issues that may impact the security of the Intelligence Community.

vulnerability reports, network activity notices, and blogs. Also, cybersecurity products are available on the NSA Pulse website for users with appropriate security clearances to access the network on which the website is maintained, and the Defense Industrial Base Net and Homeland Security Information Network web portals.

CONTINUING EFFORTS TO SHARE CYBER THREAT INFORMATION

The Federal entities reviewed continue to share cyber threat information through various reporting means, including email, written reports, websites, and face-to-face communications. Specifically:

- ODNI, its service provider, and DOJ (FBI/NCIJTF) share cyber threat information via email distributions. For example, IC SCC provides email alerts of critical cyber security vulnerabilities requiring immediate attention to officials within the IC that include details on how to obtain related DMs. Additionally, multiple cyber threat-related reports are available on the IC SCC website.
- ODNI's Cyber Threat Intelligence Integration Center produces a weekly cyber security threat digest and an annual threat report that highlights aspects of cyber threats that were new or noteworthy during the year.
- During CY 2019 and CY 2020, Treasury (GSOC and OCCIP) developed 9 Treasury Early Warning Indicators (TEWIs)[22] and 15 Circulars[23] related to CTIs and DMs. The TEWIs and Circulars are shared via internal and external web portals.
- Commerce, DOE, DHS, DOJ, the Treasury (GSOC), and five DoD components—DC3, DCSA, DISA, NSA, and USCYBERCOM—used the AIS capability to share or receive cyber threat information.
- ODNI's IC SCC designs and conducts ICE STORM, an annual cyber security exercise. A goal of the ICE STORM exercise is to share cyber information with participants from IC elements, DoD, and law enforcement, as well as with international partners.

PRIVATE SECTOR SHARING OF CYBER THREAT INDICATORS AND DEFENSIVE MEASURES USING THE AUTOMATED INDICATOR SHARING CAPABILITY

DHS developed AIS in 2016 to comply with the requirements of the Act. AIS enables the timely exchange of CTIs and DMs among the private sector; state, local, tribal, and territorial governments; and the Federal Government. DHS officials stated that DHS shares cyber threat information with more than 300 AIS partners. Of the AIS partners, 52 are Federal departments and agencies, such as the Departments of Agriculture, Commerce, Defense, Education, Energy, Health and Human Services, Housing and Urban Development, Justice, Transportation, Treasury, and Veteran Affairs; and the National Aeronautics and Space Administration, National Science Foundation, and Nuclear Regulatory Commission.

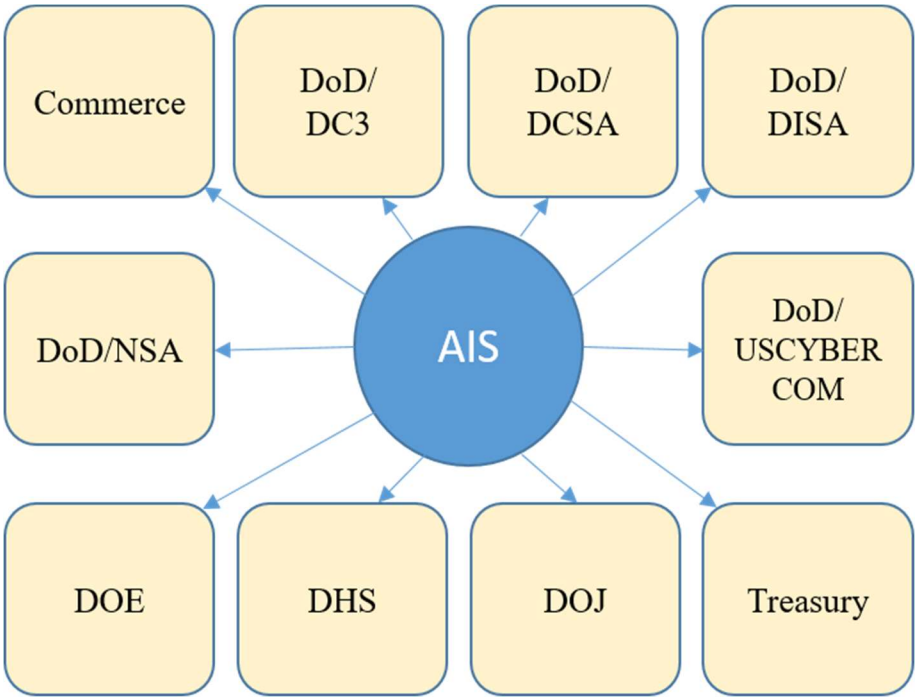
[22] A TEWI is a document that includes a brief description of the event and other details, such as source Internet Protocol (IP) addresses, timestamps, and attachments from relevant tickets.

[23] Circulars are created by OCCIP to share timely, actionable cybersecurity information with partner agencies related to the Financial Services Sector and other critical infrastructure partner organizations to assist in their network defense capabilities and planning. Contents of a Circular include the purpose, a summary of the information being provided, and the details.

According to DHS officials, some Federal entity representatives expressed concerns regarding distribution of information outside of certain "communities." For example, some Federal entities were open to sharing with the private sector but were concerned with sharing with the international community. The AIS public feed has some level of participation from the international community.

The figure below illustrates the Federal entities reviewed and their components who received cyber threat information from the private sector through AIS in CY 2019 and CY 2020.

Figure 1: Federal Entities Reviewed and Their Components That Receive AIS Data



Source: IC IG auditor-generated based on information obtained by the OIGs.

AIS and ICOAST-U are not the only capabilities that allow sharing of cyber threat information between Federal entities and the private sector. Other capabilities include the following:

- DHS's Cyber Information Sharing and Collaboration Program enables actionable, timely unclassified information exchange through trusted public-private partnerships across all critical infrastructure sectors. Cyber Information Sharing and Collaboration Program partners have access to DHS and Integrated Operations Division services. Analyst-to-analyst sharing of threat and vulnerability information allows partners to proactively detect, prevent, mitigate, respond to, and recover from cybersecurity incidents.

- DOE's Cybersecurity Risk Information Sharing Program, managed by the Electricity Information Sharing and Analysis Center since 2014, is a platform for energy sector owners and operators to voluntarily share threat information in near-real time. DOE analysts identify threat patterns and attack indicators across the energy industry and

share the information using the Cybersecurity Risk Information Sharing Program. Electric utilities participating in the program account for more than 80 percent of U.S. electric customers.

- DoD's DIB Cybersecurity Program is a voluntary public-private cybersecurity partnership in which DoD and participants share cyber threat information, and mitigation and remediation strategies. The DoD established the DIB Cybersecurity Program to enhance and supplement DIB participants' capabilities to safeguard DoD information that resides or is transmitted on DIB unclassified networks or information systems. This public-private cybersecurity partnership is designed to improve DIB network defenses, reduce damage to critical programs, and increase DoD and DIB cyber situational awareness.
- Commercial-off-the-shelf automated tools receive and process indicator information. These tools provide a global threat sharing platform for information sharing and analysis centers and organizations, industry groups, and other threat intelligence sharing communities seeking secure collaboration.

RESULTS FOR OVERSIGHT OF GOVERNMENT ACTIVITIES

The Act requires the OIGs of the "appropriate Federal entities" to assess specific areas concerning the implementation of the Act, as follows:[24]

SUFFICIENCY OF POLICIES AND PROCEDURES

The Act requires the OIGs to assess:

> the sufficiency of policies, procedures, and guidelines relating to the sharing of cyber threat indicators within the Federal Government, including the policies, procedures, and guidelines relating to the removal of information not directly related to a cybersecurity threat that is personal information of a specific individual or information that identifies a specific individual.[25]

The OIGs determined that the policies, procedures, and guidelines the Federal entities reviewed used for sharing CTIs within the Federal Government were sufficient, with the exception of the Department of Commerce and four DoD components (*see* Table 1 for details).

Policies and procedures establish the processes and boundaries within which an organization should be operating. The Act designated seven Federal entities—the Departments of Homeland Security, Justice, Defense, Commerce, Energy, and the Treasury, and the ODNI—to coordinate and develop publicly-available policies, procedures, and guidance to assist Federal and non-Federal entities in their efforts to receive and share CTIs and DMs consistent with the protection of classified information, intelligence sources and methods, and privacy and civil liberties.[26] In response to the Act, the following four documents were developed and publicly issued:

- *Final Procedures Related to the Receipt of Cyber Threat Indicators and Defensive Measures by the Federal Government* (June 2016) provides a process for receiving, handling, and disseminating information shared with and from DHS, primarily through the use of the AIS capability. (Document 1)
- *Privacy and Civil Liberties Final Guidelines: Cybersecurity Information Sharing Act of 2015* (June 2018, updated January 2021) addresses limiting the impact on privacy and civil liberties in the receipt, retention, use, and dissemination of cyber threat information. (Document 2)
- *Guidance to Assist Non-Federal Entities to Share Cyber Threat Indicators and Defensive Measures with Federal Entities under the Cybersecurity Information Sharing Act of 2015* (June 2016, updated October 2020) assists non-Federal entities with sharing CTIs and DMs with Federal entities and describes the protections non-Federal entities receive under the Act. (Document 3)
- *Sharing of Cyber Threat Indicators and Defensive Measures by the Federal Government under the Cybersecurity Information Sharing Act of 2015* (February 2016) facilitates and promotes the timely sharing of classified and unclassified CTIs and

[24] *See supra* note 8.

[25] 6 U.S.C. § 1506(b)(2)(A).

[26] *See* 6 U.S.C. § 1502(a).

DMs. The procedures include details on existing government programs that facilitate sharing information on cybersecurity threats and the periodic publication of cybersecurity best practices. (Document 4)

Section 1504(d)(5)(C) of the Act requires that the CTIs and DMs provided to the Federal Government under the Act be retained, used, and disseminated in accordance with Documents 1 and 2. The entities are not required to use Document 3 because this guidance is specific to and for use by non-Federal entities. The use of Document 4 is not required by the Act. Document 4 explicitly states that its purpose is to facilitate and promote the sharing of cyber threat information among and between Federal and non-Federal entities. Instead, some entities used the *Federal Multilateral Information Sharing Agreement* (January 2019). The purpose of this Agreement is to enhance cybersecurity information sharing among Federal entities and to improve cyber situational awareness across all classification domains by using machine-speed sharing of cybersecurity information. The agreement establishes information sharing responsibilities—such as protecting data that is shared from unauthorized access, disclosure, and compromise—for Federal entity participants. The goal is to establish cross-government cybersecurity information sharing that enables integrated operational action.

The Act required the Government Accountability Office (GAO) to submit a report to Congress, not later than three years after the date of the Act's enactment, that assessed the sufficiency of the policies, procedures, and guidelines established under the Act in addressing concerns relating to privacy and civil liberties.[27] In December 2018, GAO submitted a report to Congress.[28] According to its report, GAO reviewed the policies, procedures, and guidelines issued in response to the Act's provisions and concluded that ODNI and the six other designated Federal agencies developed policies, procedures, and guidelines that met all of the Act's provisions relevant to the removal of personal information from CTIs and DMs.

DHS and DOJ used Documents 1 and 2; DHS and DOJ auditors relied on GAO's assessment that these policies, procedures, and guidelines were sufficient. The entities included in Table 1 use agency-specific policies, procedures, and guidelines instead of Documents 1 and 2. The agencies' auditors reviewed the agency-specific policies, procedures, and guidelines to determine whether they were sufficient.[29] The results of the auditors' assessments are provided in Table 1.

[27] 6 U.S.C. § 1506(c).

[28] GAO report, *Cybersecurity: Federal Agencies Met Legislative Requirements for Protecting Privacy When Sharing Threat Information,* dated December 6, 2018 (GAO-19-114R).

[29] "Sufficient" means that the policies, procedures, and guidelines used in place of Document 1 address audit capabilities regarding the receipt of cyber threat information shared by any non-Federal entity and appropriate sanctions for individuals who knowingly and willfully conduct activities under the Act in an unauthorized manner. When used in place of Document 2, "sufficient" means that the policies, procedures, and guidelines address safeguarding and removing PII, and notifying entities when information received under the Act did not constitute a cyber threat.

Table 1. Assessment of Agency-specific Documents Used to Govern Information Sharing Activities

Entity Name	Agency-specific Policies, Procedures, and Guidelines Assessed as Sufficient by the Auditors	Comment
Commerce	No	The Commerce OIG reviewed the Department's policies, procedures, and guidelines relating to CTI and DM sharing activities and found they did not fully comply with the Act. For example, the policies, procedures and guidelines did not include guidance for removing PII not directly related to a cybersecurity threat. Commerce is in the process of updating outdated policies and drafting new policies and procedures.
DoD/DC3	Yes	DC3, NRO, NSA, and USCYBERCOM developed policies, procedures, and guidelines that were sufficient and complied with the Act.
DoD/DIA **DoD/DISA** **DoD/DCSA** **DoD/NGA**	No	DISA, DIA, DCSA, and NGA guidance did not include procedures for notifying Federal entities that they received cyber threat indicators containing known errors from other Federal entities. DISA guidance also did not identify the security controls required by the Act to protect against unauthorized access to CTIs and DMs. DIA and DCSA guidance did not include procedures for notifying individuals that their personal information was shared as part of a CTI or DM. In addition, DISA, DIA, and DCSA guidance did not include procedures for PII not directly related to a cybersecurity threat.
DOE	Yes	DOE's policies, procedures, and guidelines were sufficient and complied with the guidance in the Act.
ODNI	Yes	ODNI and its service provider use sufficient agency-specific guidance for handling PII. ODNI and its service provider do not use Document 1 because they do not receive CTIs from AIS.

Entity Name	Agency-specific Policies, Procedures, and Guidelines Assessed as Sufficient by the Auditors	Comment
Treasury	Yes	GSOC and OCCIP use sufficient agency-specific policies, procedures, and practices that align with the guidance in the Act.

Source: IC IG auditor-generated based on information obtained by the OIGs.

The Act requires the Attorney General and the Secretary of Homeland Security, in coordination with the heads of the "appropriate Federal entities," to periodically review, at least once every two years, the guidelines relating to privacy and civil liberties.[30] The guidelines on privacy and civil liberties were updated in January 2021.

PROPER CLASSIFICATION OF CYBER THREAT INDICATORS AND DEFENSIVE MEASURES, AND AUTHORIZATION OF SECURITY CLEARANCES

The Act requires "an assessment of whether cyber threat indicators or defensive measures have been properly classified and an accounting of the number of security clearances the Federal Government authorized for the purpose of sharing cyber threat indicators and defensive measures with the private sector."[31] The OIGs determined that the entities properly classified CTIs and DMs when necessary. Proper classification of documents protects intelligence information and allows appropriate dissemination and use.

Proper Classification of Cyber Threat Indicators and Defensive Measures

ODNI, its service provider, and DHS properly classify CTIs and DMs. Based on the auditors' testing of a sample of CTIs and DMs, the documents had appropriate portion marks and overall classifications were consistent with the sources, references, or embedded links used for the content. According to DHS and ODNI officials, when classifying cybersecurity information, they either retain the original classification of the information received or classify the information using the appropriate classification guides prior to sharing the information.

Commerce, DoD, DOE, DOJ, and the Treasury OIGs did not determine whether the shared cyber threat information was properly classified because the Department or component did not share classified CTIs or DMs with the private sector or did not classify CTIs or DMs.

[30] 6 U.S.C. § 1504(b)(2)(B).

[31] 6 U.S.C. § 1506(b)(2)(B).

The Treasury's OCCIP held classified meetings for sharing cybersecurity information with Financial Services Sector officials who already have active security clearances issued by DHS's Private Sector Clearance Program for Critical Infrastructure. The information discussed at the classified meetings is not actionable; therefore, the information is not re-disseminated. Treasury's OCCIP retains the original classification of information received.

Authorization of Security Clearances

DHS and DOJ accounted for the number of security clearances authorized for the purpose of sharing cyber threat information with the private sector.[32]

- DHS authorized 200 security clearances in CY 2019 and 274 in CY 2020 to private sector partners participating in DHS's various information sharing programs.
- DOJ (FBI) authorized 37 security clearances in CY 2019 and 24 in CY 2020 for sharing cyber threat information with private sector individuals. Under certain operational circumstances, the FBI authorizes short-term access to classified information for private sector partners after they undergo an abbreviated background investigation.

Commerce, DoD, DOE, the Treasury, and ODNI did not authorize security clearances for the purpose of sharing cyber threat information with the private sector.

- Commerce and DoD did not share classified CTIs or DMs with the private sector.
- DOE did not authorize security clearances expressly for the purpose of sharing CTIs and DMs with the private sector.
- ODNI did not share classified cyber threat information with the private sector, and ODNI's service provider may share classified cyber threat information with private sector officials who already have the appropriate security clearances.
- Treasury did not authorize security clearances for the purpose of sharing cyber threat information with the private sector. The Treasury's OCCIP holds classified meetings to share cyber threat information with Financial Services Sector officials who already have the appropriate security clearances issued by DHS's Private Sector Clearance Program for Critical Infrastructure.

[32] Entities that authorize security clearances conduct an investigation of persons who are proposed for access to classified information to ascertain whether such persons satisfy the criteria for obtaining and retaining access to such information.

The Act requires "a review of the actions taken by the Federal Government based on cyber threat indicators or defensive measures shared with the Federal Government," to include the appropriateness of dissemination and use of the cyber threat information and "whether the cyber threat indicators or defensive measures were shared in a timely and adequate manner with appropriate entities, or, if appropriate, were made publicly available."[33]

Appropriate Dissemination and Use of Cyber Threat Information

The OIGs determined that the Federal entities appropriately disseminated and/or used CTIs or DMs shared by Federal entities. Upon receipt of information other Federal and non-Federal entities shared, the Federal entities disseminated relevant information to entity officials. Cyber threat information is considered appropriately disseminated when the information is shared with individuals having the proper security clearance, and when the information does not contain PII. Use of cyber threat information is considered appropriate when the information is applied for the intended purpose of mitigating a threat. The agencies' auditors tested shared cyber threat information to verify appropriate dissemination within the entities and subsequent use. The results of the testing are summarized in Table 2.

Table 2. Auditor Testing Results for Entity Dissemination and Use of Cyber Threat Information

Entity	Information Disseminated and Used Was Assessed Appropriate by the Auditors	Dissemination and Use of Cyber Threat Information
Commerce	Yes	Commerce disseminated shared cyber threat information internally to the bureaus using the Commerce Threat Intelligence Portal. Each bureau can also upload CTIs and DMs to the portal. Commerce used the ingested cyber threat information to mitigate threats if they provided relevant and sufficient information for action.
DoD	Yes	Seven DoD components—DC3, DCSA, DIA, NGA, NRO, NSA, and USCYBERCOM—used CTIs and DMs shared by other Federal agencies. The DC3 disseminated the cyber threat information shared by other Federal agencies. DISA only received CTIs from AIS.
DOE	Yes	DOE connected to AIS every 15 minutes and downloaded the cyber threat data for redistribution across the enterprise and to private sector entities.

[33] 6 U.S.C. § 1506(b)(2)(C).

Entity	Information Disseminated and Used Was Assessed Appropriate by the Auditors	Dissemination and Use of Cyber Threat Information
DHS	Yes	DHS shared unclassified indicators via AIS to help Federal agencies protect their networks and improve their cybersecurity posture.
DOJ	Yes	DOJ disseminated shared cyber threat information to their components through automated and monitoring tools.
ODNI	Yes	ODNI and its service provider disseminated shared cyber threat information using email and websites.
Treasury	Yes	GSOC disseminated shared cyber threat information by issuing TEWIs related to threats detected against Treasury's network and distributed them within Treasury.

Source: IC IG auditor-generated based on information obtained by the OIGs.

Timely, Adequate, and Appropriate Sharing of Cyber Threat Information with other Federal Entities

The agencies' auditors determined that the Federal entities reviewed shared CTIs and DMs in a timely and adequate manner with appropriate Federal entities (with the exception of Commerce who only shared CTIs and DMs when required to do so). Sharing cyber threat information is considered timely when it is available in real time or as quickly as operationally possible, and it is considered adequate when it encompasses relevant and meaningful CTIs or DMs, and when the information is safeguarded from unauthorized access. Sharing cyber threat information with appropriate entities entails using a sharing capability that ensures delivery to the intended recipient(s) of an entity with the need for the cyber threat information and the proper security clearances based on the security classification level of the information. The agencies' auditors tested cyber threat information to verify that the information was shared in a timely and adequate manner with appropriate Federal entities. The results of the testing are summarized in Table 3.

Table 3. Auditor Testing Results for Entity Sharing Cyber Threat Information

Entity	Sharing Information Was Assessed as Timely, Adequate, and Appropriate by the Auditors	Sharing Cyber Threat Information
Commerce	N/A	Commerce only shared CTIs and DMs with other Federal entities when required to do so, such as when reporting security incident information to the Cybersecurity and Infrastructure Security Agency.
DoD	Yes[34]	Five of the eight DoD Components shared CTIs and DMs with other Federal agencies—DC3, DIA, NGA, NSA, and USCYBERCOM. The DoD used tools such as ICOAST, AIS, Threat Intelligence reports, significant cyber activity reports, and e-mail lists to share cyber threat information. DISA, NRO, and DCSA did not share CTIs with other Federal entities.
DOE	Yes	DOE shared CTIs and DMs with other Federal agencies through the use of Cyber Fed Model and Analyst1[35] threat indicator uploads to DHS's FEDGOV, AIS, and/or the Cyber Information Sharing and Collaboration Program.
DHS	Yes	DHS shared unclassified CTIs and DMs directly with Federal agencies and indirectly with Federal agencies via third-party data aggregators.
DOJ	Yes	JSOC used automated tools to share cyber threat information with the private sector and other Federal entities, including the DHS's AIS capability. NCIJTF shared cyber threat information using Lighthouse—an analytical platform of Cyber data from multiple agencies—and via the National Security Agency (NSA) Pulse website, email, video teleconference, phone, and in-person meetings.

[34] DISA NRO, and DCSA did not share CTIs and DMs with other Federal agencies. DoD auditors reviewed a sample for three of the remaining five components and determined that NSA and DC3 shared CTIs in a timely, adequate, and appropriate manner; and NGA adequately shared CTIs, but did not share CTIs in a timely or appropriate manner. USCYBERCOM and DIA did not provide sample information.

[35] Analyst1 provides a centralized location to collect and analyze evidence of malicious activity and manage indicators.

Entity	Sharing Information Was Assessed as Timely, Adequate, and Appropriate by the Auditors	Sharing Cyber Threat Information
ODNI	Yes	ODNI and its service provider shared CTIs and DMs by uploading cyber threat information and reports to ICOAST and providing the information using email. The time it takes to share such information depends on the amount of research needed to add context and the urgency for sharing the information. In addition, some ODNI components prepared summary reports containing cyber threat information that are only produced weekly, monthly, or yearly. These types of reports were not intended for real-time distribution.
Treasury	Yes	GSOC shared CTIs within the Federal Government by uploading TEWIs to the FS-ISAC portal. TEWIs were developed and shared within a reasonable timeframe with other Federal entities when GSOC analysts determined the CTIs and DMs were significant. OCCIP analyzed cyber information from its sources and repackaged the cyber information at an unclassified level into Circulars, which are shared via the Homeland Security Information Network and FS-ISAC portals.

Source: IC IG auditor-generated based on information obtained by the OIGs.

Timely and Adequate Receiving of Cyber Threat Information from other Federal Entities

The agencies' auditors determined that the Federal entities received CTIs and DMs in a timely and adequate manner from other Federal entities. Receiving cyber threat information is considered timely when it is received in real time or quickly enough to ensure the data is still relevant and useful, and it is considered adequate when it encompasses relevant and meaningful CTIs or DMs, and when the information is safeguarded from unauthorized access. The agencies' auditors tested cyber threat information to verify that the information was received in a timely and adequate manner. The results of the testing are summarized in Table 4.

Table 4. Auditor Testing Results for Entity Receiving Cyber Threat Information

Entity	Information Received Was Assessed as Timely and Adequate by the Auditors	Receiving Cyber Threat Information
Commerce	Yes	Commerce received cyber threat information in an adequate manner from other Federal entities through the AIS capability, conference calls, secured email, and briefings.
DoD	Yes[36]	Seven DoD components—DC3, DCSA, DIA, NGA, NRO, NSA, and USCYBERCOM—received CTIs and DMs from the IC, DOE, FBI, NCIJTF, U.S. Computer Emergency Readiness Team, and the Naval Criminal Investigative Service. DISA only received CTIs from AIS.
DOE	Yes	Other Federal entities shared CTIs and DMs with DOE. In particular, DOJ shared threat indicators with DOE through a manual process. In addition, other Federal entities that are also part of the electricity subsector shared cyber threat information with DOE through the Cybersecurity Risk Information Sharing Program.
DHS	Yes	DHS received cyber threat information from other Federal entities—such as DoD (DC3, DISA and NSA) and DOE—after the Federal entities uploaded CTIs and DMs into AIS.
DOJ	Yes	DOJ received cyber threat information from commercial-off-the-shelf automated tools, Lighthouse, and other FBI systems.
ODNI	Yes	ODNI and its service provider received cyber threat information from ICOAST, IC websites, and emails.
Treasury	Yes	Treasury GSOC received notifications of CTIs and DMs via the Malware Information Sharing Platform and emails to an inbox monitored by GSOC. Treasury OCCIP received cyber threat information from financial sector companies, industry groups, and government partners.

Source: IC IG auditor-generated based on information obtained by the OIGs.

[36] DoD auditors reviewed a sample for five components and determined that the NSA, NRO, and DC3 received CTIs in a timely, adequate, and appropriate manner; the DCSA adequately and appropriately received CTIs, but did not receive them in a timely manner; and the NGA review results are classified. USCYBERCOM and DIA did not provide sample information. The DoD auditors did not perform a review of DISA because DISA only received CTIs from AIS.

The Act requires "an assessment of the cyber threat indicators or defensive measures shared with the appropriate Federal entities," to include:

- the number of CTIs or DMs shared through the use of the AIS capability;
- handling information not directly related to a cybersecurity threat that is known at the time of sharing to contain PII;
- the number of times shared information was used to prosecute an offense;
- the impact on privacy and civil liberties; and
- the steps taken to reduce adverse effects on privacy and civil liberties.[37]

Use of the Automated Indicator Sharing Capability

The Act requires OIGs to determine the number of CTIs or DMs shared using the DHS implemented AIS capability.[38] The following entities received CTIs and DMs using AIS:

- Commerce received CTIs from AIS, but the number could not be determined because Commerce did not track the information.
- Five DoD components—DC3, DCSA, DISA, NSA and USCYBERCOM—received CTIs from AIS. According to DHS, it shared 1,217,900 CTIs and DMs in CY 2019 and 2,182,253 in CY 2020 with DoD using the AIS capability.
- DOE officials indicated that the Department received 920,411 unique CTIs and DMs in CY 2019 and 8,183,149 in CY 2020 from the AIS capability.
- According to DHS officials, the Department received 4,584,463 CTIs in CY 2019 and 12,041,366 CTIs in CY 2020 through the AIS capability. DHS subsequently shared the indicators with other Federal entities.
- DOJ received 940,963 CTIs in CY 2019 and 1,242,937 CTIs in CY 2020 through the AIS capability.
- Treasury's GSOC decided to stop receiving CTIs and DMs shared via the AIS capability in early CY 2020 because it was not providing useful information. The number of indicators received during CY 2019 and during the period before they stopped receiving the AIS feed in CY 2020 could not be determined because Treasury GSOC no longer had access to the server.

ODNI, its service provider, and three DoD components—DIA, NGA and NRO—did not obtain CTIs or DMs from AIS in CY 2019 and CY 2020.

Handling Information Containing Personally Identifiable Information

The Act requires OIGs to assess "any information not directly related to a cybersecurity threat that is personal information of a specific individual or information identifying a specific individual and was shared by a non-Federal government entity with the Federal government in

[37] 6 U.S.C. § 1506(b)(2)(D).

[38] 6 U.S.C. § 1506(b)(2)(D)(i).

contravention" of the Act or the guidelines.[39] Officials at Commerce, DoD, DOE, DHS, DOJ, the Treasury, and ODNI, stated they have not received information that is unrelated to a cybersecurity threat that included PII. During testing, such instances did not come to the auditors' attention.

Use of Shared Information to Prosecute an Offense

The Act requires the joint report to address the number of times, according to the Attorney General, that a Federal entity used information shared under the Act to prosecute an offense listed in section 1504(d)(5)(A) of the Act.[40] DOJ officials stated that DOJ is not tracking this metric.

Effects of Sharing on Privacy and Civil Liberties

The Act requires OIGs to assess:

> the effect of sharing cyber threat indicators or defensive measures with the Federal Government on privacy and civil liberties of specific individuals, including the number of notices that were issued with respect to a failure to remove information not directly related to a cybersecurity threat that was personal information of a specific individual or information that identified a specific individual.[41]

Officials at Commerce, DoD, DOE, DHS, DOJ, the Treasury, and ODNI told the auditors that they have not received notices for a failure to remove information not directly related to a cybersecurity threat that was PII.[42] During testing, such instances did not come to the auditors' attention.

Steps Taken to Address Adverse Effects on Privacy and Civil Liberties

The Act requires OIGs to assess "the adequacy of steps taken by the Federal Government to reduce any adverse effect from activities carried out under [the Act] on the privacy and civil liberties of United States persons."[43] Officials at Commerce, DoD, DOE, DHS, DOJ, the Treasury, and ODNI told the auditors that to their knowledge, the activities carried out under the Act did not have adverse effects on the privacy and civil liberties of U.S. persons; therefore, steps to minimize adverse effects were not necessary. During testing, such instances did not come to the auditors' attention.

BARRIERS TO SHARING CYBER THREAT INFORMATION

The Act requires OIGs to assess whether "inappropriate barriers to sharing information" among Federal entities exist.[44] Officials at the Federal entities described to the auditors barriers that they have experienced or observed. DOE and Treasury officials stated that the barriers did not adversely affect sharing CTIs and DMs. DoD and ODNI described barrier-specific effects on

[39] 6 U.S.C. § 1506(b)(2)(D)(ii).

[40] 6 U.S.C. § 1506(b)(2)(D)(iii).

[41] 6 U.S.C. § 1506(b)(2)(D)(iv).

[42] 6 U.S.C. § 1502(b)(1)(F) requires procedures for notifying, in a timely manner, any U. S. person whose personal information is known or determined to have been shared by a Federal entity. 6 U.S.C. § 1504(b)(3)(E) requires procedures for notifying entities and federal entities, when there is a determination that information received does not constitute a CTI. According to the *Privacy and Civil Liberties Final Guidelines: Cybersecurity Information Sharing Act of 2015,* the disseminating entity is to notify all the entities who have received the information determined to be in error as soon as practicable, and the guidelines provide details on information to be contained in a notice.

[43] 6 U.S.C. § 1506(b)(2)(D)(v).

[44] 6 U.S.C. § 1506(b)(2)(E).

sharing CTIs and DMs as identified in the below bullets. The remaining agencies—Commerce, DHS, and DOJ—did not describe any effects of the barriers identified. Barriers described include:

Reluctance to Share

- Components may not share mission-related information because information was previously shared with unauthorized entities or the information was compromised (USCYBERCOM).
- Some private sector companies and industries do not share based on the perception that cooperation with law enforcement may lead to negative business and regulatory consequences (DOJ).
- Different trust levels between Federal entities created a reluctance to share information over concerns of potential misuse of sensitive information (Treasury).
- Private sector entities are reluctant to share information with Federal entities because they do not understand how Federal entities use and protect the information being shared (Treasury).
- Personnel expressed concern that the Cybersecurity and Infrastructure Security Agency requires information but does not reciprocate (Commerce).

Classification Concerns

- Cross-domain sharing is not viable. CTIs and DMs obtained from classified sources could not be ingested and utilized to mitigate risks on unclassified systems because agencies lacked a capability to transfer them to unclassified environments (Commerce, DOJ, and DISA) or lacked appropriate facility security clearance to receive the information (DOJ).
- Restrictive or over-classification makes it difficult to share cyber threat information (DIA, DISA, and Energy).
- Over-classification may significantly delay or halt the ability to analyze shared indicators due to the amount of effort necessary to declassify and transfer the indicators to unclassified systems (Treasury).
- Requests for additional information regarding classified CTIs and DMs received were sometimes denied, rendering agencies unable to effectively assess classified alerts, incidents, and risks (Treasury).

AIS Challenges

- AIS only allows users to subscribe to one, all-inclusive feed, which makes sharing difficult because it is not easily searchable and the users must sort through all of the information to find what is relevant instead of only receiving information that is applicable to them (DC3 and NSA).

- Quality concerns remain with AIS because it provided raw information that was not vetted. Specifically, much of the CTI and DM information received through AIS did not contain any context as to why the indicator was bad (lacking attribution) or whether it was still relevant. Consequently, most AIS indicators would require data enrichment to be usable (Commerce).
- AIS contains redundant CTIs because it does not remove identical CTIs uploaded by multiple entities; in addition, AIS CTIs lack context, such as e-mail or Internet Protocol addresses, which makes it difficult to determine the significance of the potential threat and requires additional research to determine their relevance to agencies (DISA).
- Some entities stated that they had difficulty implementing the AIS platform and Trusted Automated Exchange of Intelligence Information feeds. Due to these difficulties in setting up the feeds, they could not share information (DHS).
- Private sector feedback has identified concerns with AIS customers experiencing false positives (DHS).
- Some Federal AIS participants have shared unconfirmed malware CTI information or low confidence threat information that resulted in false positive alerting within security tools. Some Federal stakeholders can filter out some of these lower confidence indicators while others may not have the expertise or intermediate tools to further refine relevant CTIs before deploying them into security tools for automated alerting or mitigation (DHS).
- Participants in the AIS are not extensively vetted, which raises concerns with sharing certain CTIs and DMs through AIS, particularly those that may contain some degree of sensitivity (DOJ).

Policy Challenges

- Agencies tend not to share CTIs because there is no requirement to do so (USCYBERCOM).
- Agencies develop inconsistent guidance to implement the Act because of a lack of governance structure for sharing and analyzing CTIs across Federal entities (USCYBERCOM).
- Agencies share duplicate and inconsistent data because there is no standard for sharing CTIs (NGA).
- Federal entities are not adhering to interagency policy agreements with regard to Federal cyber information sharing documented in the Multilateral Information Sharing Agreement (DHS).

Inconsistent Format

- Federal Government organizations created indicator repositories or capabilities that were not designed to enable flexible sharing of threat information (ODNI).

- Adequate data standards are lacking. Officials explained that certain file formats are limited and do not support adding additional threat information (NSA). Additionally, when CTIs and DMs were received in PDF and Word document formats, they required manual extraction, verification, and human analysis rather than automated functions to determine cyber threat prioritization (Treasury).

Resource Constraints

- Two entities noted a lack of automated tools to process cyber threat information and remove PII or protected health information, which then requires manual analysis and limits the entities' ability to quickly analyze a large amount of data (NGA and DISA).
- Some agencies lack formal dedicated funding for Federal agencies to implement cyber information capabilities that follow the agreed upon policy requirements. Some agencies also do not have internal staff and resources to share indicators in support of the Cybersecurity and Infrastructure Security Agency via AIS. As a result, these agencies are not able to complete the additional automated workflows required to generate and transmit machine-to-machine cyber information sharing; they can produce human readable reporting disseminated via email, but the technical barriers to convert this information into AIS open standard format remain high (DHS).
- Some agencies and private sector entities do not have the resources to sift through the large number of indicators that are available via AIS (DHS).
- Due to the amount of raw data received, agencies need to increase the number of technically trained personnel, analysts, and subject matter experts to review the information. Agencies also need more analysis tools and infrastructure to store and share the data with other members of the Cyber Community (DOJ).

ACTIONS TAKEN TO MITIGATE BARRIERS TO SHARING CYBER THREAT INFORMATION

Actions planned or taken to mitigate barriers include:

- USCYBERCOM is working to better define mission-critical information to increase information sharing.
- The USCYBERCOM Plans and Policy Directorate is drafting a proposal to create a governance working group at USCYBERCOM and may develop DoD-wide governance on sharing cyber threat indicators uniformly across the DoD.
- DISA officials stated that they have:
    - Collaborated with other agencies to find solutions to incorporate the automation of activity reports, cross-domain sharing, and minimize over-classification.

- Instituted a process to manually review indicators provided to other Federal entities and insert additional context into cyber threat indicators in AIS.
- Manually examined data shared with other entities for PII or protected health information before dissemination.

- DIA officials stated that they discussed the over-classification of reports during meetings with the Cybersecurity Performance Evaluation Model working group and National Security Tiger Team.
- DHS is upgrading the AIS capability and implementing the latest Organization for the Advancement of Structured Information Standards. The Cybersecurity and Infrastructure Security Agency is also proactively updating stakeholder engagement and awareness documentation.
- The Cybersecurity and Infrastructure Security Agency has responded to private sector feedback related to false positives from the AIS public feed by improving the AIS 'allowlist' to ensure that known false positives are not distributed via the AIS environment to stakeholders.
- The DOJ NCIJTF is testing a platform to host some of the data in a cloud environment for the purpose of access across the IC. The cloud project is in the test phase to understand the benefit as well as the associated costs. The NCIJTF also works with affected entities to bring their analysts and subject matter experts on-site to review the data.
- Treasury's OCCIP noted they have implemented memorandum(s) of understanding with other Federal entities that clarified how information may be shared and used.

APPENDIX A: OBJECTIVES, SCOPE, AND METHODOLOGY

The Offices of the Inspectors General (OIGs) for the Departments of Energy, Homeland Security, Justice, Defense, Commerce, the Treasury, and the Office of the Director of National Intelligence assessed the implementation of the *Cybersecurity Information Sharing Act of 2015* (the Act) for calendar years 2019 and 2020.[45] The objective of the assessment was to review actions taken over the prior, most recent, two-year period to carry out the requirements of the Act.

To accomplish the assessment objective, the agencies' auditors:

- Researched applicable laws, policies, regulations, and guidance regarding the sharing of cyber threat information and protecting personally identifiable information (PII).
- Interviewed entity and component officials to discuss their processes for sharing and receiving cyber threat indicators (CTI) and defensive measures (DM), to include sharing or receiving information using various capabilities, such as the Department of Homeland Security's Automated Indicator Sharing capability.
- Reviewed the sufficiency of the policies and procedures used by the entities for protecting and/or removing information shared under the Act that contains PII; and tested a sample of cyber threat information received by the entities to determine whether it contained PII, if applicable.
- Interviewed entity officials to determine the process used to retain or modify the classification of cyber threat information, if applicable; and tested a sample of the shared cyber threat information to determine whether the process resulted in the proper classification, if applicable.
- Interviewed entity officials to determine whether they authorized security clearances for sharing cyber threat information with the private sector.
- Interviewed entity officials to determine whether they disseminated cyber threat information within the entity; and performed testing on a sample of disseminated and used cyber threat information, if applicable.
- Interviewed entity and component officials to determine whether cyber threat information was shared with or received from other Federal entities; and tested a sample of cyber threat information shared with and received from other Federal entities, if applicable.

[45] The OIGs of the Departments of Energy, Homeland Security, and the Treasury, and Office of the Director of National Intelligence prepared separate reports specific to their organization's implementation of the Act. *See* (1) *The Department of Energy's Implementation of the Cybersecurity Information Sharing Act of 2015,* (2) *Review of DHS' Implementation of the Cybersecurity Act of 2015 for Calendar Years 2019 and 2020* (21-026-AUD-DHS); (3) *Audit of the Department of Treasury's Cybersecurity Information Sharing* (OIG-22-013), and (4) *Audit of the Office of the Director of National Intelligence's Implementation of the Cybersecurity Information Sharing Act of 2015* (AUD-2021-003), respectively.

- Interviewed entity officials and tested a sample of cyber threat information shared with other Federal entities to determine whether the privacy and civil liberties of any individuals were impacted due to the entity sharing cyber threat information, if applicable.
- Interviewed entity and component officials to identify barriers that adversely impacted the sharing of cyber threat information.
- Briefed the Council of Inspectors General on Financial Oversight on the progress and status of the project and provided them the draft report for review and comment.

A separate report included For Official Use Only information—*Joint Report on the Implementation of the Cybersecurity Information Sharing Act of 2015* (AUD-2021-002)—and was submitted to the appropriate members of Congress.

The OIGs for the Departments of Defense, Justice, the Treasury, and the Office of the Director of National Intelligence conducted audits from December 2020 through September 2021 in accordance with generally accepted government auditing standards. Those standards require that the auditors plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for the findings and conclusions based on the audit objectives. The OIGs for the Departments of Commerce, Energy, and Homeland Security conducted an evaluation, inspection, and review, respectively, from January 2021 to November 2021 in accordance with the *Council of the Inspectors General on Integrity and Efficiency's Quality Standards for Inspection and Evaluation*, January 2012. The auditors believe the evidence obtained provides a reasonable basis for the findings and conclusions based on the assessment objectives.

APPENDIX B: ABBREVIATIONS AND ACRONYMS

AIS	Automated Indicator Sharing
CTI	Cyber Threat Indicator
CY	Calendar Year
DC3	DoD Cyber Crime Center
DCSA	Defense Counterintelligence and Security Agency
DHS	Department of Homeland Security
DIA	Defense Intelligence Agency
DIB	Defense Industrial Base
DISA	Defense Information Systems Agency
DM	Defensive Measures
DoD	Department of Defense
DOE	Department of Energy
DOJ	Department of Justice
ESOC	Enterprise Security Operations Center
FBI	Federal Bureau of Investigation
FS-ISAC	Financial Services – Information Sharing and Analysis Center
GAO	Government Accountability Office
GSOC	Government Security Operations Center
IC	Intelligence Community
ICOAST	Intelligence Community Analysis and Signature Tool
IC IG	Intelligence Community Inspector General
IC SCC	Intelligence Community Security Coordination Center
JSOC	Justice Security Operations Center
NCIJTF	National Cyber Investigative Joint Task Force
NGA	National Geospatial-Intelligence Agency
NRO	National Reconnaissance Office
NSA	National Security Agency
OCCIP	Office of Cybersecurity and Critical Infrastructure Protection
ODNI	Office of the Director of National Intelligence

OIG	Office of the Inspector General
PII	Personally Identifiable Information
SOC	Security Operations Center
TEWI	Treasury Early Warning Indicator
U.S.	United States
USCYBERCOM	United States Cyber Command


INSPECTOR GENERAL
INTELLIGENCE COMMUNITY
INDEPENDENCE • INTEGRITY • PROFESSIONALISM