OFFICE OF THE INSPECTOR GENERAL OF THE INTELLIGENCE COMMUNITY

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

★★★★

Audit Division
AUD-2023-002

December 12, 2023

This report contains information that the Office of the Inspector General of the Intelligence Community has determined is confidential, sensitive, or protected by Federal Law, including protection from public disclosure under the Freedom of Information Act (FOIA) 5 U.S.C. § 552. Recipients may not further disseminate this information without the express permission of the Office of the Inspector General of the Intelligence Community personnel. Accordingly, the use, dissemination, distribution or reproduction of this information to or by unauthorized or unintended recipients may be unlawful. Persons disclosing this information publicly or to others not having an official need to know are subject to possible administrative, civil, and/or criminal penalties. This report should be safeguarded to prevent improper disclosure at all times. Authorized recipients who receive requests to release this report should refer the requestor to the Office of the Inspector General of the Intelligence Community.

OFFICE OF THE INSPECTOR GENERAL OF THE INTELLIGENCE COMMUNITY
AUDIT DIVISION
WASHINGTON, DC

MEMORANDUM FOR: See Distribution

SUBJECT: Joint Report on the Implementation of the Cybersecurity Information Sharing Act of 2015 (AUD-2023-002)

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 2021 and 2022 to carry out the requirements of the Cybersecurity Information Sharing Act of 2015.

On December 18, 2015, Congress enacted the Cybersecurity Information Sharing Act of 2015 (6 U.S.C. § 1501 et seq.) (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 to carry out the Act over the most recent two-year period. 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 its comments were incorporated when preparing this report.

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

NG RICHARD M WZFKND

Digitally signed by NG RICHARD M WZFKND
Date: 2023.12.15 08:46:03 -05'00'

Richard M. Ng
Assistant Inspector General for Audit
Office of the Inspector General of the Intelligence Community

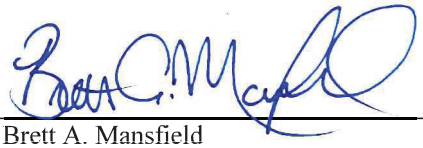
Date

FREDERICK MENY

Digitally signed by FREDERICK MENY
Date: 2023.12.15 11:35:38 -05'00'

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

Date



December 15, 2023

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

Date

Kshemendra N. Paul

Digitally signed by Kshemendra N. Paul
Date: 2023.12.15 10:55:38 -05'00'

Kshemendra Paul
Assistant Inspector General for Cyber Assessments and Data Analytics
Department of Energy, Office of the Inspector General

Date

Kristen Bernard

12-18-23

Kristen Bernard
Acting Deputy Inspector General for Audits
Department of Homeland Security, Office of Inspector General

Date

Carol S. Taranzka

Deputy Assistant Inspector General for Audit, signing for:

December 18, 2023

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

Date

Deborah L. Harker

Digitally signed by Deborah L. Harker
Date: 2023.12.20 15:25:39 -05'00'

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
President of the Senate
Speaker of the House of Representatives

CONTENTS

OFFICE *of the* INSPECTOR GENERAL *of the* INTELLIGENCE COMMUNITY

EXECUTIVE SUMMARY

Joint Report on the Implementation of the Cybersecurity Information Sharing Act of 2015 (AUD-2023-002)

WHY WE DID THIS REVIEW

On December 18, 2015, Congress enacted the Cybersecurity Information Sharing Act of 2015 (6 U.S.C. § 1501 et seq.) (the Act).[1] The Act was established to improve cybersecurity in the United States through enhanced sharing of cyber threat information.[2] The Act creates a framework to facilitate and promote the voluntary sharing of cyber threat indicators (CTIs)[3] and defensive measures (DMs)[4] among and between Federal and non-Federal entities.[5] 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 to carry out the Act over the most recent two-year period.[6] This report meets the biennial joint reporting requirement.

The Offices of Inspector General (OIGs) of the Departments of Commerce, Defense, Energy, Homeland Security, Justice, and the Treasury, and of the Intelligence Community assessed the implementation of the Act for calendar years (CYs) 2021 and 2022 for their respective entities.

---

[1] For the purposes of this report, we will refer to the Cybersecurity Information Sharing Act of 2015 as "the Act" to distinguish it from the Cybersecurity and Infrastructure Security Agency (CISA) established in November 2018.

[2] "Cybersecurity threat" is used by the Act, as defined by 6 U.S.C. § 650(8), to generally mean an action, not protected by the First Amendment of the U.S. Constitution, 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.

[3] "Cyber threat indicator" is used by the Act, as defined by 6 U.S.C. § 650(5), to 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.

[4] "Defensive measures" is used by the Act, as defined by 6 U.S.C. § 650(9), to generally mean 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.

[5] "Federal entity" is defined by the Act to mean 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 entity" is defined by the Act to include state, local, and tribal governments; private sector companies; and academic institutions. *See* 6 U.S.C. § 1501(14).

[6] 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. 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 at the Top Secret security level, including Indicators of Compromise[7] and malware signatures.[8] Additionally, in January 2020, the IC SCC deployed ICOAST-U, an unclassified version of ICOAST. ICOAST-TS and ICOAST-U are collectively known as ICOAST. ICOAST integrates CTIs 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. In CY 2021, ODNI released a new tool, which integrates Cyber Threat Intelligence Data and Vulnerability Management Data and serves as a centralized repository.

In CY 2016, the Department of Homeland Security's Cybersecurity Infrastructure Security Agency (CISA) developed the Automated Indicator Sharing (AIS) capability, which enables the real-time exchange of unclassified CTI and DMs to participants of the AIS community. CISA offers the AIS service at no cost to participants as part of CISA's mission to work with public and private sector partners to identify and help mitigate cyber threats through information sharing. The fundamental concept of the AIS capability is to promote interaction among participants. In CY 2021 and CY 2022, entities continued to share cyber threat information through various reporting means in addition to AIS and ICOAST, 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.[9] 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.
- 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 Federal and non-Federal entities shared, 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.

---

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

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

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

- Use the Department of Homeland Security capability, AIS, to receive CTIs or DMs, with the exception of Treasury and ODNI.
- 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 U.S. 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 recommendations.

BACKGROUND

CYBERSECURITY INFORMATION SHARING ACT OF 2015

On December 18, 2015, Congress enacted the Cybersecurity Information Sharing Act of 2015 (6 U.S.C. § 1501 et seq.) (the Act).[10] The Act was established to improve cybersecurity in the United States through enhanced sharing of cyber threat information.[11] The Act creates a framework to facilitate and promote voluntary cyber threat indicator (CTI)[12] and defensive measure (DM)[13] sharing among and between Federal and non-Federal entities.[14]

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.[15] Without legislative action, the Act will sunset on September 30, 2025 (except with respect to actions authorized and information obtained under the Act before such date).

OFFICES OF INSPECTOR GENERAL REPORTING REQUIREMENT

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 report to Congress by December 18, every two

---

[10] *See supra* note 1.

[11] "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.

[12] *See supra* note 3.

[13] *See supra* note 4.

[14] *See supra* note 5.

[15] 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).

years, on the actions taken to carry out the Act over the most recent two-year period.[16] Section 1506(b) of the Act requires the biennial joint report to include the following:

- An assessment of the sufficiency of policies, procedures, and guidelines related to sharing CTIs within the Federal Government.
- An assessment of 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.
- A review of the actions taken by the Federal Government based on CTIs or DMs shared with the Federal Government, including the appropriateness of subsequent uses and disseminations of CTIs and DMs and whether the CTIs or DMs were shared in a timely and adequate manner with appropriate entities or the public.
- An assessment of 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 6 U.S.C § 1504(d)(5)(A).
    - 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.
    - he 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.
- An assessment of barriers affecting the sharing of CTIs or DMs.[17]

[16] *See supra* note 5.
[17] 6 U.S.C. § 1506(b)(2).

ENTITIES REVIEWED

The Offices of Inspector General (OIGs) reviewed their agencies' components responsible for sharing, receiving, or disseminating CTIs and DMs during calendar year (CY) 2021 and CY 2022 as follows:

Department of Commerce (Commerce). The Enterprise Security Operations Center (ESOC) within Commerce serves as the focal point for many security operations activities, including cyber threat information sharing.

Department of Defense (DoD). The following eight DoD components are responsible for sharing cyber threat information with Federal and non-Federal entities:

- The U.S. Cyber Command (USCYBERCOM) is a combatant command that directs, synchronizes, and coordinates cyberspace planning and operations. Among other responsibilities, USCYBERCOM defends the DoD Information Network, provides support to combatant commanders for global mission execution, and strengthens the nation's ability to withstand and respond to cyberattacks.
- The National Security Agency (NSA) is a combat support agency that leads the Federal Government in cryptology for signals intelligence and cybersecurity products and services. The NSA enables computer network operations to gain an advantage for the United States against its adversaries. In addition, the NSA uses industry partnerships and information sharing to prevent and eliminate foreign cyber threats to national security systems and the DoD.
- The Defense Information Systems Agency (DISA) is a combat support agency that plans, engineers, tests, fields, and operates information sharing capabilities for joint service members, national-level leaders, and other mission and coalition partners across DoD.
- The Defense Intelligence Agency (DIA) is a combat support agency that produces, analyzes, and disseminates military intelligence to service members, defense policymakers, and force planners in the DoD and Intelligence Community (IC) in support of U.S. military operations. The DIA is also the DoD cybersecurity service provider for classified networks, in coordination with other DoD stakeholders.
- The National Reconnaissance Office (NRO) is responsible for developing, acquiring, launching, and maintaining intelligence satellites. The NRO provides global communications, early warning of missile launches, and imagery to the DoD to support its operations.
- The National Geospatial-Intelligence Agency (NGA) is a combined intelligence and combat support agency that provides geographical data to the DoD and the IC.
- The Defense Counterintelligence and Security Agency (DCSA) provides security and counterintelligence support to the DoD through vetting, industry engagement, education, and other support. The DCSA also performs background investigations for certain branches of the Federal Government.
- The DoD Cyber Crime Center (DC3) provides digital and multimedia forensics, specialized cyber training, and cyber analytics for the DoD. The DC3 is the operational focal point for the Defense Industrial Base (DIB) Cybersecurity Program and analyzes, produces, and distributes

cyber products that contain actionable cyber threat information to the DoD, Federal Government, and the private sector.

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.

Department of Homeland Security (DHS). DHS's Cybersecurity and Infrastructure Security Agency (CISA) 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 CISA 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). The following three 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 Federal Bureau of Investigation (FBI) Cyber Division (CyD) gathers cyber threat indicators and other cyber threat information through its investigations and a variety of intelligence sources and shares them with partners through a variety of means.
- The Enterprise Security Operations Center (ESOC) within the Information Technology Branch is responsible for proactively identifying, detecting, protecting, and responding to all cyber threats and attacks against the FBI data and Information Technology systems.

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 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 departments and agencies.
- The Cyber Threat Intelligence Integration Center (CTIIC) integrates and enables IC cyber analysis, collection, and resources to protect critical infrastructure and support and inform national interests on current and future cyber threats.
- The National Intelligence Council is responsible for leading analysis across the IC to inform immediate and long-term policy deliberations. National Intelligence Officers serve as the

principal subject matter experts to the Director of National Intelligence and national security decision makers on all aspects of analysis related to their regional and functional roles.

Department of the Treasury (Treasury). Two components within the Department of the Treasury are responsible for sharing CTIs for Treasury: the Treasury Shared Services Security Operations Center (TSSSOC) and the Office of Cybersecurity and Critical Infrastructure Protection (OCCIP). TSSSOC uses an internal ticketing system to track CTIs and DMs, then scans Treasury's network for matching events. If TSSSOC analysts determine that cyber threat indicators and defensive measures are a novel threat that originated in Treasury and is unknown to the public or other federal entities, a Treasury Early Warning Indicator (TEWI) is developed and shared with other Federal entities. OCCIP monitors and analyzes intelligence related to cyber threats to the financial services sector received from intelligence sources, primarily from Treasury's Office of Intelligence and Analysis (OIA), as well as Treasury's Financial Crimes Enforcement Network and Federal law enforcement sources, and repackages the cyber information at an unclassified level into Circulars, before sharing with federal partners and the financial services sector.

ASSESSMENT RESULTS

SHARING HAS IMPROVED AND EFFORTS ARE UNDERWAY TO EXPAND ACCESSIBILITY TO INFORMATION

Progress in Sharing Cyber Threat Information Among Federal Entities

In CY 2021 and CY 2022, 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 incidents.

In April 2017, ODNI's IC SCC deployed the Intelligence Community Analysis and Signature Tool (ICOAST) to increase cybersecurity threat intelligence sharing at the Top Secret security level, including Indicators of Compromise[18] and malware signatures.[19] Additionally, in January 2020, the IC SCC deployed ICOAST-U, an unclassified version of ICOAST. An IC SCC official stated that the IC SCC developed an automated process to move indicators from ICOAST-U to populate ICOAST-TS, but the movement of Unclassified//For Official Use Only events and indicators from ICOAST-TS to ICOAST-U requires a manual review and transfer process. The official stated that the ICOAST-TS and ICOAST-U have similar sharing and population processing through machine-to-machine transfers, crowdsourcing, and commercial data feeds. ICOAST-TS and ICOAST-U are collectively known as ICOAST. 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. Six of the Federal entities reviewed, Commerce, DOE, DHS, DOJ, ODNI, and DoD, received CTI from ICOAST. Treasury and portions of FBI did not receive cyber threat information from ICOAST.

In CY 2021, ODNI released a new tool. It is the first tool to integrate Cyber Threat Intelligence Data and Vulnerability Management Data and serves as a centralized repository for cyber threat intelligence and vulnerability data.

Additionally, Commerce, DOE, DHS, DOJ, and DoD used the AIS capability to share or receive cyber threat information. Treasury decided to stop receiving CTIs and DMs shared via the AIS capability in early CY 2020. IC SCC officials told Intelligence Community Inspector General (IC IG) auditors that, from 2020 to 2022, 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 create a sharing mechanism between AIS and ICOAST in 2023.

Continuing Efforts to Share Cyber Threat Information

In addition to AIS, ICOAST, and a new ODNI tool, 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:

---

[18] *See supra* note 7.
[19] *See supra* note 8.

- Websites increased the amount of shared cybersecurity information in CY 2021 and CY 2022. For example, ODNI's 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,[20] situational awareness reports, weekly and monthly vulnerability reports, requests for information, and blogs. Officials with appropriate access to the Top Secret network can obtain and use this information. 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 DoD Secure Access File Exchange.
- DOJ shares cyber threat information via raw intelligence information reports to IC partners, various sharing mechanisms defined in the *Framework for Improved Cyber Information Sharing and Interagency Coordination (FBI−April 2020)*, Cybersecurity Awareness messages, FLASH products, Private Industry Notifications, and direct sharing in real time with Federal partners embedded at the National Cyber Investigative Joint Task Force (NCIJTF).
- ODNI's Cyber Threat Intelligence Integration Center (CTIIC) produced several product lines including Cyber Threat Intelligence Summaries, cyber memorandums, and stand-alone cyber threat graphics.
- During CY 2021 and CY 2022, Treasury (TSSSOC) did not develop any Treasury Early Warning Indicators (TEWIs),[21] however, it reported that it did work with partners to contribute to online publication of novel malware samples found during a recent high profile cyber incident. Treasury (OCCIP) developed 7 cybersecurity alerts, 11 circulars,[22] 20 Cyber Threat Intelligence and Indicators Notices, referred to as CTIIN-FINs, and 39 Indicator Notices related to CTIs and DMs. Products are shared via unclassified meetings, internal and external web portals, and email distribution lists.
- ODNI's IC SCC designs and conducts ICE STORM, an annual cybersecurity exercise. ICE STORM brings together participants from IC elements, DoD, and law enforcement, as well as international partners, to share cybersecurity information, develop cybersecurity risk management activities, and plan incident response.

Private Sector Sharing Using the Automated Indicator Sharing and Other Capabilities

As noted, DHS developed AIS in 2016 to enable the real-time exchange of unclassified CTIs and DMs to participants of the AIS community. CISA offers the AIS service at no cost to participants as part of CISA's mission to work with public and private sector partners to identify and help mitigate cyber threats through information sharing. The fundamental concept of the AIS capability is to promote interaction among participants.

---

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

[21] 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.

[22] OCCIP monitors and analyzes intelligence related to cyber threats to the financial services sector received from intelligence sources and repackages the cyber information at an unclassified level into circulars.

AIS is not the only capability that allows sharing of cyber threat information between Federal entities and the private sector. Other capabilities include:

- DHS's CISA shares cyber threat information, including CTIs and DMs, with non-Federal entities that have signed a Cyber Information Sharing and Collaboration Agreement with CISA.
- DOE shares CTIs and DMs with the private sector through the use of the Cybersecurity Risk Information Sharing Program (CRISP), Analysis of Risks in the Energy Sector (ARES) reports, and Joint Cybersecurity Advisories.
- DoD's USCYBERCOM has partnerships with at least 12 private sector companies with which it shares unclassified cyber threat information to improve responses to cyber threats. To share CTIs and DMs with the private sector, USCYBERCOM uses its UNDER ADVISEMENT and Cyber 9-Line programs. The UNDER ADVISEMENT program is USCYBERCOM's private sector partnership that facilitates information sharing between the Cyber National Mission Force and private sector partners. The Cyber 9-Line program allows participating partners to access an unclassified portal, amongst other methods, to communicate with USCYBERCOM regarding cyber threats to their networks and obtain support.
- DoD's Cyber Crime Center shares unclassified CTIs and DMs with the private sector through the DIB–Network, an unclassified portal that private sector companies, which are already part of the DIB Cyber Security Program, may join to share cybersecurity information with the DoD. When sharing information through the DIB–Network, DoD Cyber Crime Center officials will review and share information that other DIB partners prepared or review and share information that DoD Cyber Crime Center officials prepared to help the DIB partners secure their networks. The DoD Cyber Crime Center also produced five classified cyber threat information products that it shared with its DIB partners.
- The DOJ JSOC uses Anomali, a commercial-off-the-shelf (COTS) automated tool that receives and processes indicator information from the DHS AIS system. By using this automated tool, the JSOC has created numerous detection rules to prevent and detect cybersecurity incidents. Consequently, public and private sector entities using the same COTS platform have access to the indicator information.
- The FBI Cyber Division provides briefings regarding cyber threats and indicators to private sector partners. Additionally, the Cyber Division crafts private sector products (i.e., Private Industry Notifications (PINs) and FBI Liaison Alert System (FLASH) reports and Joint Cybersecurity Advisories (JCSA)) that contain threat information to include indicators of compromise and disseminates these products to private sector partners.

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.[23]

[23] *See supra* note 17.

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 those 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.[24]

The OIGs determined that the policies, procedures, and guidelines the Federal entities reviewed used for sharing CTIs within the Federal Government were sufficient (see Table 1).

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.[25] In response to the Act, they developed and publically issued the following four documents:

- *Final Procedures Related to the Receipt of Cyber Threat Indicators and Defensive Measures by the Federal Government* 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* 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* 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* facilitates and promotes the timely sharing of classified and unclassified CTIs and 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)

Under 6 U.S.C. § 1504(d)(5)(C), the CTIs and DMs provided to the Federal Government under the Act shall be retained, used, and disseminated in accordance with Documents 1 and 2. Document 3 is specific to and for use by non-Federal entities. Document 4 states that its purpose is to facilitate and promote the sharing of cyber threat information among and between Federal and non-Federal entities.

---

[24] 6 U.S.C. § 1506(b)(2)(A).
[25] *See* 6 U.S.C. § 1504.

The OIGs of the designated Federal entities reviewed the specific policies, procedures, and guidelines their respective elements used to determine whether they sufficiently adhered to the four documents created as a result of CISA. DHS uses the four CISA documents, and Commerce and DOJ stated that they use the CISA documents in conjunction with additional policies, procedures, and guidelines. A few entities stated that they do not use the CISA documents, however they use other policies, procedures, and guidelines to meet the criteria laid out in the CISA documents. The OIG results of those entities are provided in Table 1.

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
DoD	Yes	DoD components developed and implemented policies, procedures, and guidelines that aligned with 6 U.S.C. §§ 1502(a) and (b) and 1504(a), (b), and (d), and therefore, were sufficient and in compliance with those sections.
DOE	Yes	DOE's policies, procedures, and guidelines were sufficient and complied with the guidance in the Cybersecurity Information Sharing Act.
ODNI	Yes	ODNI does not use the four documents developed under the Act for sharing and receiving cyber threat information. ODNI sufficiently meets the principles of the document using other policies and procedures.
Treasury	Yes	TSSSOC and OCCIP use sufficient agency-specific policies, procedures, and practices that align with the guidance in the Cybersecurity Information Sharing Act.

Table 1

Source: IC IG auditor-generated based on information obtained by the OIGs of the organizations listed in the table.

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.[26] The guidelines on privacy and civil liberties were updated in November 2022.

Proper Classification 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."[27] Proper classification of documents protects intelligence information and allows appropriate dissemination and use.

Proper Classification of Cyber Threat Indicators and Defensive Measures

ODNI, DoD, and DHS properly classify CTIs and DMs. Based on the testing of examples of CTIs and DMs, the documents had appropriate portion marks and overall classifications were consistent with the

[26] 6 U.S.C. § 1504(b)(2)(B).
[27] 6 U.S.C. § 1506(b)(2)(B).

sources, references, or embedded links used for the content. According to DHS, DoD, 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, 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 orginally classify the CTIs or DMs shared, or did not share classified CTIs or DMs with the private sector.

Authorization of Security Clearances

DHS, DOE and DOJ authorized security clearances for the purpose of sharing cyber threat information with the private sector.

- DHS authorized 236 security clearances in CY 2021 and 506 in CY 2022 to private sector partners participating in DHS's various information sharing programs.
- DOE maintained 32 active security clearances in CY 2021 and 67 active security clearances in CY 2022.
- DOJ (FBI) authorized 39 security clearances in CY 2021 and 31 in CY 2022 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, the Treasury, and ODNI did not authorize security clearances for the purpose of sharing cyber threat information with the private sector.

- Commerce and ODNI did not share classified CTIs or DMs with the private sector.
- DoD did not authorize security clearances expressly for the purpose of sharing CTIs and DMs with the private sector.
- Treasury did not authorize security clearances for the purpose of sharing cyber threat information with the private sector. The Treasury's OCCIP hosted unclassified, and attended classified meetings to discuss 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.

Actions Taken by Entities

The Act requires OIGs to conduct "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."[28]

[28] 6 U.S.C. § 1506(b)(2)(C).

Appropriate Dissemination and Use of Cyber Threat Information

The OIGs determined that the Federal entities appropriately disseminated and/or used CTIs or DMs Federal entities shared. 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 Name	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 using the Commerce Threat Intelligence Portal. CTIs and DMs were ingested into Security Information and Event Management software to identify actionable items.
DoD	Yes	DoD component officials stated they used and disseminated CTIs and DMs shared by other Federal agencies. The DoD OIG confirmed that DoD components shared cyber threat information that listed a source of the information as a non-DoD Federal agency.
DOE	Yes	DOE connected to AIS every 240 minutes and to the Cyber Information Sharing Collaboration Program every 120 minutes and downloaded the cyber threat data for redistribution across the enterprise.
DHS	Yes	DHS shared unclassified indicators via AIS with CISA's threat intelligence platform, Analyst1. AIS also enables cyber threat indicators from Analyst1 and other internal cyber threat indicator generation sources to be disseminated to AIS Trusted Automated Exchange of Intelligence Information (TAXII) collections. CISA shares unclassified indicators via the AIS program according to DHS's Traffic Light Protocol and classified indicators under the business rules of the Enhanced Cybersecurity Services programs.
DOJ	Yes	DOJ disseminated shared cyber threat information to its components through automated sharing and monitoring tools.
ODNI	Yes	ODNI appropriately internally disseminated cyber threat indicators or defensive measures that have been shared by Federal and non-Federal entities to relevant components, and these components used this information.
Treasury	Yes	TSSSOC ingested and incorporated Indicators of Compromise (IOCs) into monitoring and alerting mechanisms.

Table 2

Source: IC IG auditor-generated based on information obtained by the OIGs of the organizations listed in the table.

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

The OIGs 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, which 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 Name	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	DoD shared CTIs and DMs with other Federal agencies using multiple capabilities and tools, such as AIS, ICOAST, and the DoD Secure Access File Exchange.
DOE	Yes	DOE shared CTIs and DMs with other Federal agencies through the use of Analyst1 threat indicator uploads to DHS's AIS, and/or the Cyber Information Sharing and Collaboration Program.
DHS	Yes	DHS shared unclassified CTIs and DMs directly with Federal agencies via AIS.
DOJ	Yes	JSOC used automated tools to share cyber threat information with the other Federal entities, including the DHS's AIS capability. The NCIJTF shared cyber threat information using Paladin, an analytical platform of cyber data from multiple agencies, and via the NSA Pulse website, email, video teleconference, phone, and in-person meetings.

Entity Name	Sharing Information Was Assessed as Timely, Adequate, and Appropriate by the Auditors	Sharing Cyber Threat Information
ODNI	Yes	ODNI shared CTIs and DMs in a timely and adequate manner with appropriate Federal entities. The time it takes to share such information varies depending on the amount of research needed to add context and the urgency for sharing the information. In addition, some components prepare summary reports containing cyber threat information that are only produced weekly, monthly, or yearly. These types of reports are not intended for real-time distribution.
Treasury	Yes	TSSSOC worked with partners, sharing CTIs during a sensitive incident. The CTIs were then published by TSSSOC's partners in two on-line publications. OCCIP used emails, unclassified meetings, as well as posts to various portals, to share cyber threat information with Federal agencies such as the Federal Reserve Board, Consumer Financial Protection Bureau, Commodity Futures Trading Commission, Federal Deposit Insurance Corporation, Office of the Comptroller of the Currency, Securities and Exchange Commission, Farm Credit Administration, National Credit Union Administration, and Federal Housing Finance Agency.

Table 3

Source: IC IG auditor-generated based on information obtained by the OIGs of the organizations listed in the table.

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

The OIGs determined that the Federal entities received CTIs and DMs in a timely and adequate manner from other Federal entities, except for DoD and Treasury, which could not determine timeliness and adequacy due to lack of information. 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. 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 Name	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	Not Determined	DoD component officials stated that they received CTIs and DMs from other Federal entities. However, DoD OIG was unable to determine whether the information received from other Federal agencies was timely, adequate, and appropriate because the DoD component officials stated that they could not track the cyber threat information received from other Federal entities due to the high volume of information received.
DOE	Yes	Other Federal entities shared CTIs and DMs with DOE through Analyst1's direct API connection to AIS.
DHS	Yes	DHS received cyber threat information from other Federal entities, such as DoD and DOE, after the Federal entities uploaded CTIs and DMs into AIS.
DOJ	Yes	External Federal entities have shared indicators directly with the DOJ, as well as indirectly via FBI investigative or operational entities such as CyWatch, NCIJTF, and various FBI Cyber Division program elements and corresponding field office components.
ODNI	Yes	ODNI received cyber threat information in real time or otherwise in a timely manner, considering time needed for additional research to incorporate context.
Treasury	Not Determined	Other Federal entities such as NATO-EUCOM and CISA have shared cyber threat information with TSSSOC. The amount of cyber threat indicators TSSSOC received cannot be quantified with certainty due to aggregation from various feed sources, and it cannot be determined how long a partner had the CTI/DM, nor what protections were applied to the information, before sharing it. Therefore, it cannot be assessed if the data was received in a timely, adequate and appropriate manner.

Table 4

Source: IC IG auditor-generated based on information obtained by the OIGs of the organizations listed in the table.

Specifics Concerning the Sharing of Cyber Threat Information

The Act requires OIGs to conduct "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;
- The handling of 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 certain offenses;
- The impact on privacy and civil liberties; and
- The steps taken to reduce adverse effects on privacy and civil liberties.[29]

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.[30] The following entities reported on the use of AIS:

- Commerce received CTIs and DMs from AIS, but Commerce did not track the information to quantify the number.
- DoD received CTIs and DMs from AIS, but DoD did not track the information to quantify the number.
- DOE received 428,391 CTIs and DMs in CY 2021 and 46,670 in CY 2022 through the AIS capability.
- DHS received 9,888,099 CTIs in CY 2021 and 809,844 CTIs in CY 2022 through the AIS capability. DHS subsequently shared the indicators with other Federal entities.
- DOJ received 600,963 CTIs and DMs in CY 2021 and 257,206 CTIs in CY 2022 through the AIS capability.
- ODNI did not obtain CTIs or DMs directly from AIS in CY 2021 and CY 2022. ODNI's IC SCC officials stated that, from 2020 to 2022, IC SCC and AIS exchanged manual data feeds of cyber threat indictors to prepare for subsequent automated exchanges of indicators. IC SCC and CISA are planning to create an automated, bi-directional sharing mechanism in 2023 between ICOAST-U and AIS.
- Treasury's TSSSOC stopped receiving CTIs and DMs shared via the AIS capability in early CY 2020. TSSSOC used the aggregator AlienVault to receive cyber threat indicators from DHS for CYs 2021 and 2022.

[29] 6 U.S.C. § 1506(b)(2)(D).
[30] 6 U.S.C. § 1506(b)(2)(D)(i).

Figure 1 illustrates the five Federal entities that use the AIS capability.

Figure 1. Federal Entities Reviewed That Used AIS Data (CY 2021 and CY 2022)

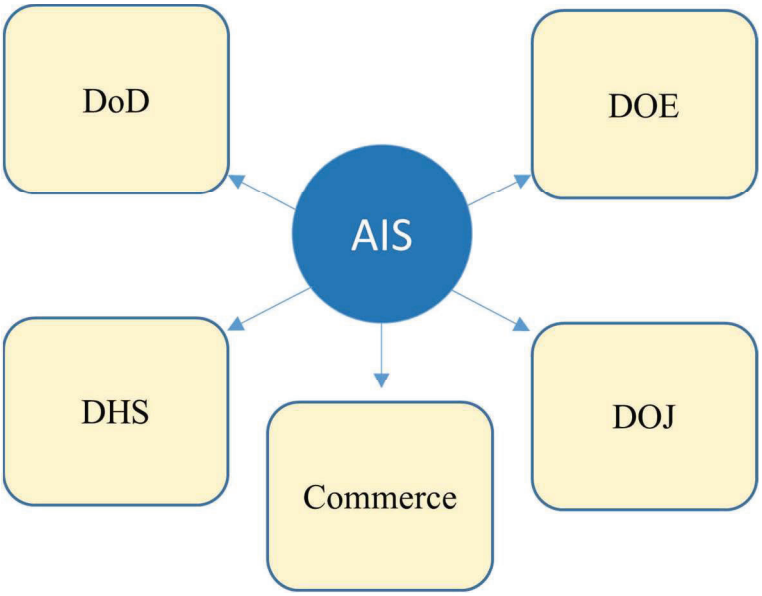


Figure 1
Source: IC IG auditor-generated based on information obtained by the OIGs.

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 contravention" of the Act or the guidelines.[31] 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.

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 6 U.S.C. § 1504(d)(5)(A).[32] DOJ officials stated that DOJ is not tracking this metric. DOJ officials told the auditors that crediting a case solely on information shared under the Act is not measurable because information gathered to prosecute an offense may come from multiple sources, including the Act. Senior prosecutors who review computer intrusion prosecutions generally told the auditors that they cannot remember any cases in which information shared under the Statute was used as evidence in a criminal prosecution.

[31] 6 U.S.C. § 1506(b)(2)(D)(ii).
[32] 6 U.S.C. § 1506(b)(2)(D)(iii).

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...[33]

Officials at Commerce, DoD, DOE, DHS, DOJ, the Treasury, and ODNI stated that they have not received notices for a failure to remove information not directly related to a cybersecurity threat that was PII.[34]

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."[35] Officials at Commerce, DoD, DOE, DHS, DOJ, the Treasury, and ODNI stated 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.

Barriers to Sharing Cyber Threat Information

The Act requires OIGs to assess whether "inappropriate barriers to sharing information" among Federal entities exist.[36] Officials at the Federal entities described barriers that they have experienced or observed. DOE and Treasury officials stated that the barriers did not adversely affect sharing CTIs and DMs. Commerce, DoD, DHS, DOJ, and ODNI described barrier-specific effects on sharing CTIs and DMs, to include:

Reluctance to Share

- Federal entities continue to be reluctant to share information into the public collection. Some prefer to share exclusively within the Federal collection. Others may have policy requirements to share only within their relevant sector among eligible stakeholders (DHS).
- Concern that the Cybersecurity and Infrastructure Security Agency could share additional information (Commerce).

---

[33] 6 U.S.C. § 1506(b)(2)(D)(iv).

[34] 6 U.S.C. § 1502(b)(1)(F) requires notification to any U.S. person whose personal information is known or determined to have been shared by a Federal entity in violation of the Act. Under 6 U.S.C. § 1502(b)(1)(E)(ii), a Federal entity, when it determines that information received does not constitute a cyber threat indicator and contains personal information, must remove such information. 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.

[35] 6 U.S.C. § 1506(b)(2)(D)(v).

[36] 6 U.S.C. § 1506(b)(2)(E).

- Some private sector companies are hesitant to share cyber threat information with others because they believe sharing such information may raise legal and competitive issues, including implicating potential antitrust issues (DOJ).
- 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. Public perception of Federal Government actions in cyberspace, especially those of law enforcement agencies, is mixed (DOJ).
- Some Federal entities are hesitant to share cyber threat information because the sharing may jeopardize ongoing operations (DOJ and DoD).

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 DoD) or lacked appropriate facility security clearance to receive the information (DOJ).
- Restrictive or over-classification makes it difficult to share cyber threat information (DoD and ODNI). 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).

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 manually sort through information to find what is relevant instead of only receiving information that is applicable to them (DoD).
- AIS provided unvetted raw information. Specifically, much of the CTI and DM information received through AIS did not contain 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).
- Inconsistent vendor support for the latest Structured Threat Information eXpression (STIX) and Trusted Automated Exchange of Intelligence Information (TAXII) specifications hinders Federal entities from being able to deploy shared CTIs and DMs from others in the community into their vendor tools (DHS).

Policy Challenges

- A lack of overarching guidance pertaining to cybersecurity information sharing policy, requiring DoD components to establish their own guidance (DoD).

Inconsistent Format

- Federal Government organizations created indicator repositories or capabilities that were not designed to enable flexible sharing of threat information. (ODNI).
- Certain file formats are limited and not always compatible with the format of the data in the component's repository, which limits sharing with DHS (DoD).
- CTI and DM sourcing is inherently problematic. The fewer the number of controls on the upload side, the higher the probability of bad indicators becoming part of the product (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. The lack of automation also limits passing unclassified CTIs and DMs to higher classification systems (DoD).
- Some agencies lack formal dedicated funding for Federal agencies to implement cyber information capabilities that follow the agreed-upon policy recommendation. Some agencies also do not have organizational resources to support machine-readable indicator sharing (DHS).
- With respect to Federal and private sector entities' ability to effectively filter and sort indicators that are appropriate for their sector, if indicator and defensive measure data is not categorized properly, entities cannot deploy relevant mitigation measures and may be less inclined to use data not targeted for their sector (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).
- The quality of information received varies from each provider. The differences in quality and variation from each provider presents issues in the ingestion of large datasets. As the data ingestion increases, the labor required to organize the data into an effective massive data ingest increases (DOJ).

Actions Taken to Mitigate Barriers to Sharing Cyber Threat Information

Actions planned or taken to mitigate barriers include:

- Commerce used third-party software to enhance AIS indicator quality with additional context.
- The DoD's actions to mitigate barriers include:

- A DoD component developed internal guidance for sharing CTIs and DMs and established a data governance working group to address the lack of overarching DoD wide guidance and maximize cyber threat information sharing.
- DISA officials stated that they are working with USCYBERCOM, Joint Force Headquarters – DoD Information Network, and the U.S. Air Force Program Management Office to pursue internal technical long-term solutions for the interoperability and automation barriers. DISA is also pursuing commercial short-term solutions to improve the effectiveness and efficiency of information sharing.
- DIA officials stated that they analyzed the cyber threat data in the DMs the agency received from Joint Force Headquarters – DoD Information Network to validate the accuracy of the data before implementing the DMs.
- NGA officials stated that they would implement an automation tool to search for historical data to make cyber threat data more valuable.

- DHS's Cybersecurity and Infrastructure Security Agency implemented the latest STIX 2.1 and TAXII 2.1 capability in March 2022 to improve delivery of indicators and defensive measures to participants. In its latest TAXII 2.1 capability, CISA responded to previously identified quality concerns by introducing an CISA opinion score of all shared indicators to ensure that participants can filter indicators by opinion score and make their own decisions about which indicators to deploy for detection and mitigation measures in their environments. This would reduce the risk of false positives and/or allow participants to triage which alerts to prioritize among the growing volume of alerts within operations teams. CISA continues to work with the cybersecurity vendor community to grow adoption of the latest specifications and increase the number of sharing tools that are interoperable with DHS' capabilities. Further, CISA continues to engage with Federal and non-Federal entities to encourage sharing and document feedback to introduce new future features and capabilities that best encourage sharing of indicators and defensive measures for awareness of the latest cross-sector cyber threats.
- The FBI Cyber Division is evaluating the IC Data Services to store some of the data in a cloud environment for the purpose of access across the IC. This cloud project is in the evaluation phase to understand the benefit and cost of this cloud service. Additionally, the DOJ NCIJTF works with entities to bring their analysts and subject matter experts on-site to review the data.
- Treasury's TSSSOC noted that it mitigates the issue regarding the quality of information received by only ingesting information from higher quality sources that have the best coverage.

APPENDIX A: OBJECTIVES, SCOPE, AND METHODOLOGY

The Offices of Inspector 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 (6 U.S.C. § 1501 et seq.) (the Act) for calendar years 2021 and 2022. 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. As called for in the Act, we assessed:[37]

- The sufficiency of policies and procedures related to sharing cyber threat indicators within the Federal Government.
- Whether cyber threat indicators and defensive measures had been properly classified, and performed an accounting of the security clearances authorized for the purpose of sharing cyber threat indicators or defensive measures with the private sector.
- Actions taken to use and disseminate cyber threat indicators or defensive measures shared with the Federal Government.
- Specific aspects of cyber threat indicators or defensive measures that had been shared with the Federal Government, including:
    - The number of cyber threat indicators or defensive measures shared using the Automated Indicator Sharing capability implemented by Department of Homeland Security (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 this title was used by a Federal entity to prosecute an offense listed in 6 U.S.C. § 1504(d)(5)(A).
    - 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 contained PII.
    - The adequacy of steps taken by the Federal Government to reduce any adverse effect from activities carried out under this title on the privacy and civil liberties of U.S. persons.
- Barriers affecting the sharing of cyber threat indicators or defensive measures.

[37] 6 U.S.C. § 1506(b)(2).

To accomplish the assessment objective, the agencies' auditors:

- Researched applicable laws, policies, regulations, and guidance regarding the sharing of cyber threat information.
- Interviewed entity and component officials to discuss their processes for sharing and receiving cyber threat indicators and defensive measures, 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 examples 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 examples 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 examples 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 examples of cyber threat information shared with and received from other Federal entities, if applicable.
- Interviewed entity officials and tested examples 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 it the draft report for review and comment.

The OIGs for the Departments of Defense, Justice, and Treasury, and the Office of the Director of National Intelligence (ODNI) conducted audits from January 2023 through July 2023 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 their assessments in accordance with the Council of the Inspectors General on Integrity and Efficiency's Quality Standards for Inspection and Evaluation (May 2023), from January 2023 to July 2023. 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
CISA	Cybersecurity and Infrastructure Security Agency
Commerce	Department of Commerce
COTS	Commercial Off The Shelf
CRISP	Cybersecurity Risk Information Sharing Program
CTI	Cyber Threat Indicator
CTIIC	Cyber Threat Intelligence Integration Center
CY	Calendar Year
CYD	Cyber Division
DC3	Department of Defense 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
FLASH	Federal Bureau of Investigation Liaison Alert System
IC	Intelligence Community
ICOAST	Intelligence Community Analysis and Signature Tool
IC IG	Intelligence Community Inspector General
IC SCC	Intelligence Community Security Coordination Center
IP	Internet Protocol
JCSA	Joint Cybersecurity Advisories

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
OIA	Office of Intelligence and Analysis (Department of the Treasury)
OIG	Office of the Inspector General
PII	Personally Identifiable Information
PINs	Private Industry Notifications (FBI product)
STIX	Structured Threat Information eXpression
TAXII	Trusted Automated Exchange of Intelligence Information
TEWI	Treasury Early Warning Indicator
TS	Top Secret
TSSSOC	Treasury Shared Services Security Operations Center
USCYBER COM	United States Cyber Command


INSPECTOR GENERAL
INTELLIGENCE COMMUNITY