Intelligence Community Office of the Inspector General

Interagency Joint Report on Compliance with the Cybersecurity Information Sharing Act of 2015

Audit Division
Report AUD-2025-001

December 2025

Intelligence Community Office of the Inspector General
Audit Division
Washington, DC

MEMORANDUM FOR: See Distribution

SUBJECT: Interagency Joint Report on Compliance with the Cybersecurity Information Sharing Act of 2015

The Office of the Inspector General of the Intelligence Community (IC OIG) provides this summary report for your awareness. The objective was to provide a joint report on actions taken during calendar years 2023 and 2024 to carry out the requirements of the Cybersecurity Information Sharing Act of 2015 (6 U.S.C. § 1501 et seq.) (the Act).

On 18 December 2015, Congress enacted the Act, requiring the Inspectors General of the "Appropriate Federal entities"—defined as the Departments of Commerce, Defense, Energy, Homeland Security, Justice, and the Treasury, and the Office of the Director of National Intelligence—to jointly report to Congress on the actions taken to fulfill the Act during the most recent two-year period. Each of the Offices of the Inspector General assessed their agency's compliance with the Act's requirements. The IC OIG compiled the results in this report.

The IC OIG provided a draft of this report to the Council of Inspectors General on Financial Oversight and incorporated their comments into this report.

We appreciate the courtesies extended to our staff throughout this review. Please direct any questions to ICIGPress@odni.gov.

NG RICHARD M WZFKND

Digitally signed by NG RICHARD M WZFKND
Date: 2025.12.10 16:29:01 -05'00'

Richard M. Ng

Date

Assistant Inspector General for Audit
Office of the Inspector General of the
Intelligence Community

KEVIN RYAN Digitally signed by KEVIN RYAN Date: 2025.12.11 14:54:51 -05'00'

Kevin D. Ryan

Director for Engineering, Cybersecurity, and Systems performing the duties of Assistant Inspector General for Audit and Evaluation
Department of Commerce, Office of the Inspector General

Date

MANSFIELD.BRETT.A.1229241709 Digitally signed by MANSFIELD.BRETT.A.1229241709 Date: 2025.12.11 14:25:09 -05'00'

Brett A. Mansfield

Deputy Inspector General for Audit
Department of Defense, Office of the Inspector General

Date

Craig Adelman

Craig Adelman

Deputy Inspector General for Audits
Department of Homeland Security, Office of the Inspector General

2025.12.15

Date

MATTHEW DOVE Digitally signed by MATTHEW DOVE Date: 2025.12.15 11:10:16 -05'00'

Matthew Dove

Assistant Inspector General for Audits
Department of Energy, Office of the Inspector General

Date

Jason Malmstrom

Assistant Inspector General for Audit
Department of Justice, Office of the
Inspector General

Date

Pauletta P. Battle Digitally signed by Pauletta P. Battle
Date: 2025.12.12 09:17:50 -05'00'

Pauletta P. Battle

Acting Assistant Inspector General for
Audit, Department of the Treasury,
Office of the Inspector General

Date

Distribution:

Director of National Intelligence
Secretary of Commerce
Secretary of War
Secretary of Energy
Secretary of Homeland Security
Attorney General, Department of Justice
Secretary of the Treasury
President of the Senate
Speaker of the House of Representatives

Table of Contents

Executive Summary

Interagency Joint Report on Compliance with the Cybersecurity Information Sharing Act of 2015 (AUD-2025-001)

Why We Did This Review

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

What We Found

The Offices of the Inspectors General (OIGs) determined that CTI and DM sharing improved over the past two years, and they were expanding accessibility to information.

---

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

[2] The Act incorporates the definition of "cybersecurity threat" in 6 U.S.C. § 650(8). It generally means an action, not protected by the First Amendment of the U.S. Constitution, on or through an information system that may result in an unauthorized effort to adversely impact the security, availability, confidentiality, or integrity of an information system.

[3] The Act incorporates the definition of "cyber threat indicator" in 6 U.S.C. § 650(5). It includes 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] The Act incorporates the definition of "defensive measures" in 6 U.S.C. § 650(9). It generally means an action, device, procedure, technique, or other measure applied to an information system that detects, prevents, or mitigates a known or suspected cybersecurity threat or vulnerability.

[5] "Federal entity" is defined by the Act as a department or agency of the United States or any component of such department or agency. See 6 U.S.C. § 1501(8). "Non-Federal entity" is defined by the Act to include state, local, and tribal governments; private sector companies; and academic institutions. See 6 U.S.C. § 1501(14).

[6] 6 U.S.C. § 1506(b)(1).

In calendar year (CY) 2023 and CY 2024, entities continued to share unclassified cyber threat information through the Automated Indicator Sharing (AIS) capability and top-secret cyber threat information through the Intelligence Community Analysis and Signature Tool (ICOAST), as well as various other reporting means, including email, written reports, websites, and face-to-face communications.

Concerning the specific areas that the Act required the OIGs to assess and report, the "appropriate Federal entities" continued to implement the Act. Specifically, the "appropriate Federal entities" responsible for sharing, receiving, or disseminating cyber threat information:

- Used sufficient policies and procedures.
- Properly classified CTIs and DMs when classified information was shared.
- Authorized security clearances for the purpose of sharing CTIs or DMs with the private sector as needed.
- Appropriately disseminated and used cyber threat information that Federal and non-Federal entities shared.
- Shared CTIs and DMs in a timely and adequate manner and with appropriate entities, with the exception of the Department of Commerce that only shared CTIs and DMs when required.
- Received CTIs and DMs in a timely and adequate manner.
- Used the Department of Homeland Security (DHS) capability, AIS, to receive CTIs or DMs, with the exception of Treasury and ODNI.
- Did not share 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 for failing to remove personal information of a specific individual not directly related to a cybersecurity threat.
- Did not need to take steps to minimize adverse effects on the privacy and civil liberties of U.S. persons from activities carried out under the Act because there were no known adverse effects.
- Identified barriers that hindered sharing CTIs and DMs.

What We Recommend

This report does not include any recommendations.

Background

Cybersecurity Information Sharing Act of 2015

On December 18, 2015, Congress enacted the Act[7], to improve cybersecurity in the United States through enhanced sharing of cyber threat information.[8] The Act created a framework to facilitate and promote voluntary CTI[9] and DM[10] sharing among Federal entities and between Federal and non-Federal entities.[11]

The Act also required DHS to establish a capability and process that allows Federal entities to receive cyber threat information from non-Federal entities. The Act designated the Attorney General and the Secretary of Homeland Security, in consultation with the heads of the appropriate Federal entities, to coordinate and develop publicly available policies, procedures, and guidance to assist Federal and non-Federal entities in their efforts to receive and share CTIs and DMs.

Other key provisions in the Act include liability protection for private entities that share cybersecurity information in accordance with established procedures, and protection of privacy and civil liberties. Specifically, Federal and non-Federal entities must remove personal information of a specific individual or information that identifies a specific individual that is not directly related to a cybersecurity threat. The Act sunsets on 30 January 2026 (except with respect to actions authorized and information obtained under the Act before such date).

Offices of the Inspector General Reporting Requirement

The Act required the Inspectors General of the appropriate Federal entities to provide a biennial joint report to Congress that includes:

- An assessment of the sufficiency of policies, procedures, and guidelines related to sharing CTIs within the Federal Government.
- An assessment of whether CTIs and DMs have been properly classified, and an accounting of the security clearances authorized for the purpose of sharing CTIs or DMs with the private sector.
- A review of the actions the Federal Government has taken based on CTIs or DMs shared with the Federal Government, including the appropriateness of subsequent

[7] See supra note 1.
[8] See supra note 2.
[9] See supra note 3.
[10] See supra note 4.
[11] See supra note 5.

uses and disseminations of CTIs and DMs and whether the CTIs or DMs were shared in a timely and adequate manner with appropriate entities or the public.

- An assessment of specific aspects of CTIs or DMs that have been shared with the Federal Government, including:
    - The number of CTIs or DMs shared using the capability implemented by DHS.
    - Instances in which any Federal or non-Federal entity shared information that was not directly related to a cybersecurity threat and contained personally identifiable information (PII).
    - The number of times, according to the Attorney General, that a Federal entity used information shared under this title to prosecute an offense listed in 6 U.S.C. § 1504(d)(5)(A).
    - The effect of sharing CTIs or DMs with the Federal Government on privacy and civil liberties of specific individuals, including the number of notices issued regarding a failure to remove information not directly related to a cybersecurity threat that contained PII.
    - The adequacy of steps the Federal Government has taken to reduce any adverse effect from activities carried out under the Act on the privacy and civil liberties of U.S. persons.
- An assessment of barriers affecting the sharing of CTIs or DMs.[12]

Responsible Components

The appropriate Federal entities' components responsible for sharing, receiving, or disseminating CTIs and DMs during CY 2023 and CY 2024 were:

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

Department of Defense (DoD).[13] Eight DoD components were responsible for sharing cyber threat information with Federal and non-Federal entities:

- The U.S. Cyber Command (USCYBERCOM) is a combatant command that directed, synchronized, and coordinated cyberspace planning and operations. Among other responsibilities, USCYBERCOM defended the DoD Information Network, provided

[12] 6 U.S.C. § 1506(b)(2).
[13] We recognize the rebranding of the Department of Defense (DoD) to Department of War (DoW), but continued the naming convention used during the reporting period of CYs 2023 and 2024.

support to combatant commanders for global mission execution, and strengthened the nation's ability to withstand and respond to cyberattacks.

- The National Security Agency/Central Security Service (NSA/CSS) is a combat support agency that led the U.S Government in cryptology that encompasses both signals intelligence (SIGINT) insight and cybersecurity products and services and enables computer network operations to gain a decisive advantage for the nation and U.S. allies. NSA Cybersecurity prevents and eradicates threats to U.S. national security systems with a focus on the Defense Industrial Base and the improvement of U.S. weapons' security. It also strives to promote cybersecurity education, research, and career-building.
- The Defense Information Systems Agency is a combat support agency that planned, engineered, tested, fielded, and operated information sharing capabilities for the joint service members, national-level leaders, and other mission and coalition partners across the DoD.
- The Defense Intelligence Agency (DIA) is a combat support agency that produced, analyzed, and disseminated military intelligence to service members, defense policymakers, and force planners in the DoD and Intelligence Community (IC) in support of U.S. military operations. DIA was also the DoD cybersecurity service provider for classified networks, in coordination with other DoD stakeholders.
- The National Reconnaissance Office (NRO) is responsible for developing, acquiring, launching, and maintaining intelligence satellites. NRO provided global communications, early warning of missile launches, and imagery to the DoD to support its operations.
- The National Geospatial-Intelligence Agency (NGA) is a combined intelligence and combat support agency that provided geographical data to the DoD and the IC.
- The Defense Counterintelligence and Security Agency (DCSA) provided security and counterintelligence support to the DoD through vetting, industry engagement, education, and other support. DCSA also performed background investigations for certain branches of the Federal Government.
- The DoD Cyber Crime Center (DC3) provided digital and multimedia forensics, specialized cyber training, and cyber analytics for the DoD. DC3 was the operational focal point for the Defense Industrial Base Cybersecurity Program and analyzed, produced, and distributed cyber products that contain actionable cyber threat information to the DoD, Federal Government, and the private sector.

Department of Energy (DOE). Two DOE components were responsible for sharing cyber threat information:

- The Integrated Joint Cyber Security Coordination Center was responsible for sharing CTIs and DMs within DOE and with other Federal entities.
- The Office of Cybersecurity, Energy Security, and Emergency Response was responsible for sharing CTIs and DMs with the private sector.

Department of Homeland Security (DHS). The Cybersecurity and Infrastructure Security Agency (CISA) led the national effort to protect critical infrastructure and advance cybersecurity by working with partners across all levels of government and in the private sector to promote information sharing. CISA managed the AIS capability, which enabled the real-time exchange of unclassified CTIs and DMs between government entities and private sector partners to identify and help mitigate threats.

Department of Justice (DOJ). Three DOJ components were responsible for sharing cyber threat information:

- The DOJ Chief Information Officer delegated responsibility for incident response to the Justice Security Operations Center (JSOC). The JSOC worked with DOJ components to prevent, detect, and respond to cyberattacks and espionage against the Department. The JSOC shared CTIs with other Federal entities and the private sector.
- The Federal Bureau of Investigation (FBI) Cyber Division gathered CTIs and other cyber threat information through its investigation and a variety of intelligence sources and shared them with partners through a variety of means.
- The FBI Enterprise Security Operations Center was responsible for proactively identifying, detecting, protecting, and responding to all cyber threats and attacks against FBI data and systems.

Office of the Director of National Intelligence (ODNI). ODNI and its service provider were responsible for information security services for systems and networks used by ODNI. The following ODNI components shared and received cyber threat information with other Federal entities:

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

- The Cyber Threat Intelligence Integration Center integrated and enabled IC cyber analysis, collection, and resources to protect critical infrastructure and support and inform national interests on current and future cyber threats.
- ODNI had a third group charged with managing all ODNI information assurance, cybersecurity engineering, interoperability, and integration activities. This group oversaw ODNI-wide efforts to safeguard the ODNI's complex environment of mission and business information technology.

Department of the Treasury (Treasury). Two Treasury components were responsible for sharing cyber threat information:

- The Treasury Shared Services Security Operations Center (TSSSOC) used an internal ticketing system to track CTIs and DMs, then scanned Treasury's network for matching events. If TSSSOC analysts determined that CTIs and DMs were a novel threat that originated in Treasury and was unknown to the public or Federal entities, a Treasury Early Warning Indicator was developed. Upon approval from TSSSOC leadership, TSSSOC shared cyber threats internally with Treasury bureaus and offices and externally with other Federal entities.
- The Office of Cybersecurity and Critical Infrastructure Protection (OCCIP) monitored and analyzed intelligence related to actionable cyber threats to the financial services sector received from intelligence sources, primarily from Treasury's Office of Intelligence and Analysis (OIA), as well as Treasury's Financial Crimes Enforcement Network and Federal law enforcement sources, and repackaged the cyber information at an unclassified level after verification by OIA, before sharing with Federal partners and the financial services sector.

Assessment Results

Information Sharing and Act Implementation in 2023 and 2024

Sharing Cyber Threat Information Among Federal Entities

In CYs 2023 and 2024, the appropriate Federal entities made progress enhancing accessibility to cyber threat information for improved information sharing with other Federal entities. Sharing CTIs and DMs increases the amount of information available for defending systems and networks against cyberattacks.

ODNI utilized multiple tools to meet the Act's requirements. In April 2017, the IC SCC deployed ICOAST to increase cybersecurity threat intelligence sharing at the top-secret security level, including indicators of compromise and malware signatures. Additionally, ODNI developed and introduced a program that provides commercial cyber threat intelligence to the 18 IC elements. The program improved the availability of commercial cyber threat intelligence across the IC and provided a pathway to reduce duplicative commercial cyber threat intelligence purchases, allowing those resources to be redirected to other needs.

CISA managed an automated system called the AIS capability, which provided a means for participating Federal agencies and non-Federal entities to share unclassified cyber threat information with each other.

Continuing Efforts to Share Cyber Threat Information

In addition to AIS, ICOAST, and the new ODNI program, the Federal entities continued to share cyber threat information through various other reporting means, including email, written reports, websites, and face-to-face communications. Specifically:

- Websites were used to share cybersecurity information. For example, ODNI's IC SCC maintained a website on a top-secret network containing various reports on cyber threats, vulnerabilities, and mitigation information. Available reports and products included: ICOAST Correlation Reports, situational awareness reports, weekly and monthly vulnerability reports, requests for information, and blogs. Officials with appropriate access could obtain and use this information.
- ODNI produced and disseminated a weekly Cyber Threat Intelligence Digest to Congress.
- For classified sharing, CISA used Enhanced Cybersecurity Services, an intrusion detection, prevention, and analysis capability and EINSTEIN 3 Accelerated, a system used to detect cyberattacks targeting Federal Civilian Executive Branch networks and actively prevent potential compromises. Both systems were decommissioned in December 2023. CISA replaced EINSTEIN 3 Accelerated with Protective Domain Name System During CY 2024, CISA did not share classified CTIs

and DMs because they decided to move to an unclassified service. CISA determined that using classified indicators proved to be more costly in technology and manpower than any assumed successes warranted.

- Treasury has supplemented the process of sharing CTIs from a variety of sources through its Automated Threat Information Feed (ATIF) program, launched on 9 May 2024. ATIF was intended to help financial institutions improve their network defense by aggregating data sources tailored to the needs of financial institutions in a single place to enable faster and more efficient detection of malicious activity targeting the sector.

Private Sector Sharing Using the Automated Indicator Sharing and Other Capabilities

DHS developed the AIS capability in 2016 to enable the real-time exchange of unclassified CTIs and DMs to participants of the AIS community. CISA offered the AIS capability at no cost to participants as part of CISA's mission to work with public and private sector partners to identify and help mitigate cyber threats through information sharing. The fundamental concept of the AIS capability is to promote interaction among participants. In CY 2024, CISA reported 18 Federal agencies and 3 DHS components directly connected to AIS to receive CTIs. Federal agencies also received AIS data indirectly from CISA's Shared Cybersecurity Services program.

CISA shared cyber threat information, including CTIs and DMs, with non-Federal entities through AIS as Cyber Information Sharing and Collaboration Program (CISCP) packages. CISA's implementation of the AIS capability allowed other Federal agencies to share their unclassified CTIs and DMs with non-Federal entities.

Other capabilities also allowed sharing of cyber threat information between Federal entities and the private sector, including:

- DOE:
    - Cybersecurity Risk Information Sharing Program and Analysis of Risks in the Energy Sector (ARES) reports. The Cybersecurity Risk Information Sharing Program used information sharing devices at the boundaries of networks to gather and share CTIs to both industry and private sectors. A report was generated and forwarded to the applicable industry and private sectors. ARES ingested cyber threat data from all sources internal and external to DOE and DOE published an ARES report distributed to internal and external partners.
    - Cybersecurity baselines created for small private sector utility companies via partnership with the National Association of Regulatory Utility Commissioners.

- DoD:
    - The UNDER ADVISEMENT program, USCYBERCOM's private sector partnership that facilitated information sharing between the Cyber National Mission Force and private sector partners.
    - The Defense Industrial Base–Network, an unclassified portal for private entities such as defense contractors.
    - Threat Vulnerability Reports, issued to impacted private entities in response to identified CTIs.
- DOJ:
    - Anomali ThreatStream, a commercial-off-the-shelf (COTS) automated tool that received and processed indicator information from the AIS capability. Anomali ThreatStream was used to create numerous detection rules to prevent and detect cybersecurity incidents. Public and private sector entities using the same platform had access to the indicator information.
    - FBI, through its cyber campaign coordination process and the National Cyber Investigative Joint Task Force, coordinated the sharing of CTIs and DMs relevant to the campaigns with the private sector. FBI case teams also shared CTIs and DMs with the private sector in connection with investigations.
    - FBI provided briefings regarding cyber threats and indicators to private sector partners and crafted private sector products (e.g., Private Industry Notifications and FBI Liaison Alert System reports, Public Service Announcements, Joint Cybersecurity Advisories, Joint Malware Analysis Reports, Cybersecurity Information Sheets, and published guides) that contained threat information to include indicators of compromise.
- Treasury:
    - Treasury shared Cyber Threat Intelligence and Indicator Notices,[14] Indicator Notices,[15] Circulars, and Spotlight Reports with the private sector via email.
    - Treasury also shared indicators via the ATIF, which included the threat indicators from the Circulars plus a variety of additional sources.

[14] Cyber Threat Intelligence and Indicator Notices are shared "as-is" by OCCIP in coordination with Treasury's Financial Crimes Enforcement Network and consist of relevant information on cybercriminal activity and indicators potentially associated with cyber-enabled financial origins derived from various sources, including U.S. Government research and private financial sector reporting.
[15] Indicator Notices are shared "as-is" by OCCIP and are intended to assist network defense efforts by informing cybersecurity practitioners of indicators associated with malicious cyber activity.

- ODNI:
    - ODNI disseminated information through their Critical Infrastructure Intelligence Initiative to increase collaboration with State, Local, Tribal, and Territorial government partners and private sector critical infrastructure providers for the protection of critical services underpinning national and economic security.

Results for Oversight of Government Activities

The Act required the OIGs of the Appropriate Federal Entities to assess specific areas concerning the implementation of the Act. These areas included the sufficiency of policies and procedures, proper classification of information and authorization of security clearances, actions taken by entities, specifics concerning the sharing of cyber threat information, barriers to sharing cyber threat information, and actions taken to mitigate barriers to sharing cyber threat information.

Sufficiency of Policies and Procedures

The Act required the OIGs to assess "the sufficiency of policies, procedures, and guidelines relating to the sharing of CTIs within the Federal Government, including those policies, procedures, and guidelines relating to the removal of information not directly related to a cybersecurity threat that is personal information of a specific individual or information that identifies a specific individual."[16]

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

Policies and procedures establish the processes and boundaries within which an organization should operate. The Act designated the Attorney General and the Secretary of Homeland Security, in consultation with the heads of the appropriate Federal entities, to coordinate and develop publicly available policies, procedures, and guidance to assist Federal and non-Federal entities in their efforts to receive and share CTIs and DMs consistent with the protection of classified information, intelligence sources and methods, and privacy and civil liberties.[17] In response to the Act, these entities developed and publicly issued the following documents:

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, primarily through the use of the AIS capability.

[16] 6 U.S.C. § 1506(b)(2)(A).
[17] *See* 6 U.S.C. § 1504.

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.
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 CTIs and DMs with Federal entities and describes the protections non-Federal entities receive under the Act.
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 CTIs and DMs. The procedures include details on existing government programs that facilitate sharing information on cybersecurity threats and the periodic publication of cybersecurity best practices.

Documents 1 and 2 addressed the Act's mandate that the Federal Government retain, use, and disseminate CTIs and DMs. Document 3 was specific to, and for use by, non-Federal entities. Document 4 was intended to facilitate and promote the sharing of cyber threat information among Federal and between Federal and non-Federal entities.

The OIGs of the designated Federal entities reviewed the specific policies, procedures, and guidelines used by their respective entities to determine whether they sufficiently adhered to the four documents created because of the Act. Commerce, DHS, and DOJ stated they used the CISA documents in conjunction with additional policies, procedures, and guidelines. DoD, DOE, ODNI, and Treasury stated that they do not use the CISA documents; however, they use other policies, procedures, and guidelines to meet the criteria laid out in the CISA documents. The OIG results for those entities are provided in Table 1.

Table 1: Assessment of Agency-Specific Documents Used to Govern Information Sharing Activities

Entity Name	Agency-Specific Policies, Procedures, and Guidelines Assessed as Sufficient	Comment
DoD	Yes	All DoD component policies and procedures aligned with sections 103(a) and (b) and 105(a), (b), and (d) of the Act, and were sufficient and compliant with those sections.

DOE	Yes	DOE determined there is no significant difference between its guidance and the four CISA documents. Therefore, there was no impact to the sharing of cyber threat information.
ODNI	Yes	ODNI did not use the four CISA documents. ODNI used other agency, IC, and government-wide guidance that was sufficient to meet the requirements of the Act.
Treasury	Yes	TSSSOC and OCCIP used sufficient agency-specific policies, procedures, and practices which were aligned with the guidance in the Act.

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

The Act required 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.[18] The guidelines on privacy and civil liberties were updated in April 2025.

Proper Classification of Information and Authorization of Security Clearances

The Act required "an assessment of whether CTIs or DMs have been properly classified and an accounting of the number of security clearances the Federal Government authorized for the purpose of sharing CTIs and DMs with the private sector."[19] Proper classification of information protects intelligence and allows for appropriate dissemination and use.

Proper Classification of Cyber Threat Indicators and Defensive Measures

ODNI properly classified and shared CTIs and DMs in CY 2023 and CY 2024. DHS properly classified and shared CTIs and DMs in CY 2023. However, in CY 2024, they did not share classified CTIs and DMs because they moved to an unclassified service. DHS and ODNI officials stated that they either retained the original classification of cybersecurity information or reclassified it using the appropriate guides before sharing.

[18] 6 U.S.C. § 1504(b)(2)(B).
[19] 6 U.S.C. § 1506(b)(2)(B).

DOE did not share classified CTIs and DMs during the time period evaluated, but they had previously shared classified CTIs and DMs and had a process whereby such information could be shared.

Commerce did not share CTIs or DMs with the private sector during CYs 2023 and 2024. DoD and Treasury did not share classified CTIs or DMs with the private sector during the same period.

DOJ determined that certain divisions did not share classified CTIs and DMs with the private sector; however, some did share classified CTIs and DMs relevant to campaigns or, depending on the situation, conduct classified briefings for cleared private sector partners. Although these divisions shared information, they did not originally classify CTIs and DMs.

Authorization of Security Clearances

DHS, DOE, DOJ, and ODNI authorized security clearances for the purpose of sharing cyber threat information with the private sector.[20]

- DHS authorized 256 security clearances in CY 2023 and 396 in CY 2024 to private sector partners participating in DHS's various information-sharing programs.
- DOE maintained active security clearances in CY 2023 and CY 2024.
- DOJ (FBI) authorized 12 security clearances in CY 2023 and 19[21] in CY 2024 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.
- ODNI did not share classified CTIs or DMs with the private sector. However, they had personnel with active security clearances who supported the work of facilitating engagement with private partners.

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

- Commerce did not share classified CTIs or DMs with the private sector.
- DoD did not authorize security clearances expressly for the purpose of sharing CTIs and DMs with the private sector.

[20] Entities that authorize security clearances conduct an investigation of persons proposed for access to classified information to determine whether they satisfy the criteria for obtaining and retaining access.
[21] Of the 19 clearances initiated, seven are under background investigation and have not yet been adjudicated.

- Treasury did not authorize security clearances for the purpose of sharing cyber threat information with the private sector.

Actions Taken by Entities

The Act required OIGs to conduct "a review of the actions taken by the Federal Government based on CTIs or DMs shared with the Federal Government," to include the appropriateness of dissemination and use of the cyber threat information, and "whether the CTIs or DMs were shared in a timely and adequate manner with appropriate entities, or, if appropriate, were made publicly available."[22]

Appropriate Dissemination and Use of Cyber Threat Information

The Federal entities appropriately disseminated and/or used CTIs or DMs shared by other Federal and non-Federal entities. Upon receipt of shared information, the Federal entities disseminated relevant information to entity officials. Cyber threat information is considered appropriately disseminated when the information is shared with individuals having the proper security clearance and 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 OIG results for each entity are summarized in Table 2.

Table 2: Entity Dissemination and Use of Cyber Threat Information

Entity Name	Information Disseminated and Used Assessed Appropriate	Dissemination and Use of Cyber Threat Information
Commerce	Yes	The ESOC shared information internally with the Department's bureaus through email distribution and ingested indicators of compromise into the ESOC Security Information and Event Management System.
DoD	Yes	Multiple DoD components used and disseminated CTIs and DMs shared by other Federal agencies.

[22] 6 U.S.C. § 1506(b)(2)(C).

DOE	Yes	DOE officials used and disseminated CTIs and DMs shared by other Federal agencies through Analyst1, which is configured to download threat information automatically and redistribute it across DOE via the site's automated access to Analyst1 or a COTS service used by the agency.
DHS	Yes	CISA used and disseminated CTIs and DMs on a case-by-case basis. CISA coordinated and cleared information received from Federal agencies for wider dissemination through information-sharing channels.
DOJ	Yes	DOJ disseminated shared cyber threat information to its components through automated sharing and monitoring tools. JSOC disseminated actionable threats to key stakeholders. Additionally, they leveraged CTIs received within their tools. The FBI shared threat intelligence through reports or published cybersecurity alerts, including those distributed via partner agencies like CISA.
ODNI	Yes	ODNI appropriately disseminated CTIs or DMs internally, which were shared by Federal and non-Federal entities, to relevant ODNI components. These components then used the information to address cyber threats.
Treasury	Yes	Treasury used and disseminated CTIs and DMs shared by other Federal agencies to the appropriate audience using the Traffic Light Protocol designations. Treasury used this process to mitigate potential threats by reviewing actionable indicators of compromise and importing them into its security information and event management tool to perform historical searches for evidence of indicator activity.

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

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

The Federal entities generally shared CTIs and DMs in a timely and adequate manner with appropriate Federal entities (except for Commerce, which shared CTIs and DMs only when required). Sharing cyber threat information is considered timely when available in real-time or as quickly as operationally possible. It is considered adequate when the shared information encompasses relevant and meaningful CTIs or DMs and when such information is safeguarded to prevent unauthorized access. Sharing cyber threat information with appropriate entities entails using a sharing capability that ensures delivery to the intended recipients 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 OIG results for each entity are summarized in Table 3.

Table 3: Entity Sharing Cyber Threat Information

Entity Name	Sharing Information Assessed as Timely, Adequate, and Appropriate	Sharing Cyber Threat Information
Commerce	N/A	Commerce generally did not share with other Federal agencies; however, it reported CTIs and DMs to CISA as part of incident reporting.
DoD	Yes	All DoD components shared CTIs and DMs with Federal agencies through automated tools to share near real-time threats with the appropriate entities.
DOE	Yes	DOE shared CTIs and DMs with other Federal agencies through the use of Analyst1's direct Application Programming Interface (API) connection to AIS. This sharing was performed in a timely and adequate manner, as Analyst1 is configured to automatically publish CTIs.
DHS	Yes	DHS shared CTIs and DMs with other Federal agencies using both automated and manual mechanisms.

DOJ	Yes	DOJ shared indicators derived from its internal response, threat hunting, and proactive defense operations with U.S. Government AIS partners (AIS Trusted Automated Exchange of Intelligence Information (TAXII)). Additionally, they collaborated and shared detection methodology and unique indicators associated with large-scale malicious email phishing campaigns and operations. DOJ sometimes made information publicly available to support joint-sequenced activities.
ODNI	Yes	ODNI shared CTIs and DMs with appropriate Federal entities in a timely and adequate manner. The time taken to share information varied by the amount of research required to provide context, as well as the urgency. Some ODNI components prepared summary reports containing cyber threat information that are only produced weekly, monthly, or yearly. These types of reports were not intended for real-time distribution.
Treasury	Yes	In accordance with its concept of operations document, TSSSOC shared Treasury Early Warning Indicators as soon as possible to appropriate entities. OCCIP shared Circulars, Cyber Threat Intelligence and Indicator Notices, and Spotlight Reports.

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

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

The Federal entities generally received CTIs and DMs in a timely and adequate manner, with the exception of Treasury, which could not determine timeliness and adequacy due to lack of information. The OIG results for each entity are summarized in Table 4.

Table 4: Entity Receiving Cyber Threat Information

Entity Name	Information Received Assessed as Timely and Adequate	Receiving Cyber Threat Information
Commerce	Yes	Commerce received cyber threat information in an adequate manner from other Federal entities through the AIS capability, conference calls, secure emails, and briefings.
DoD	Partial	All DoD components received CTIs and DMs in a timely and adequate manner; however, DIA reported that the accuracy of information received was inconsistent. For example, in May 2023 a Federal entity shared information that was inaccurate, which prevented DIA from acting on it.
DOE	Yes	Other Federal entities shared CTIs and DMs with DOE through Analyst1's direct API connection to AIS and CISCP feeds.
DHS	Yes	DHS received cyber threat information from other Federal entities, such as DoD, NSA and DOE, and shared the information with AIS subscribers.
DOJ	Yes	External Federal entities shared indicators directly with DOJ, as well as indirectly via FBI investigative or operational entities such as CyWatch, National Cyber Investigative Joint Task Force, and various FBI Cyber Division program elements and corresponding field office components.
ODNI	Yes	ODNI received cyber threat information in a timely manner, considering time needed for additional research to incorporate context.

Treasury	Partial	TSSSOC reported that information was received from CISA but several weeks or months after the adversaries were active. OCCIP reported they received adequate information in a timely manner.

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

Specifics Concerning the Sharing of Cyber Threat Information

The Act required the OIGs to conduct an assessment of the CTIs or DMs shared with the appropriate Federal entities, to include:

- The number of CTIs or DMs shared through the use of the AIS capability.
- The handling of information not directly related to a cybersecurity threat that is known at the time of sharing to contain PII.
- The number of times shared information was used to prosecute certain offenses.
- The impact on privacy and civil liberties.
- The steps taken to reduce adverse effects on privacy and civil liberties.[23]

Use of the Automated Indicator Sharing Capability

The Act required OIGs to determine the number of CTIs or DMs shared using DHS implemented AIS capability.[24] The following entities received CTIs and DMs using AIS:

- Commerce received CTIs and DMs from AIS, but Commerce did not track the information to quantify the number.
- Three DoD components, NSA, DC3, and NGA, received CTIs and DMs from AIS.
- DOE received 180,790 CTIs and DMs in CY 2023 and 274,972 in CY 2024.
- DHS received 1,052,596 CTIs and DMs in CY 2023 and 10,281,582 CTIs and DMs in CY 2024. DHS subsequently shared the indicators with other Federal entities.
- DOJ received 184,310 CTIs and DMs in CY 2023 and 123,172 CTIs in CY 2024.
- ODNI did not obtain CTIs or DMs directly from AIS. ODNI's IC SCC stated that they received indicators manually from AIS. IC SCC ingested more than 2,300 indicators of compromise in CY 2023 and almost 6,000 indicators of compromise in CY 2024.

[23] 6 U.S.C. § 1506(b)(2)(D).
[24] 6 U.S.C. § 1506(b)(2)(D)(i).

- Treasury's TSSSOC opted not to use AIS to receive CTIs and DMs from DHS. Instead, they used AlienVault, an aggregator, to receive CTIs from DHS for CYs 2023 and 2024. OCCIP did not have access to AIS during CYs 2023 and 2024. However, OCCIP's ATIF aggregates CTIs from various open sources including AlienVault.

Handling Information Containing Personally Identifiable Information

The Act required OIGs to assess "any information not directly related to a cybersecurity threat that is personal information of a specific individual or information identifying a specific individual and was shared by a non-Federal Government entity with the Federal Government in contravention" of the Act or the guidelines.[25] Officials at Commerce, DoD, DOE, DHS, DOJ, the Treasury, and ODNI stated they have not shared information that is unrelated to a cybersecurity threat that included PII.

Use of Shared Information to Prosecute an Offense

The Act required the joint report to address the number of times, according to the Attorney General, that a Federal entity used information shared under the Act to prosecute an offense listed in 6 U.S.C. § 1504(d)(5)(A).[26] DOJ officials stated that DOJ is not tracking this metric. DOJ officials told the auditors that crediting a case solely on information shared under the Act is not measurable because information gathered to prosecute an offense may come from multiple sources, including the Act. Senior prosecutors who review computer intrusion prosecutions generally told the auditors that they cannot recall any instances in which information shared under the Statute was used as evidence in a criminal prosecution.

Effects of Sharing on Privacy and Civil Liberties

The Act required OIGs to assess the effect of sharing CTIs or DMs with the Federal Government on privacy and civil liberties of specific individuals, including the number of notices that were issued with respect to a failure to remove information not directly related to a cyber security threat that was personal information of a specific individual or information that identified a specific individual.[27]

Officials at Commerce, DoD, DOE, DHS, DOJ, Treasury, and ODNI stated that they did not receive notices for failing to remove PII not directly related to a cybersecurity threat.[28]

---

[25] 6 U.S.C. § 1506(b)(2)(D)(ii).
[26] 6 U.S.C. § 1506(b)(2)(D)(iii).
[27] 6 U.S.C. § 1506(b)(2)(D)(iv).
[28] 6 U.S.C. § 1502(b)(1)(F) requires notification to any U.S. person whose personal information is known or determined to have been shared by a Federal entity in violation of the Act. Under 6 U.S.C. § 1502(b)(1)(E)(ii), a Federal entity, when it determines that information received does not constitute a CTI and contains personal

Steps Taken to Address Adverse Effects on Privacy and Civil Liberties

The Act required OIGs to assess "the adequacy of steps taken by the Federal Government to reduce any adverse effect from activities carried out under [the Act] on the privacy and civil liberties of United States persons."[29] Officials at Commerce, DoD, DOE, DHS, DOJ, Treasury, and ODNI stated that the activities carried out under the Act did not have adverse effects on the privacy and civil liberties of U.S. persons; therefore, steps to minimize adverse effects were not necessary.

Barriers to Sharing Cyber Threat Information

The Act required OIGs to assess whether "inappropriate barriers to sharing information" among Federal entities exist.[30] All OIGs described barrier-specific effects on sharing CTIs and DMs, to include:

- Reluctance to Share
    - Federal entities continued to be reluctant to share information into the public collection. Some prefer sharing exclusively within the Federal collection. Others may have policy requirements to share only within their relevant sector among eligible stakeholders. (DHS)
    - Perception among some private sector companies and industries that cooperation with law enforcement may lead to negative business and regulatory consequences. (DOJ)
    - Information-sharing fatigue from industry partners due to the large number of CTIs and DMs received, and a lack of maturity in information characterization. (DOE)
    - Belief of some private sector companies that sharing cyber threat information may jeopardize ongoing operations and raise legal and competitive issues, including implicating potential antitrust issues. (DOJ)
- Classification Concerns
    - Cross-domain sharing was not viable. CTIs and DMs obtained from classified sources could not be ingested and utilized to mitigate risks on unclassified systems because agencies lacked a capability to transfer them to unclassified environments. (Commerce and DOJ)

---

information, must remove such information. According to the *Privacy and Civil Liberties Final Guidelines: Cybersecurity Information Sharing Act of 2015,* the disseminating entity is to notify all the entities who have received the information determined to be in error as soon as practicable, and the guidelines provide details on information to be contained in a notice.

[29] 6 U.S.C. § 1506(b)(2)(D)(v).

[30] 6 U.S.C. § 1506(b)(2)(E).

  - Cyber threat information that came from other agencies was typically classified. This greatly reduced the actionability and operational value and when they were declassified, they were often shared without any accompanying context. (Treasury)

- Technical Challenges
  - Integration of greater volumes of cyber threat information requires better analytical tools, more training, and analysts to detect and deter anomalous activities. (ODNI and DOJ)
  - Capability to use big data platform tools to share CTIs and DMs was challenging because the DoD had multiple big data platforms, and in some instances, data could not easily be transferred between all of them. (DoD)
  - There continued to be inconsistent vendor support for the latest cyber threat information language and sharing protocol specifications which hindered Federal entities from deploying shared CTIs and DMs from others in the community into their vendor tools. (DHS)
  - From an AIS update in 2023 into 2024, a firewall blocked sensitive data and delayed information sharing. (DoD)
- Quality Challenges
  - Many sharing partners continued to operate under the assumptions of an outdated threat landscape and provided inaccurate and/or unspecific reporting that could overwhelm processing resources. (Treasury)
  - Quality concerns remained because many of the CTIs and DMs received through AIS lacked context or sufficient information to understand if they were still relevant. (Commerce)
  - The quality of information received varies from each provider, which can present issues when ingesting large datasets. As the data ingestion increases, the labor required to organize the data to be used effectively increases. (DOJ)
  - Issues were reported with receiving inadequate cybersecurity threat information from other Federal agencies that limited their ability to act on information in a timely manner. Sometimes it took weeks to provide sufficient information and occasionally a DoD component was denied access to the information when it did not contain additional limited distribution labels preventing sharing. (DoD)

Actions Taken to Mitigate Barriers to Sharing Cyber Threat Information

Actions planned or taken to mitigate barriers included:

- Commerce used third-party software to enhance AIS indicator quality with additional context.
- CISA continued to work with the cybersecurity vendor community to increase adoption of the latest specifications and the number of sharing tools that are interoperable with DHS' capabilities. They also continued to engage with Federal and non-Federal entities to encourage sharing and document feedback to introduce future features and capabilities. In its latest TAXII 2.1 capability, CISA responded to previously identified quality concerns by introducing a CISA opinion score applied to all shared CTIs and DMs to enable participants to filter indicators by opinion score and make their own decisions about which CTIs and DMs to deploy for detection and mitigation measures in their environments. The intent of this feature is to reduce the risk of false positives and allow participants to triage which alerts to prioritize among the growing volume of alerts within operations teams.
- DoD transferred U//FOUO CTIs and DMs manually to the affected Federal entities during the time period of May 2023 to January 2024.
- Treasury's TSSSOC worked closely with Treasury's Office of Counterintelligence to determine actionability and operational utility of the information and to assist with requests to declassify reporting. Regarding the quality issues, TSSSOC included as much context regarding the incident as possible when sharing indicators and to include the provenance [place of origin] and/or original source reporting whenever possible. TSSSOC only ingested indicators from sources that have a proven track record of combining higher quality indicators and the best coverage.
- The ODNI IC SCC improved its CTI sharing architecture to enable improved data tagging, data analytics, and the integration of new technologies, including artificial intelligence and machine learning.
- FBI Cyber Division regularly identified cybersecurity best practices and coordinated across the interagency on language to publish in Joint Cybersecurity Advisories, Private Industry Notifications, FBI Liaison Alert Systems, and other advisories, including the Secure-by-Design series of products and Hardening Guidance. Many of these best-practice recommendations were based on intelligence gathered from Cyber Action Team deployments to cyberattack victims across the nation. The best practices included, in several instances, zero-day vulnerabilities.

Appendix A: Objectives, Scope, and Methodology

The Offices of Inspector General (OIGs) for the Departments of Energy, Homeland Security, Justice, Defense, Commerce, the Treasury, and the Office of the Director of National Intelligence assessed the implementation of the Cybersecurity Information Sharing Act of 2015 (6 U.S.C. § 1501 et seq.) (the Act) for calendar years 2023 and 2024. The objective of the assessment was to review actions taken over the prior, most recent, two-year period to carry out the requirements of the Act. As called for in the Act, the OIGs assessed the following:[31]

- The sufficiency of policies and procedures related to sharing cyber threat indicators (CTIs) within the Federal Government.
- Whether CTIs and defensive measures (DMs) had been properly classified, and performed an accounting of the security clearances authorized for the purpose of sharing CTIs or defensive measures with the private sector.
- Actions taken to use and disseminate CTIs or DMs shared with the Federal Government.
- Specific aspects of CTIs or DMs that had been shared with the Federal Government, including:
    - The number of CTIs or DMs shared using the Automated Indicator Sharing (AIS) capability implemented by Department of Homeland Security (DHS).
    - Instances in which any Federal or non-Federal entity shared information that was not directly related to a cybersecurity threat and that contained personally identifiable information (PII).
    - The number of times, according to the Attorney General, that information shared under this title was used by a Federal entity to prosecute an offense listed in 6 U.S.C. § 1504(d)(5)(A).
    - The effect of sharing CTIs or DMs with the Federal Government on privacy and civil liberties of specific individuals, including the number of notices that were issued with respect to a failure to remove information not directly related to a cybersecurity threat that contained PII.

[31] 6 U.S.C. § 1506(b)(2).

    - The adequacy of steps taken by the Federal Government to reduce any adverse effect from activities carried out under this title on the privacy and civil liberties of U.S. persons.
- Barriers affecting the sharing of CTIs or DMs.

To accomplish the assessment objective, the OIGs:

- Researched applicable laws, policies, regulations, and guidance regarding the sharing of cyber threat information.
- Interviewed entity and component officials to discuss their processes for sharing and receiving CTIs and DMs, to include sharing or receiving information using various capabilities such as the DHS's AIS capability.
- Reviewed the sufficiency of the policies and procedures used by the entities for protecting and/or removing information shared under the Act that contains PII and tested examples of cyber threat information received by the entities to determine whether it contained PII, as needed.
- Interviewed entity officials to determine the process used to retain or modify the classification of cyber threat information, if applicable, and tested examples of the shared cyber threat information to determine whether the process resulted in the proper classification, as needed.
- Interviewed entity officials to determine whether they authorized security clearances for sharing cyber threat information with the private sector.
- Interviewed entity officials to determine whether they disseminated cyber threat information within the entity; and performed testing on examples of disseminated and used cyber threat information, as needed.
- Interviewed entity and component officials to determine whether cyber threat information was shared with or received from other Federal entities; and tested examples of cyber threat information shared with and received from other Federal entities, as needed.
- Interviewed entity officials and tested examples of cyber threat information shared with other Federal entities to determine whether the privacy and civil liberties of any individuals were impacted due to the entity sharing cyber threat information, as needed.
- Interviewed entity and component officials to identify barriers that adversely impacted the sharing of cyber threat information.
- Briefed the Council of Inspectors General on Financial Oversight on the progress and status of the project and provided it the draft report for review and comment.

The OIGs for DoD and Treasury conducted audits in accordance with generally accepted government auditing standards (GAGAS). Those standards required 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 OIG for DoD conducted fieldwork from January 2025 through July 2025, while the OIG for Treasury conducted fieldwork from December 2024 through August 2025.

The OIG for the DOJ conducted its review from January 2025 through July 2025 in accordance with the principles of GAGAS, which provided a reasonable basis for its findings and conclusions.

The OIGs for the Departments of Commerce, Energy, Homeland Security, and the Office of the Director of National Intelligence conducted their assessments in accordance with the Council of the Inspectors General on Integrity and Efficiency's Quality Standards for Inspection and Evaluation (May 2023), from January 2025 to July 2025. The auditors believe the evidence obtained provides a reasonable basis for the findings and conclusions based on the assessment objectives.

Appendix B: Abbreviations and Acronyms

AIS	Automated Indicator Sharing
ARES	Analysis of Risks in the Energy Sector
ATIF	Automated Threat Information Feed
CISA	Cybersecurity and Infrastructure Security Agency
Commerce	Department of Commerce
COTS	Commercial-Off-the-Shelf
CTI	Cyber Threat Indicator
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
DM	Defensive Measure
DoD	Department of Defense
DOE	Department of Energy
DOJ	Department of Justice
ESOC	Enterprise Security Operations Center
FBI	Federal Bureau of Investigation
GAGAS	Generally Accepted Government Auditing Standards
IC	Intelligence Community
ICOAST	Intelligence Community Analysis and Signature Tool
IC OIG	Intelligence Community Office of the Inspector General
IC SCC	Intelligence Community Security Coordination Center
JSOC	Justice Security Operations Center
NGA	National Geospatial Agency
NSA	National Security Agency
OCCIP	Office of Cybersecurity and Critical Infrastructure Protection
ODNI	Office of the Director of National Intelligence

OIA	Office of Intelligence and Analysis
OIG	Office of the Inspector General
PII	Personally Identifiable Information
TAXII	Trusted Automated Exchange of Intelligence Information
The Act	Cybersecurity Information Sharing Act of 2015
TSSSOC	Treasury Shared Services Security Operations Center
USCYBERCOM	United States Cyber Command