OFFICE OF THE INSPECTOR GENERAL OF THE INTELLIGENCE COMMUNITY

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

December 19, 2019 AUD-2019-005-U


INSPECTOR GENERAL
INTELLIGENCE COMMUNITY
INDEPENDENCE • INTEGRITY • PROFESSIONALISM

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

MEMORANDUM FOR: Public Release

SUBJECT: Report No. AUD-2019-005-U, Unclassified Joint Report on the Implementation of the Cybersecurity Information Sharing Act of 2015, December 19, 2019

We are providing this final report for your information and use. Our objective was to provide a joint report on actions taken during Calendar Year 2017 and Calendar Year 2018 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 Statute). The Statute 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 Statute. Each of the Offices of Inspector General assessed its agency's implementation of the Statute 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, classified report—*Joint Report on the Implementation of the Cybersecurity Information Sharing Act of 2015* (AUD-2019-005)—has been provided to the appropriate Congressional Committees and Federal Entity Officials.

We appreciate the courtesies extended to our staffs throughout this review. Please direct questions related to this report to Patti Maccini, Assistant Inspector General for Audit, Office of the Inspector General of the Intelligence Community, at 571-204-8056.

Patti L. Maccini

12/18/19

Patti L. Maccini
Assistant Inspector General for Audit
Office of the Inspector General of the
Intelligence Community

Date

FREDERICK MENY Digitally signed by FREDERICK MENY
Date: 2019.12.18 12:47:15 -05'00'

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

Date

Jacqueline L. Wicecarver

12/18/2019

Jacqueline L. Wicecarver
Deputy Inspector General for Audit
Department of Defense Office of Inspector General

Date

Sarah B. Nelson

2019-12-18

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

Date

Sondra F. McCauley

12/18/19

Sondra F. McCauley
Assistant Inspector General for Audits
Department of Homeland Security Office
of Inspector General

Date

Jason R. Malmstrom

12/18/2019

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

Date

Digitally signed by Deborah L. Harker
DN: c=US, o=U.S. Government, ou=Department of the Treasury, ou=Inspector General, ou=People, serialNumber=625359, cn=Deborah L. Harker
Date: 2019.12.19 08:40:46 -05'00'

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

Date

TABLE OF CONTENTS

EXECUTIVE SUMMARY

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 Statute).[1] The Statute was established to improve cybersecurity in the United States through enhanced sharing of cyber threat information.[2] The Statute creates a framework to facilitate and promote the voluntary sharing of cyber threat indicators[3] and defensive measures[4] among and between Federal and non-Federal entities.[5]

The Statute 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 Statute (*see* Appendix A, Objectives, Scope, and Methodology, of this report for the specific areas to be addressed in the report).[6] 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 Statute for Calendar Year (CY) 2017 and CY 2018 for their respective entities.

The OIGs determined that sharing of cyber threat indicators and defensive measures has improved over the past two years and efforts are underway to expand accessibility to information. Sharing cyber threat indicators and defensive measures increases the amount of information available for defending systems and networks against cyber attacks. In April 2017, the Intelligence Community Security Coordination Center (IC SCC) deployed a capability—the Intelligence Community Analysis and Signature Tool (ICOAST)—to increase sharing of cybersecurity threat intelligence at the top secret security level. According to the Director of IC SCC, the deployment of ICOAST has enabled cyber analysts to more rapidly share high-quality cyber threat information and has enabled analytic collaboration. Also, in CY 2017 and CY 2018, entities continued to share cyber threat information through various reporting means, including email, written reports, and websites. In addition, efforts are underway

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

[2] "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. The term "cyber threat information" is used in this report to refer to both cyber threat indicators and defensive measures.

[3] According to 6 U.S.C. § 1501(6), cyber threat indicators include threat-related information such as methods of defeating or causing users to unwittingly enable the defeat of security controls and methods of exploiting cybersecurity vulnerabilities.

[4] According to 6 U.S.C. § 1501(7)(A), defensive measures include 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] A Federal entity is a department or agency of the United States or any component of such department or agency. 6 U.S.C. § 1501(8). Non-Federal entities include state, local, and tribal governments; private sector companies; and academic institutions. 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. 6 U.S.C. § 1501(14).

[6] 6 U.S.C. § 1506(b)(1).

to further enhance accessibility to cyber threat information and reports included in ICOAST. Given the availability of the secret and unclassified government computing clouds, IC SCC is in the planning and development stages for the deployment of ICOAST instances at the secret and unclassified security classification levels, with the goal of operating at those security classification levels by the end of 2019. Although progress has been made to improve cyber threat information sharing, using the Automated Indicator Sharing (AIS) remains a challenge.[7] Specifically, the number of non-governmental entities using AIS is minimal, and other challenges with AIS information deter its use.

Concerning the specific areas that the Statute requires be assessed and reported on by the OIGs, the auditors determined that the "appropriate Federal entities" continue to implement the Statute.[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 (*i.e.,* the policies and procedures met the legislative requirements of the Statute), with the exception of five Department of Defense (DoD) components.
- Properly classify cyber threat indicators and defensive measures.
- Authorize security clearances for the specific purpose of sharing cyber threat indicators or defensive measures with the private sector.
- Appropriately disseminate cyber threat information that had been shared by Federal and non-Federal entities, and appropriately used that information.
- Share cyber threat indicators and defensive measures in a timely and adequate manner and with appropriate entities.
- Receive cyber threat indicators and defensive measures in a timely and adequate manner.
- Use the Department of Homeland Security capability—AIS—to receive cyber threat indicators or defensive measures, with the exception of six DoD components 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 United States persons from activities carried out under the Statute because there were no known adverse effects.

[7] AIS is the capability developed by the Department of Homeland Security as required by the Statute from which the Federal Government receives cyber threat information in real-time that has been made available by non-Federal entities.

[8] 6 U.S.C. § 1506(b)(2).

- Identified barriers that have hindered sharing of cyber threat indicators and defensive measures, to include:
    - Restrictive classifications limit cyber threat information from being widely shared.
    - Inability of machines to communicate with each other reduces the speed at which cyber threat information sharing occurs.
    - Uncertainty about the protection from liability provided by the Statute impacts the willingness of private sector entities to share cyber threat information.
    - Challenges with AIS information that deter its use.

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 Statute).[9] The Statute was established to improve cybersecurity in the United States through enhanced sharing of cyber threat information.[10] The Statute creates a framework to facilitate and promote the voluntary sharing of cyber threat indicators[11] and defensive measures[12] among and between Federal and non-Federal entities.[13]

The Statute 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 Statute 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 cyber threat indicators and defensive measures.

Other key provisions in the legislation include protection from liability for private entities that share cybersecurity information in accordance with established procedures, and the protection of privacy and civil liberties when implementing the Statute. Specifically, the Statute 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 Statute does not create any duty to share cyber threat indicators or defensive measures and does not impose a duty to warn or act based on the receipt of shared information. Subject to exceptions, the Statute will sunset on September 30, 2025.

Offices of Inspectors General Reporting Requirement

Section 107(b) of the Statute 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 years—on the actions taken over the most recent two-year period to carry out the Statute.[15] Section 107(b) of the Statute requires the biennial report to include an assessment that determines:[16]

[9] *See supra* note 1.

[10] *See supra* note 2.

[11] *See supra* note 3.

[12] *See supra* note 4.

[13] *See supra* note 5.

[14] The Statute speaks to the removal of "personal information" from cyber threat indicators and defensive measures. This information is commonly referred to as personally identifiable information (PII).

[15] *See supra* note 6.

[16] *See supra* note 8.

- The sufficiency of policies and procedures related to sharing cyber threat indicators within the Federal Government.

- Whether cyber threat indicators and defensive measures have been properly classified, as well as an accounting of the security clearances authorized for the purpose of sharing cyber threat indicators or defensive measures with the private sector.

- The appropriateness, adequacy, and timeliness of the 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 have been shared with the Federal Government, including:

    - The number of cyber threat indicators or defensive measures shared using the capability implemented by the DHS [Automated Indicator Sharing].

    - 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 section 105(d)(5)(A).[17]

    - 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 United States persons.

- Barriers affecting the sharing of cyber threat indicators or defensive measures.

[17] According to Section 105(d)(5)(A) of the Statute, 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. 6 U.S.C. § 1504(d)(5)(A).

Entities Reviewed

For this assessment, the Offices of Inspectors General (OIGs) reviewed their agencies' components responsible for sharing, receiving, or disseminating cyber threat indicators and defensive measures during Calendar Year (CY) 2017 and CY 2018 as follows:

Department of Commerce. Commerce has many bureaus that fall under its organizational structure. The Department of Commerce's Enterprise Security Operation Center serves as the focal point for many security operations, to include interfacing with the individual bureau Security Operation Centers and receiving cyber threat information from AIS. Some bureaus operate their own Security Operation Centers and others rely on Commerce's Enterprise Security Operations Center.

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:

- DoD Cyber Crime Center (DC3) is a technical center for digital and multimedia forensics, cyber investigative training, technical solutions development for cyber security, and cyber analytics. As the DoD's operational focal point for the Defense Industrial Base (DIB) Cybersecurity (CS) program, DC3 officials receive cyber threat reports from defense contractors and voluntary non-Federal participants using the DoD-DIB Collaborative Information Sharing Environment. DC3 officials analyze the reported cyber threats and share reports with the DIB CS program participants for their cyber situational awareness and threat mitigation strategies. DC3 officials also share cyber threat reports with Federal entities on Intelink.[18]

- Defense Intelligence Agency (DIA) is responsible for development, implementation, and operation of a secure information technology infrastructure and an assured data environment for all source intelligence.

- Defense Information Systems Agency (DISA) is a combat support agency that provides information sharing capabilities to joint warfighters, national-level leaders, and other mission and coalition partners across the full spectrum of DoD operations.

- Defense Counterintelligence and Security Agency (DCSA) provides security and counterintelligence support services to DoD and 31 other Federal entities, including law enforcement, intelligence community partners, and cleared contractors participating in the National Industrial Security Program (NISP).[19] DCSA receives suspicious incident reporting from cleared contractors, and proactively develops cyber vulnerability and anomalous threat information affecting unclassified cleared industry networks. DCSA shares actionable cyber threat information with Federal entities and cleared industry through cyber threat alert products, a formal referral process, and

[18] Intelink is a set of web-based services, tools, technologies, and information repositories that allow classified and unclassified intelligence and related information sharing between intelligence producers and consumers.

[19] The NISP, established under Executive Order 12829, serves as the single integrated, cohesive industrial security program to protect classified information.

intelligence community protocols. DCSA integrates all cyber threat reporting into the Federal Bureau of Investigation (FBI) Cyber Guardian.[20]

- National Geospatial-Intelligence Agency (NGA) identifies cyber threat information through automated tools that monitor the NGA network, and then shares the information through email, posting reports to classified websites, and uploading to a classified capability.

- National Reconnaissance Office (NRO) identifies cyber threat information through automated tools that monitor the NRO network, and then shares the information using a classified capability.

- National Security Agency (NSA) receives and disseminates information relevant to cybersecurity at the top secret, secret, and unclassified levels. NSA receives cyber threat information through Signal Intelligence (SIGINT) collection, cybersecurity operations, foreign partners, open source information, and commercial arrangements regarding foreign cyber threats. The information from all of these sources may assist the NSA's cybersecurity mission to help protect DoD information networks and other national security systems.

- United States Cyber Command (USCYBERCOM) unifies the direction of the DoD cyberspace operations by focusing on defending DoD information networks, providing support to combatant commanders for execution of their missions around the world, and strengthening the Nation's ability to withstand and respond to cyber attacks.

Department of Energy (DOE). DOE shares cyber threat information with DHS and the energy industry in near real-time. In addition, DOE participates in the monthly Integrated Cyber Defense Working Group, which analyzes cyber threat indicators and discusses the effectiveness of cybersecurity, technical management of cybersecurity threats, best practices, and information sharing issues.

Department of Homeland Security. DHS's Cybersecurity and Infrastructure Security Agency (CISA) leads the national effort to defend critical infrastructure against cyber threats by working with partners across all levels of government and in the private sector to protect against evolving risk. CISA manages the AIS program, which enables the real-time exchange of cyber threat indicators and defensive measures between Federal Government and private sector partners to improve protection against cyber attacks. The National Cybersecurity and Communications Integration Center (NCCIC), within CISA, serves as a central location where a diverse set of partners involved in cybersecurity and communications protection coordinate and synchronize their efforts. NCCIC's partners include other government agencies, the private sector, and international entities. NCCIC and its partners analyze cybersecurity and communications information, share timely and actionable information, and coordinate response, mitigation, and recovery efforts.

Department of Justice (DOJ). Two components within the DOJ are responsible for sharing cyber threat information. The Justice Security Operations Center (JSOC) is responsible for sharing cyber threat information. JSOC works with DOJ components to prevent, detect, and respond to cyber attacks and espionage against the Department. JSOC shares cyber threat indicators with other Federal entities and the

[20] Cyber Guardian is an FBI system that tracks the production, dissemination, and disposition of cyber victim notifications and is accessible by all National Cyber Investigative Joint Task Force participants. Cyber Guardian is being replaced by CyNERGY.

private sector. The National Cyber Investigative Joint Task Force (NCIJTF)—within the 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 used by ODNI. The following three components within ODNI are responsible for sharing and receiving cyber threat information with other Federal entities.

- Intelligence Community Security Coordination Center (IC SCC) leads the information technology transformation and protection of the Intelligence Community Information Environment. The IC SCC obtains cyber threat information from various sources, including other Intelligence Community entities, and shares the cyber threat information within ODNI and with other Federal entities, including Intelligence Community entities. The IC SCC is the only United States federal cyber center that integrates the counterintelligence and computer network defense disciplines.

- Cyber Threat Intelligence Integration Center (CTIIC) produces coordinated Intelligence Community analysis of foreign cyber threats to United States national interests, ensures that information is shared among the Federal cyber community, and supports the work of departments/agencies and policy makers with timely intelligence about significant cyber threats and threat actors. CTIIC products are available to the Intelligence Community on a classified website.

- The National Intelligence Council leads analysis across the Intelligence Community to inform immediate and long-term policy deliberations. The National Intelligence Council develops multiple written products that can contain cyber threat information, which are shared via email and are available on a classified website.

Department of the Treasury. Two components within the Department of the Treasury (Treasury), the Government Security Operations Center (GSOC) and the Cyber Information Group (CIG)/Office of Cybersecurity and Critical Infrastructure Protection (OCCIP), are responsible for sharing cyber threat indicators for Treasury. GSOC shares cyber threat indicators with the Financial Services – Information Sharing and Analysis Center (FS-ISAC),[21] US-CERT Homeland Security Information Network (HSIN) portal,[22] and all Treasury bureaus' Security Operation Centers. CIG/OCCIP analyzes information related to cyber threats to the financial services sector received from Treasury's Office of Intelligence and Analysis (OIA), the Financial Crimes Enforcement Network (FinCEN), and Federal law enforcement sources. CIG/OCCIP repackages the unclassified cyber threat information into CIG Circulars before sharing it with the financial services sector, Federal and non-Federal partners, and cybersecurity centers, such as NCCIC.

[21] FS-ISAC is a member-owned non-profit association of financial services firms that creates and develops processes for detecting and providing information on physical or cyber security risks.

[22] The US-CERT HSIN portal is available to Federal, state, and local government agencies and contractors supporting Federal entities.

ASSESSMENT RESULTS

Sharing of Cyber Threat Indicators and Defensive Measures within the Intelligence Community Has Improved Over the Past Two Years and Efforts Are Underway to Expand Accessibility to Information, but Sharing by the Private Sector Using the Automated Indicator Sharing Capability Remains a Challenge

Progress in Sharing Cyber Threat Information Among Federal Entities

In CY 2017 and CY 2018, the "appropriate Federal entities" made progress enhancing accessibility to cyber threat information for improved sharing of information with other Federal entities. Cyber threat reporting serves two distinct audiences: policy decision-makers and cyber defenders. Sharing cyber threat indicators and defensive measures increases the amount of information available for defending systems and networks against cyber attacks.

In April 2017, ODNI's Intelligence Community Security Coordination Center deployed a capability—the Intelligence Community Analysis and Signature Tool (ICOAST)—to increase sharing of cybersecurity threat intelligence at the top secret security level, including Indicators of Compromise[23] and malware signatures.[24] Information is shared among Federal entities with officials having the appropriate security clearance. As of August 2019, ICOAST had several thousand Intelligence Community, DoD, and other Federal users, with approximately 70 percent having read-only access and 30 percent having an input role. Four "appropriate Federal entities" and some of their components upload cyber threat information to ICOAST. Cyber threat indicators and defensive measures obtained from technical capabilities, email distributions, paid commercial sources, and open source are input to ICOAST by IC SCC analysts, as well as ICOAST authorized users from other Federal entities. ICOAST users can download defensive measures into a report for immediate action. IC SCC produces Correlation Reports with aggregated technical data from ICOAST, such as Indicators of Compromise, and provides insight to previously unknown threat actors' Tactics, Techniques, and Procedures (TTPs). The Correlation Reports include analytical comments detailing the relevance of the aggregated technical data. According to the Director of IC SCC, the deployment of ICOAST has enabled cyber analysts to more rapidly share high-quality cyber security information, which includes contextual data lacking in other threat indicator data sets, and has improved cyber analytic collaboration.

Over the past two years, various websites have increased the amount of shared cybersecurity information. IC SCC maintains a website on the top secret network containing various reports on the security of and vulnerabilities with information technology infrastructure. Reports and other information (*i.e.*, products) specifically related to cybersecurity that are available on the website include: ICOAST Correlation Reports, Situational Awareness Reports, Monthly Activity Reports, Vulnerability Reports, Network Activity Notices, Tippers, and Blogs. Officials with access to the top secret network can obtain and use this information. IC SCC reports are also made available on a DIA sharing website on the top secret network. Also, beginning in July 2018, ODNI's Cyber Threat Intelligence Integration Center products, which were previously emailed to recipients, were made available on an NSA website for users with appropriate security clearances to access the top secret network on which the website is maintained.

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

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

The NSA website also has intelligence reports, which can include cyber threat information, from NSA, USCYBERCOM, and NGA. Both DIA and NSA websites replicate secret and below reporting to an instance on the secret domain to allow greater access to the information.

Continuing Efforts for Sharing Cyber Threat Information

The "appropriate Federal entities" continue to share cyber threat information through various reporting means, including email, written reports, and websites. Specifically:

- ODNI, ODNI's service provider, and several DoD components email reports on cyber security vulnerabilities to Intelligence Community recipients using established classified networks. Two DoD components and NCIJTF also provide cyber threat information to the Intelligence Community.

- ODNI's CTIIC and National Intelligence Council create documents containing cyber threat information that are distributed through email or Intelligence Community classified websites. For example, CTIIC produces a daily summary that provides situational awareness on cyber security threats to Intelligence Community agencies, policymakers, and the White House. In addition, CTIIC produces a weekly cyber security threat report for Congressional Intelligence Committees as well as other reports concerning specific cyber events.

- ODNI's IC SCC designs and conducts an annual cyber security exercise: ICE STORM. One goal of the ICE STORM exercise is to share cyber information with participants from Intelligence Community agencies, DoD, and law enforcement, as well as with international partners.

- Several DoD components and the Departments of Energy, Homeland Security, and Justice use AIS to share cyber threat information.

- Since 2015, DoD's DCSA has been developing a unique machine-learning assisted analysis process for detecting atypical cyber behavior and enhancing cyber threat data. The cyber threat information is shared with cleared contractors and other government entities and provided to Federal and DoD law enforcement and counterintelligence entities for investigation.

Plans to Expand Cyber Threat Information Sharing

Efforts are underway to further enhance accessibility to cyber threat information and reports. ODNI's IC SCC officials told the auditors that they are striving to provide cyber threat information to other Federal entities at the secret and unclassified security classification levels. Given the availability of the secret and unclassified government computing clouds, IC SCC is in the planning and development stages for the deployment of ICOAST instances at the secret and unclassified security classification levels. At the secret and unclassified levels, the ICOAST instances will interface with multiple DoD components and other Federal entities that have the responsibility for distributing cyber threat information to Federal, state, and local entities and the private sector. IC SCC officials told the auditors that personnel are needed to modify the software for deployment, extract the secret and unclassified data from ICOAST on a periodic basis, perform quality assurance checks, and transmit the information to the secret and unclassified instances of ICOAST. An official of IC SCC told the auditors that the goal is to deploy ICOAST on the secret and unclassified computing clouds by the end of 2019. The Fiscal Year 2020 budget request includes additional resources for the ICOAST project. In addition, IC SCC is working with DoD and

DHS's CISA to develop indicator sharing interfaces at the top secret, secret, and unclassified security classification levels. According to CISA officials, DHS has undertaken efforts to increase the context and enrichment of AIS data to facilitate integration with ICOAST.

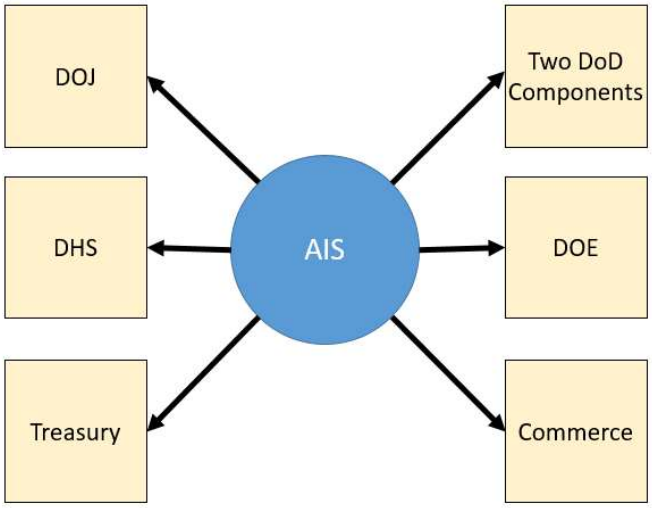
Sharing Cyber Threat Indicators and Defensive Measures by the Private Sector Using the Automated Indicator Sharing Capability Remains a Challenge

The number of non-government organizations using the AIS capability to share cyber threat indicators is minimal. As a result, the goal of the Statute of having companies share threat information using the capability is not being fully achieved. AIS, developed in 2016 by DHS to comply with the requirements of the Statute, is designed to be the primary mechanism by which private sector companies share cyber threat information. AIS enables the near real-time exchange of cyber threat indicators and defensive measures between Federal Government and private sector partners intended to improve protection against cyber attacks.

As of December 2018, 252 federal and non-federal entities and 13 international computer emergency response teams were connected to receive cyber threat information from AIS. However, DHS has only experience a slight increase in the number of data producers sharing cyber threat indicators and defensive measures using AIS and, as of June 2019, only four Federal and six non-Federal entities used AIS to share cyber threat information. DHS reported that the limited number of participants who input cyber threat information to AIS is the main barrier for DHS to improve the quality of the indicators with more actionable information to mitigate potential cyber threats. In its efforts to increase participation, DHS has developed the AIS Engagement Plan that calls for identifying and recruiting targeted partners and helping entities that are not sharing information with DHS to overcome their challenges through a series of webinars focused on providing information about AIS. Figure 1 illustrates the "appropriate Federal entities" and their components who received cyber threat information from the private sector through AIS in CY 2017 and CY 2018.

According to some of the entities subject to this assessment, barriers to sharing cyber threat information involve the use of AIS information. For example, some entities told the auditors that the cyber threat indicators coming from AIS did not contain the context needed to determine why the indicator was an issue. As a result, the entities did not know what actions to take based on the information received from AIS without performing additional research. (*See* section "Barriers to Sharing Cyber Threat Information" of this report for a discussion on the challenges with sharing information using AIS.) According to CISA officials, in 2017, DHS began adding context to AIS data from more than 90 different data feeds and two data enrichment sources.

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



Source: Auditor-generated based on information obtained by the OIGs.

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

- The Cyber Information Sharing and Collaboration Program (CISCP) enables actionable, timely unclassified information exchange through trusted public-private partnerships across all critical infrastructure sectors. CISCP partners have access to DHS and National Cybersecurity and Communications Integration Center services. The analyst-to-analyst sharing of threat and vulnerability information allows partners to proactively detect, prevent, mitigate, respond to, and recover from cybersecurity incidents.

- The Cybersecurity Risk Information Sharing Program (CRISP), managed by the Electricity Information Sharing and Analysis Center (E-ISAC) 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 CRISP. Electric utilities participating in the program account for about 75 percent of the United States' electric customers.

- The Defense Industrial Base (DIB) Cybersecurity (CS) program was established in 2013 as a bilateral cybersecurity information sharing activity, in which DoD components provide cyber threat reports to DIB partners to enhance their capabilities for safeguarding DoD's unclassified information, and DIB partners report certain types of cyber intrusion incidents to the DoD-DIB Collaborative Information Sharing Environment. The DIB partners are private companies that own systems where DoD's unclassified information resides and have entered into an agreement with DoD to mutually share cyber threat reports using the DoD-DIB Collaborative Information Sharing Environment.

Results for "Oversight of government activities:" Implementation of the Statute

The Statute requires the OIGs of the "appropriate Federal entities" to assess specific areas concerning the implementation of the Statute, as follows:[25]

Sufficiency of Policies and Procedures

The Statute 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."[26] The OIGs determined that the policies, procedures, and guidelines used by the "appropriate Federal entities" for sharing cyber threat indicators within the Federal Government were sufficient, with the exception of five DoD components (*see* Table 1 for details). Policies and procedures establish the processes and boundaries within which an organization should be operating.

The Statute 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 cyber threat indicators and defensive measures consistent with the protection of classified information, intelligence sources and methods, and privacy and civil liberties. In response to the Statute, the following four documents were developed and publicly issued:

- Document 1: *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, including the use of the AIS capability.

- Document 2: *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 3: *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 cyber threat indicators and defensive measures with Federal entities and describes the protections non-Federal entities receive under the Statute.

- Document 4: *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 cyber threat indicators and defensive measures. The procedures include details on existing government programs that facilitate the sharing of information on cybersecurity threats and the periodic publication of cybersecurity best practices.

[25] *See supra* note 7.

[26] 6 U.S.C. § 1506(b)(2)(A).

Section 105(d)(5)(C) of the Statute requires that the cyber threat indicators and defensive measures provided to the Federal Government under the Statute be retained, used, and disseminated in accordance with Document 1 and Document 2. The entities do not 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 Statute. 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. Consistent with the Statute's framework of voluntary sharing, other documents encourage the sharing of cyber threat information, such as:

- *Guiding Principles for Sharing Classified National Intelligence with US Entities.* This guidance, issued by ODNI, provides implementation guidance to the Executive Branch. It establishes DHS and FBI as principally responsible for overseeing and ensuring the dissemination of classified national intelligence information to United States entities, to include state, local, and tribal governments and private sector entities. The guidance also requires that sharing of classified national intelligence information with United States entities shall routinely include cyber threats to United States infrastructures.

- *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 Pathfinder Initiative*. This memorandum was signed by the Secretaries of Defense and DHS in October 2018 to improve the protection and defense of the United States homeland from strategic cyber threats. The memorandum defines DoD's responsibility to support efforts to protect Defense critical infrastructure and the DIB networks and systems from malicious cyber activity that could undermine the United States military. Specifically, the memorandum outlined DoD's role to defend against cyber threats, and DHS's role to oversee national preparedness and protect critical infrastructure. The memorandum also identified joint principles across DoD and DHS missions and addressed improving joint operations planning and coordination, among other initiatives.

The Statute required the Government Accountability Office (GAO) to submit a report to Congress, not later than three years after the date of the Statute's enactment, that assessed the sufficiency of the policies, procedures, and guidelines established under the Statute 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 Statute's provisions and concluded that ODNI and the six other designated Federal agencies developed policies, procedures, and guidelines that met all the Statute's provisions relevant to the removal of personal information from cyber threat indicators and defensive measures.

[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).

The OIG auditors assessed the "appropriate Federal entities" using Document 1 and 2 as having sufficient policies, procedures, and guidelines. The Departments of Energy, Homeland Security, and Justice, and two DoD components use and adhere to Documents 1 and 2. In addition, another DoD component used Document 2, but did not need to use Document 1 because it did not receive cyber threat indicators from AIS in CY 2017 or CY 2018. The entities included in Table 1 use agency-specific policies, procedures, and guidelines. The auditors tested the agency-specific policies, procedures, and guidelines to determine whether they were sufficient.[29] The results of the auditors' testing are provided in Table 1. The Department of Commerce does not share cyber threat information with other Federal entities; therefore, Commerce OIG did not need to assess the sufficiency of the documents.

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
Defense	No	Instead of Document 2, five of the eight DoD components use agency-specific policies and procedures but they are not sufficient because they do not include the Statute's requirements for safeguarding and removing PII or notifying entities when information received under the Statute does not constitute a cyber threat. The five DoD components do not need to use Document 1, because they do not receive cyber threat indicators from AIS.
ODNI	Yes	ODNI and its service provider use agency-specific guidance for handling PII, instead of Document 2. ODNI and its service provider do not use Document 1 because they do not receive cyber threat indicators from AIS.
Treasury	Yes	GSOC and CIG/OCCIP use agency-specific policies, procedures, and practices that align with Documents 1 and 2.

Source: Auditor-generated based on information obtained by the OIGs.

The Statute 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] DHS reported that the heads of the "appropriate Federal entities" reviewed and updated the Privacy and Civil Liberties Guidelines in June 2018.

[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 this Statute 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 Statute did not constitute a cyber threat.

[30] 6 U.S.C. § 1504(b)(2)(B).

Proper Classification of Cyber Threat Indicators and Defensive Measures, and Authorization of Security Clearances

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

Proper Classification of Cyber Threat Indicators and Defensive Measures

ODNI, ODNI's service provider, and the Departments of Defense and Homeland Security properly classify cyber threat indicators and defensive measures. Based on the auditors' testing of a sample of cyber threat indicators and defensive measures, the documents had appropriate portion marks and overall classifications that were consistent with the sources, references, or embedded links used for the content. According to entity 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.

The Departments of Commerce, Energy, Justice, and the Treasury OIGs did not need to determine whether the shared cyber threat information was properly classified.

- The Departments of Commerce, Energy, and Justice do not share any classified cyber threat indicators or defensive measures.

- The Treasury's GSOC does not share classified information. Treasury's CIG/OCCIP shares unclassified CIG Circulars and also holds classified meetings for sharing cybersecurity information with financial services sector officials who already have active security clearances issued by other Federal entities or DHS's Private Sector Clearance Program for Critical Infrastructure. The information discussed at the classified meetings is not actionable. CIG/OCCIP retains the original classification of information received.

[31] 6 U.S.C. § 1506(b)(2)(B).

Authorization of Security Clearances

The Departments of Energy, Homeland Security, and Justice accounted for the number of security clearances authorized for the purpose of sharing cyber threat information with the private sector.[32]

- The DOE authorized and accounted for security clearances in CY 2017 and CY 2018, specifically for sharing information with the private sector under the Statute. Although DOE does not share classified cyber threat information with the private sector, some private sector individuals need security clearances, if based on their roles, they may access or come in contact with information that is sensitive or classified.

- The DHS authorized 129 security clearances in 2017 and 155 in 2018 to private sector partners participating in DHS's various information sharing programs, to include cyber threat information.

- The DOJ authorized four active clearances in CY 2017 and 12 in CY 2018 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.

The ODNI and its service provider and the Departments of Commerce, Defense, and the Treasury do not authorize security clearances for the purpose of sharing cyber threat information with the private sector.

- The Department of Commerce does not share classified cyber threat indicators or defensive measures with the private sector.

- Two DoD components share classified cyber threat information with DoD contractors who already have the appropriate security clearances. The auditors verified that 83 of the DoD contractors who received classified cyber threat information in CY 2017 and CY 2018, had the appropriate security clearances.

- ODNI does not share classified cyber threat information with the private sector, and ODNI's service provider only shared classified cyber threat information with private sector officials who already had the appropriate security clearances.

- The Treasury's GSOC does not share classified information with the private sector and CIG/OCCIP holds classified meetings to share cyber threat information with financial services sector officials, representatives, and regulators, who already have the appropriate security clearances issued by other Federal entities or 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.

Actions Taken by the Entities Based on Cyber Threat Indicators and Defensive Measures Shared with Them

The Statute 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 "appropriate Federal entities" appropriately disseminate and use cyber threat indicators or defensive measures that have been shared by Federal and non-Federal entities within the agency. Upon receipt of information that has been shared by other Federal and non-Federal entities, the "appropriate Federal entities" disseminate relevant information to officials responsible for the security controls of the entities' systems, networks, and enclaves. Cyber threat information is considered appropriately disseminated when the information is shared with individuals having the proper security clearance and need to know, 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 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 disseminates shared cyber threat information internally to the bureaus using the Commerce Threat Intelligence Portal. Each bureau can also upload cyber threat indicators and defensive measures to the portal.
Defense	Yes	Seven of the eight DoD components[34] disseminate cyber threat information to other entities within DoD through using email and phone calls at various intervals, such as on a daily or weekly basis, or as-needed. [35]

[33] 6 U.S.C. § 1506(b)(2)(C).

[34] According to NSA officials, NSA did not disseminate or use information shared with it under the Statute during CY 2017 and CY 2018 because AIS information was not successfully ingested into NSA's mission repositories until March 2019. Throughout this report, NSA responses are limited to the information shared through AIS. NSA understands the assessment was intended to examine entities' implementation of the Statute and to assess their compliance with the Statute for such implementing activities. NSA officials reiterated that the only activity NSA carried out to help implement the Statute in CY 2017 and CY 2018 was sharing cyber threat indicators through AIS. Therefore, disseminating, sharing, and receiving of AIS information were the only activities NSA reported on in this assessment.

[35] Some DoD components did not keep records of cyber threat indicators received; therefore, the auditors tested information disseminated by the DoD components regardless of whether it was obtained internally or externally.

Entity Name	Information Disseminated and Used Was Assessed Appropriate by the Auditors	Dissemination and Use of Cyber Threat Information
Energy	Yes	DOE disseminates shared cyber threat information across the DOE enterprise using the Cyber Fed Model, which provides machine-to-machine sharing in near real-time.
Homeland Security	Yes	DHS internally disseminates shared unclassified cyber threat information using AIS and shared classified cyber threat information using Enhanced Cybersecurity Services (ECS).[36]
Justice	Yes	DOJ disseminates shared cyber threat information to their components through various means, such as emails, security advisories, web portals, cyber threat intelligence forums, and meetings. NCIJTF only disseminates information relevant to possible operational opportunities already shared by the originating agency, and NCIJTF officials told the auditors that disseminating to a wider audience could allow NCIJTF to mitigate potential threats.
ODNI	Yes	ODNI and its service provider disseminate shared cyber threat information using email and meetings.
Treasury	Yes	GSOC disseminates shared cyber threat information by issuing Treasury Early Warning Indicators (TEWIs) related to threats detected against Treasury's network and distributes them within Treasury.[37]

Source: Auditor-generated based on information obtained by the OIGs.

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

The auditors determined that the "appropriate Federal entities" shared cyber threat indicators and defensive measures in a timely and adequate manner with appropriate Federal entities. 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 cyber threat indicators or defensive measures, 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 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.

[36] DHS's ECS capability shares sensitive and classified cyber threat information with accredited ECS commercial service providers to detect and block malicious cyber activity from entering or exiting customer networks.

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

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 does not share cyber threat information with other Federal entities.
Defense	Yes	The eight DoD components share cyber threat information with the Intelligence Community or other Federal entities by distributing reports on various websites, conducting meetings, and using capabilities, such as ICOAST, IntelShare,[38] HighPoint,[39] Fight by Indicator system,[40] BIFROST,[41] AIS, and Cyber Guardian.
Energy	Yes	The DOE's Cyber Fed Model connects to AIS and uploads cyber threat indicator data every 15 minutes, which are then redistributed to Federal entities. In addition, DOE's Cyber Fed Model uploads cyber threat information in near real-time to the Cybersecurity Risk Information Sharing Program (CRISP) to share cyber threat information throughout the energy industry.
Homeland Security	Yes	DHS shares unclassified cyber threat indicators and defensive measures with 33 Federal departments and agencies using AIS, CISCP, and FedGov data feeds. DHS shares classified cyber threat indicators using ECS. DHS shares unclassified cyber threat information using AIS when the information is received. If an automated privacy review indicates the need for a human review of potential privacy sensitive information, DHS marks the fields as "under review" and shares all other available information. DHS then releases the remaining appropriate and relevant information as quickly as operationally practicable after the human review is complete.

[38] IntelShare is a system used to facilitate collaboration within the Intelligence Community and is located on the platform, Intelink.

[39] Highpoint is a United States European Command (USEUCOM)-hosted intelligence production, authoring, and dissemination environment on the top secret and secret networks

[40] The Fight by Indicator capability allows analysts to detect indicators, develop countermeasures, and generate customized reports.

[41] The BIFROST capability allows analysts to share unclassified indicators with AIS.

Entity Name	Sharing Information Was Assessed as Timely, Adequate, and Appropriate by the Auditors	Sharing Cyber Threat Information
Justice	Yes	JSOC uses an automated tool to share cyber threat information with the private sector and other Federal entities, including DHS. NCIJTF coordinates the sharing of classified and unclassified cyber threat indicators and defensive measures relevant to various efforts between Federal entities. NCIJTF shares cyber threat information using email, video teleconference, phone, and in-person meetings. NCIJTF also integrates and makes cyber intrusion and enrichment data accessible to on-site, multi-agency analysts and staff using Lighthouse;[42] publishes NCIJTF reports and products to the Intelligence Community using an NSA-operated intelligence sharing platform; and distributes cyber incident reports and updates to FBI field offices, cyber centers, and the private sector when applicable using Cyber Guardian and other mechanisms.
ODNI	Yes	ODNI and its service provider share cyber threat indicators and defensive measures by uploading cyber threat information and reports to ICOAST and websites available on top secret and secret networks and providing the information using email. According to ODNI officers, ODNI components attempt to share cyber threat information with Federal entities within 24 hours. 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 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.

[42] Lighthouse is an internal analytical platform of integrated cyber data from multiple agencies, including DHS's AIS, housed at NCIJTF.

Entity Name	Sharing Information Was Assessed as Timely, Adequate, and Appropriate by the Auditors	Sharing Cyber Threat Information
Treasury	Yes	GSOC shares cyber threat indicators within the Federal Government using the US-CERT Homeland Security Information Network portal. When GSOC analysts determine the cyber threat indicators and defensive measures are significant, a TEWI is developed and shared within a reasonable timeframe with other Federal entities. CIG/OCCIP analyzes cyber threat information received from Treasury's Office of Intelligence and Analysis (OIA), FinCEN, and Federal law enforcement sources. The cyber threat information is included in unclassified CIG Circulars, which are shared with the financial services sector using the HSIN and FS-ISAC portals.

Source: Auditor-generated based on information obtained by the OIGs.

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

The auditors determined that the "appropriate Federal entities" receive cyber threat indicators and defensive measures 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 as quickly as operationally possible, and it is considered adequate when it encompasses relevant and meaningful cyber threat indicators or defensive measures, and when the information is safeguarded from unauthorized access. The 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 receives cyber threat information from other Federal entities through AIS.
Defense	Yes	Seven of the eight DoD components[43] receive cyber threat information from other Federal entities.[44] The DoD components receive cyber threat information through emails, phone calls, and meetings, as well as from multiple capabilities, such as HighPoint, Cyber Guardian, AIS, IntelShare, Fight by Indicator, BIFROST, and DCSA's cyber intelligence predictive analysis process. After receiving the cyber threat information, the DoD components may perform research and enhance it by adding more useful or actionable information before sharing it with other entities. Officials of the DoD components generally consider the cyber threat information they receive as useful; however, they told the auditors that the information needs to have context or sufficient details to be actionable. Officials told the auditors that it is challenging to have both useful and timely information due to additional research that is necessary to make the information meaningful.
Energy	Yes	DOE receives cyber threat information from other Federal entities through connecting to AIS and then redistributes the information across the enterprise and to private sector entities. DOE also receives cyber threat information from ICOAST and uses that information to respond to threats, specifically malware targeting the Intelligence Community.
Homeland Security	Yes	DHS receives cyber threat information from other Federal entities, such as DOE and NSA, after the Federal entities upload cyber threat indicators and defensive measures into AIS.
Justice	Yes	DOJ receives cyber threat information from an application, an NSA website, and Cyber Guardian. DOJ also receives cyber threat information from ICOAST on the top secret network and uses the information for research, investigations, and secure internal sharing.

[43] NSA did not report receiving cyber threat information from other entities because the information from AIS was not ingestible into NSA repositories during CY 2017 and CY 2018, and NSA only reported on sharing cybersecurity threat indicators through AIS (*see supra* note 34).

[44] Some DoD components did not keep records of cyber threat indicators received; therefore, the auditors tested the information regardless of whether it was obtained internally or externally.

Entity Name	Information Received Was Assessed as Timely and Adequate by the Auditors	Receiving Cyber Threat Information
ODNI	Yes	ODNI and its service provider receive cyber threat information in real time or otherwise in an adequate and timely manner, considering time needed for additional research to incorporate context. The information comes from ICOAST, Intelligence Community websites, and emails. According to an official of IC SCC, it is difficult to produce cyber threat information that is both real time and relevant because in order for the information to be relevant, time is needed to perform the research to add context. Some component officials told the auditors that they could always use more cyber threat information.
Treasury	Yes	GSOC receives unclassified cyber threat information from emails and AIS. Based on work performed by DHS auditors, the AIS information was shared in a timely and adequate manner. CIG/OCCIP receives cybersecurity information from Treasury's OIA, FinCEN, and Federal law enforcement sources.

Source: Auditor-generated based on information obtained by the OIGs.

Specifics Concerning the Sharing of Cyber Threat Indicators or Defensive Measures

The Statute requires "an assessment of the cyber threat indicators or defensive measures shared with the appropriate Federal entities," to include (i) the number of cyber threat indicators or defensive measures shared through the use of the Automated Indicator Sharing (AIS) capability; (ii) handling information not directly related to a cybersecurity threat that is known at the time of sharing to contain PII; (iii) the number of times shared information was used to prosecute an offense; (iv) the impact on privacy and civil liberties; and (v) the steps taken to reduce adverse effects on privacy and civil liberties.[45]

Use of the Automated Indicator Sharing Capability

The Statute requires OIGs to determine the number of cyber threat indicators or defensive measures shared using the AIS capability implemented by the Department of Homeland Security.[46] The following entities receive cyber threat indicators and defensive measures using AIS:

- Commerce received cyber threat indicators from AIS but the number could not be determined because Commerce did not track the information.

- Two DoD components received cyber threat indicators from AIS. However, neither component was able to provide an exact number of cyber threat indicators and defensive measures received for CY 2017 and CY 2018.

[45] 6 U.S.C. § 1506(b)(2)(D).

[46] *Id*. at § 1506(b)(2)(D)(i).

- DOE officials indicated that the Department received over 1 million cyber threat indicators and defensive measures in CY 2017 and over 3 million in CY 2018 from AIS.

- DHS received over 900,000 cyber threat indicators in CY 2017 and over 4 million cyber threat indicators in CY 2018 from AIS. DHS subsequently shared the indicators received with other Federal entities.

- DOJ received over 300,000 cyber threat indicators in CY 2017 and over 600,000 in CY 2018 from AIS. DOJ receives cyber threat indicators from AIS through a commercial off-the-shelf automated tool that receives and processes indicator information from AIS.

- Treasury received over 1.1 million cyber threat indicators and defensive measures from AIS in CY 2017 and CY 2018.

ODNI, ODNI's service provider, and six DoD components did not obtain cyber threat indicators or defensive measures from AIS in CY 2017 and CY 2018.

Handling Information Containing Personally Identifiable Information

The Statute 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 Statute or the guidelines.[47] According to officials of ODNI and its service provider, and officials of the Departments of Commerce, Defense, Energy, Homeland Security, Justice, and the Treasury, 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 Statute requires the OIGs' report to address the number of times, according to the Attorney General, that information shared under the Statute was used by a Federal entity to prosecute an offense listed in section 105(d)(5)(A) of the Statute.[48] DOJ officials told the auditors that crediting a case solely on information shared under the Statute is not measurable because information gathered to prosecute an offense may come from multiple sources, including the Statute.[49]

[47] 6 U.S.C. § 1506(b)(2)(D)(ii).

[48] *Id*. § 1506(b)(2)(D)(iii).

[49] The determination of the number of times, according to the Attorney General, that information shared under the Statute was used by a Federal entity to prosecute an offense will be determined solely by the Office of the Inspector General of the Department of Justice.

Effects of Sharing on Privacy and Civil Liberties

The Statute 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."[50] Officials of the Departments of Commerce, Defense, Energy, Homeland Security, Justice, and 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.[51] During testing, such instances did not come to the auditors' attention. In 2017, the Department of the Treasury's Office of Privacy, Transparency, and Records conducted an assessment on the effect of use or sharing of cyber threat information and determined that GSOC's activities did not have a negative impact on the privacy and civil liberties of individuals. As CIG/OCCIP did not handle or collect PII, an assessment was not applicable.

Steps Taken to Address Adverse Effects on Privacy and Civil Liberties

The Statute requires OIGs to assess "the adequacy of steps taken by the Federal Government to reduce any adverse effect from activities carried out under [the Statute] on the privacy and civil liberties of United States persons."[52] Officials from the Departments of Commerce, Defense, Energy, Homeland Security, Justice, and the Treasury and ODNI told the auditors that to their knowledge, the activities carried out under the Statute did not have adverse effects on the privacy and civil liberties of United States 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 Statute requires OIGs to assess whether "inappropriate barriers to sharing information" among Federal entities exist.[53] Officials of the appropriate Federal entities described to the auditors barriers that they have experienced or observed, which they believe have hindered the sharing of cyber threat information. The barriers described include:

- Restrictive classifications limit cyber threat information from being widely shared (reported by IC SCC, four DoD components, and DOJ). For example, cyber threat information cannot be uploaded to a capability when the information is classified at a level higher than the capability accepts, and classified cyber threat information cannot be shared with non-cleared

[50] *Id*. § 1506(b)(2)(D)(iv).

[51] *Id*. § 1502(b)(1)(F) requires notification to any United States 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 a federal entity, when it determines that information received does not constitute a cyber threat indicator and contains personal information, to 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.

[52] 6 U.S.C. § 1506(b)(2)(D)(v).

[53] 6 U.S.C. § 1506(b)(2)(E).

officials or with cleared officials who do not have proper storage in security-approved facilities. Several entities have taken actions to mitigate this barrier, to include reaching out to the information owner to inquire about the possibility of downgrading the classification level or assigning field agents to each cleared contractor.

- Inability of machines to communicate with each other (machine-to-machine ingestion of data) reduces the speed at which cyber threat information sharing occurs. Examples include:

    - Lack of automated ingestion for some cyber threat information input to ICOAST, which increases the amount of manual input (reported by IC SCC). The IC SCC is working on machine-to-machine connections and integrated modules that are necessary to allow automated ingestion of data.

    - Lack of an accessible cross-domain sharing capability to transfer unclassified cyber threat indicators and defensive measures viewed on classified sources, such as Einstein E3A and portals hosted by DoD components, to unclassified capabilities for mitigating threats (reported by Commerce).

- Uncertainty about the protection from liability provided by the Statute adversely impacts the willingness of private sector entities to provide cyber threat information. The uncertainty relates to whether the protection from liability only covers cyber threat information shared by the private sector using the AIS capability. Section 105(d)(5)(D) appears to provide liability protection for any sharing of information under the Statute.[54] Specifically, the Section provides that cyber threat indicators and defensive measures shared with the Federal Government under the Statute should not be used by any Federal, State, tribal, or local government to regulate, including an enforcement action, the lawful activities of any non-Federal entity or any activities taken by a non-Federal entity pursuant to mandatory standards, including activities relating to monitoring, operating defensive measures, or sharing cyber threat indicators. However, Section 106(b)(2) appears to limit liability protection for sharing information only when using AIS.[55] Specifically, the Section provides that "no cause of action shall lie or be maintained in any court" against a private entity for sharing or receiving cyber threat information in accordance with the Statute and consistent with Section 105(c)(1)(B).[56] This Section directs DHS to develop and implement a capability and process for the Federal Government to receive cyber threat information under the Statute shared by a non-Federal entity. DHS developed AIS to comply with the requirement. Examples of liability uncertainties include:

    - Sections 105(d)(5)(D) and 106(b)(2) of the Statute appear contradictory. In addition, one of the guidance documents required to be developed by the Statute, *Guidance to Assist Non-Federal Entities to Share Cyber Threat Indicators and Defensive Measures*

[54] 6 U.S.C. § 1504(d)(5)(D).

[55] 6 U.S.C. § 1505(b)(2).

[56] 6 U.S.C. § 1504(c)(1)(B).

with Federal Entities under the Cybersecurity Information Sharing Act of 2015, provides that only the DHS capability and associated programs and other sharing permitted under Section 105(c)(1)(B) are covered under the liability protection provision. No other liability protection is listed in the document for any other sharing conducted under the Statute. Limiting the liability protections to only sharing through AIS and associated programs could impact industry informants from coming forward with relevant information (reported by DOE).

- Officials of some private entities are hesitant to share cyber threat information with others because officials believe sharing such information may raise legal and competitive issues including potential antitrust law issues (reported by DOJ).

- Challenges with AIS information deter its use. Examples include:

  - Too many technical indicators, such as suspect email addresses or IP (Internet Protocol) addresses, without the context necessary for users to understand the significance of the potential threat (reported by Commerce, DHS, IC SCC, Treasury).

  - Low quality cyber threat indicators require research to be performed by analysts to identify additional details and context to make the information useful, or result in cyber threat information being discarded (reported by Commerce and one DoD component).

  - Lack of context included with the cyber threat indicators to allow the information to be actionable (reported by DHS and Treasury).

  - Redundant cyber threat information distributed by AIS due to multiple entities uploading the same information and AIS not removing the identical cyber threat indicators. As a result, the same threat information is reviewed multiple times (reported by DOE).

  - Not providing the source of the information in AIS and not vetting the information, which causes users to be concerned as to whether the data can be trusted (reported by IC SCC).

  - Not extensively vetting AIS participants, which causes users to be concerned about sharing certain cyber threat indicators and defensive measures through AIS, particularly information that may contain some degree of sensitivity (reported by FBI).

To mitigate the barriers associated with AIS, DHS plans to upgrade AIS to share more enriched information and trend correlation.

Observation: The Consolidated Intelligence Guidance Includes Directives to Address and Improve Cyber Threat Intelligence Sharing

The *Consolidated Intelligence Guidance* provides direction from the DNI and the Under Secretary of Defense for Intelligence to the Intelligence Community to guide development of the Fiscal Year (FY) National Intelligence Program and the Military Intelligence Program. According to the *Consolidated Intelligence Guidance* for FY 2020-2024, the Intelligence Community "must resolve long-standing barriers to successful implementation of a shared, secured information environment in which all elements participate and proactively protect for the benefit of integrated intelligence mission operations." The *Consolidated Intelligence Guidance* for FY 2020-2024 and FY 2021-2025, issued in June 2018 and April 2019, respectively, included direction to the Intelligence Community elements to improve awareness and insight into cyber threats, deepen interoperability with partners, and defend the digital enterprise. More particularly, the *Consolidated Intelligence Guidance* for FY 2020-2024 and FY 2021-2025 specified a number of programmatic actions to assist Federal and non-Federal entities in their efforts to receive and share cyber threat intelligence.

APPENDIX A: OBJECTIVES, SCOPE, AND METHODOLOGY

The Offices of the Inspectors General (OIGs) for the Departments of Energy, Homeland Security, Justice, Defense, Commerce, Energy, and the Treasury, and the Office of the Director of National Intelligence assessed the implementation of the *Cybersecurity Information Sharing Act of 2015* (the Statute) for Calendar Year 2017 and Calendar Year 2018.[57] The objective of the assessment was to review the actions taken over the prior, most recent, two-year period to carry out the requirements of the Statute. As called for in the Statute, the OIGs assessed:

- 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, as well as an accounting of the security clearances authorized for the purpose of sharing cyber threat indicators or defensive measures with the private sector.
- The appropriateness, adequacy, and timeliness of the 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 capability—Automated Indicator Sharing—implemented by the Department of Homeland Security.
    - 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 Statute was used by a Federal entity to prosecute an offense listed in Section 105(d)(5)(A) of the Statute.[58]
    - 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.

[57] The OIGs of the Departments of Commerce, 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 Statute. *See* (1) *The Department Needs to Improve Its Capability to Effectively Share Cyber Threat Information* (OIG-19-026-A), (2) *The Department of Energy's Implementation of the Cybersecurity Information Sharing Act of 2015,* (3) *Review of DHS's Implementation of the Cybersecurity Information Sharing Act of 2015 for Calendar Years 2017 and 2018* (19-040-AUD-DHS); (4) *Audit of the Department of Treasury's Cybersecurity Information Sharing* (OIG-20-019), and (5) *Office of the Director of National Intelligence's Implementation of the Cybersecurity Information Sharing Act of 2015* (AUD-2019-003), respectively.

[58] *See supra* note 17.

  - The adequacy of steps taken by the Federal Government to reduce any adverse effect from activities carried out under the Statute on the privacy and civil liberties of United States persons.

- Barriers affecting the sharing of cyber threat indicators or defensive measures.

To accomplish the assessment objective, the auditors:

- Researched applicable laws, policies, regulations, and guidance regarding the sharing of cyber threat information and protecting PII.
- Interviewed entity, component, and private sector 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 Statute that contains PII, and tested a sample of cyber threat information received by the entities to determine whether it contained PII.
- Interviewed entity officials to determine the process used to retain or modify the classification of cyber threat information, and tested a sample of the shared cyber threat information to determine whether the process resulted in the proper classification.
- 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 cyber threat information to determine if it was:

  - Provided to individuals with the appropriate security clearances and need to know,

  - Free of PII, and

  - Used to mitigate potential threats.

- Interviewed entity, component, and private sector 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 to determine whether it was:

  - Shared as quickly as operationally practicable,

  - Relevant and useful information related to a cybersecurity threat and protected from unauthorized access, and

  - Provided to other Federal entities with the need for the information and with the proper clearances.

- 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.
- Interviewed entity, component, and private sector 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.

Throughout this report, NSA responses are limited to the information shared through AIS. NSA understands the assessment was intended to examine entities' implementation of the Statute and to assess their compliance with the Statute for such implementing activities. According to NSA officials, the only activity NSA carried out to help implement the Statute in CY 2017 and CY 2018 was sharing cyber threat indicators through AIS. Therefore, disseminating, sharing, and receiving of AIS information were the only activities NSA reported on in this assessment.

A separate, classified report—*Joint Report on the Implementation of the Cybersecurity Information Sharing Act of 2015* (AUD-2019-005)—has been provided to the appropriate Congressional Committees and Federal Entity Officials.

The Offices of the Inspectors General for the Departments of Justice, Defense, Commerce, and the Treasury, and the Office of the Director of National Intelligence conducted audits during the timeframe of December 2018 to November 2019 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 Offices of the Inspectors General for the Departments of Energy and Homeland Security conducted evaluations from March 2019 to November 2019 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: ACRONYMS LIST

AIS	Automated Indicator Sharing
CIG/OCCIP	Cyber Information Group/Office of Cybersecurity and Critical Infrastructure Protection
CISA	Cybersecurity and Infrastructure Security Agency
CISCP	Cyber Information Sharing and Collaboration Program
CRISP	Cybersecurity Risk Information Sharing Program
CS	Cybersecurity
CTIIC	Cyber Threat Intelligence Integration Center
CY	Calendar Year
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
DoD	Department of Defense
DOE	Department of Energy
DOJ	Department of Justice
ECS	Enhanced Cybersecurity Services
FBI	Federal Bureau of Investigation
FinCEN	Financial Crimes and Enforcement Network
FS-ISAC	Financial Services-Information Sharing and Analysis Center
GAO	Government Accountability Office
GSOC	Government Security Operations Center
HSIN	Homeland Security Information Network
IC SCC	Intelligence Community Security Coordination Center
ICOAST	Intelligence Community Analysis and Signature Tool
JSOC	Justice Security Operations Center
NCCIC	National Cybersecurity and Communications Integration Center

NCIJTF	National Cyber Investigative Joint Task Force
NGA	National Geospatial-Intelligence Agency
NISP	National Industrial Security Program
NRO	National Reconnaissance Office
NSA	National Security Agency
ODNI	Office of the Director of National Intelligence
OIA	Office of Intelligence and Analysis
OIG	Office of the Inspector General
PII	Personally Identifiable Information
SIGINT	Signal Intelligence
STIX	Structured Threat Information eXpression
TEWI	Treasury Early Warning Indicator
USCYBERCOM	United States Cyber Command


INSPECTOR GENERAL
INTELLIGENCE COMMUNITY
INDEPENDENCE • INTEGRITY • PROFESSIONALISM