



U.S. DEPARTMENT OF HOMELAND SECURITY **OFFICE OF INSPECTOR GENERAL**

OIG-24-60

September 25, 2024

FINAL REPORT

CISA Faces Challenges Sharing Cyber Threat Information as Required by the Cybersecurity Act of 2015





OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

Washington, DC 20528 | www.oig.dhs.gov

September 25, 2024

MEMORANDUM FOR: Jen Easterly
Director
Cybersecurity and Infrastructure Security Agency

FROM: Joseph V. Cuffari, Ph.D. GLENN E SKLAR Digitally signed by
Inspector General SKLAR GLENN E SKLAR
Date: 2024.09.25 11:47:58
-04'00' for

SUBJECT: *CISA Faces Challenges Sharing Cyber Threat Information
as Required by the Cybersecurity Act of 2015*

Attached for your action is our final report, *CISA Faces Challenges Sharing Cyber Threat Information as Required by the Cybersecurity Act of 2015*. We incorporated the formal comments provided by your office.

The report contains two recommendations aimed at improving information sharing under the *Cybersecurity Act of 2015*. Your office concurred with both recommendations. Based on information provided in your response to the draft report, we consider recommendation 1 open and unresolved. As prescribed by Department of Homeland Security Directive 077-01, *Follow-Up and Resolutions for the Office of Inspector General Report Recommendations*, within 90 days of the date of this memorandum, please provide our office with a written response that includes your (1) agreement or disagreement, (2) corrective action plan, and (3) target completion date for the recommendation. Also, please include responsible parties and any other supporting documentation necessary to inform us about the current status of the recommendation. Until your response is received and evaluated, the recommendation will be considered open and unresolved.

We consider recommendation 2 open and resolved. Once your office has fully implemented the recommendations, please submit a formal closeout letter to us within 30 days so that we may close the recommendations. The memorandum should be accompanied by evidence of completion of agreed-upon corrective actions and of the disposition of any monetary amounts.

Please send your response or closure request to OIGAuditsFollowup@oig.dhs.gov.

Consistent with our responsibility under the *Inspector General Act*, we will provide copies of our report to congressional committees with oversight and appropriation responsibility over

the Department of Homeland Security. We will post the report on our website for public dissemination.

Please contact me with any questions, or your staff may contact Kristen Bernard, Deputy Inspector General for Audits, at (202) 981-6000.

Attachment



DHS OIG HIGHLIGHTS

CISA Faces Challenges Sharing Cyber Threat Information as Required by the Cybersecurity Act of 2015

September 25, 2024

Why We Did This Review

The *Cybersecurity Act of 2015* requires the Department of Homeland Security to establish a capability and process for Federal entities to receive cyber threat information from non-Federal entities. Section 107 of the Act requires Inspectors General from the Intelligence Community and appropriate agencies to submit a joint report to Congress every 2 years on Federal Government actions to share cyber threat information. We conducted this review to evaluate DHS' progress in meeting the Act's cybersecurity information-sharing requirements for CYs 2021 and 2022.

What We Recommend

We made two recommendations for CISA to establish an outreach plan and collaborate with its Chief Information Officer and Chief Financial Officer to document expenditure costs for AIS.

For Further Information:

Contact our Office of Public Affairs at (202) 981-6000, or email us at: DHS-OIG.OfficePublicAffairs@oig.dhs.gov.

What We Found

The Cybersecurity and Infrastructure Security Agency (CISA) addressed the basic information-sharing requirements of the *Cybersecurity Act of 2015*. In calendar years 2021 and 2022, CISA updated its guidance, properly classified cyber threat indicators (CTI) and defensive measures, and accurately accounted for security clearances to address the basic information-sharing requirements of the Act. In March 2022, CISA completed upgrades to its Automated Indicator Sharing (AIS) 2.0 capability to address information-sharing limitations.

Despite these improvements, the number of participants using AIS to share cyber threat information has declined to its lowest level since 2017. The overall number of AIS participants fell from 304 in CY 2020 to 135 in CY 2022. Among other factors, overall participation in AIS declined because CISA did not have an outreach strategy to recruit and retain data producers. Concurrently, sharing of CTIs through AIS declined by 93 percent from CY 2020 to CY 2022. This decline occurred because a key Federal agency stopped sharing CTIs due to unspecified security concerns with transferring information from its current system to AIS.

Further, CISA could not identify specific AIS program costs for the amount spent on upgrades and operations because it did not maintain expenditure data to readily allow auditing of AIS-related costs. Insufficient participation in AIS, along with the reduction in CTIs, has impeded CISA's ability to facilitate the sharing of cyber threats in real time. As a result, AIS stakeholders may be unable to identify and mitigate new cyber threats, potentially putting the Nation's critical infrastructure at risk. Additionally, CISA's inability to determine AIS costs limited our ability to identify whether taxpayer funds could have been put to better use.

CISA Response

CISA concurred with both recommendations. Appendix B contains CISA's management comments in their entirety.



OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

Table of Contents

Background	1
Cybersecurity Act Reporting Requirements in Relation to Previous DHS OIG Reports	3
Results of Review	4
CISA Addressed Basic Information-Sharing Requirements of the Act and Completed AIS Upgrades	5
Despite CISA’s Upgrades, Overall Participation and Information Sharing Declined	7
CISA Cannot Identify Funding Expenditures for the AIS Capability	10
Conclusion	10
Recommendations.....	11
Management Comments and OIG Analysis.....	11
Appendix A: Objective, Scope, and Methodology.....	13
DHS OIG’s Access to DHS Information.....	14
Appendix B: CISA Comments on the Draft Report	15
Appendix C: DHS’ Responses to the Office of the Inspector General of the Intelligence Community Questionnaire.....	17
Policies, Procedures, and Guidelines	17
Sharing CTIs and DMs with Private Sector	19
Accounting of Security Clearances.....	20
Using and Disseminating CTIs and DMs Shared by Other Federal Agencies	20
Sharing CTIs and DMs with Other Federal Agencies.....	21
DHS’ Sharing Capability and Processes (To be answered by DHS only)	22
CTIs and DMs Received from Other Federal Agencies	23
Personal Information Violations	23
Potential Barriers	24
Appendix D: Office of Audits Major Contributors to This Report.....	28
Appendix E: Report Distribution	29



OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

Abbreviations

AIS	Automated Indicator Sharing
CISA	Cybersecurity and Infrastructure Security Agency
CISCP	Cyber Information Sharing and Collaboration Program
CSD	Cybersecurity Division
CTI	cyber threat indicator
DM	defensive measure
NCPS	National Cybersecurity Protection System
PII	personally identifiable information
STIX	Structured Threat Information eXpression
TAXII	Trusted Automated eXchange of Indicator Information



OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

Background

The Department of Homeland Security has a critical mission to protect the Nation's cyberspace, including DHS' own computer systems and information, and those of other Federal agencies. As part of this mission, DHS coordinates and integrates information among Federal cyber operations centers, state and local governments, and the private sector. Within DHS, the Cybersecurity and Infrastructure Security Agency (CISA) protects the Nation's critical infrastructure from physical and cyber threats.

The *Cybersecurity Act of 2015* (Cybersecurity Act or Act)¹ established a voluntary process for public and private-sector entities to share cyber threat information with each other. The Act requires the Director of National Intelligence, the Secretaries of Homeland Security and Defense, and the Attorney General, in consultation with the heads of other appropriate Federal entities, to jointly develop and issue procedures to facilitate and promote sharing of classified and unclassified cyber threat indicators (CTIs), defensive measures (DMs), and best practices related to mitigating cyber threats between the Federal Government and private sector. The Act defines CTIs² as information that describes or identifies malicious reconnaissance, including anomalous patterns of communications, to gather technical information related to a cybersecurity threat or security vulnerability. Additionally, the Act defines DMs as an action, device, procedure, signature, 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 security vulnerability.

In 2016, CISA created the Automated Indicator Sharing (AIS) capability to enable real-time exchange of machine-readable CTIs and DMs to help protect the networks and systems of AIS community participants³ and reduce the prevalence of cyberattacks. The AIS capability is available at no cost, and it allows participants to voluntarily share and receive unclassified cyber threat information, such as commercially available threat information and partner-submitted data from various sources or information producers. White House Memorandum 005632,⁴ issued to Federal agencies on January 15, 2016, stipulated that to ensure the rapid expansion of this capability, all recipient departments and agencies should actively participate in AIS and allocate

¹ *Cybersecurity Act of 2015*, December 18, 2015.

² *Cybersecurity Act of 2015*, December 18, 2015, Section 102(6).

³ The AIS community comprises Federal and non-Federal entities; the latter include private-sector entities and state, local, tribal, and territorial governments. *Sharing of Cyber Threat Indicators and Defensive Measures by the Federal Government under the Cybersecurity Information Sharing Act of 2015*, February 16, 2016, Section 1 Purpose.

⁴ *Participation in Automated Cyber Indicator Sharing with the Department of Homeland Security Memorandum*, The White House, January 15, 2016.



OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

the necessary resources to make the capability effective. According to CISA, as more information is shared, participants become better informed and prepared to prevent cyber incidents.⁵

AIS is composed of three different CTI collections. AIS uses the Structured Threat Information eXpression (STIX)⁶ format and the Trusted Automated eXchange of Indicator Information (TAXII)⁷ server model, which allows participants to share and receive CTIs to these three collections. For example:

1. The Federal collection is available to all departments and agencies that sign the Multilateral Information Sharing Agreement, and it is the largest of the three.
2. The Public collection is available to all participants. All non-Federal users must sign the AIS Terms of Use.
3. The Cyber Information Sharing and Collaboration Program (CISCP) collection is available to non-Federal entities who sign the Cyber Information Sharing and Collaboration Agreement.

Figure 1 depicts how participants submit indicators to add to the three collections.

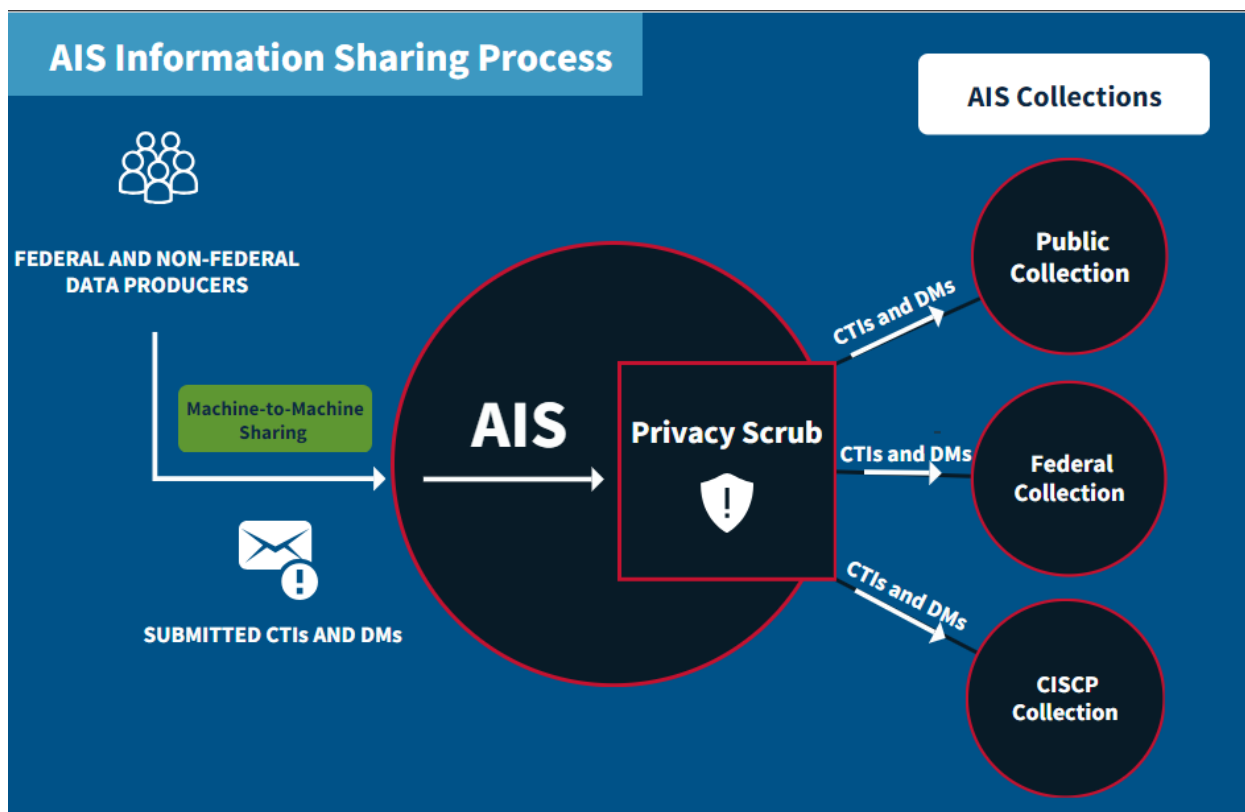
⁵ *Artificial Intelligence: Fully Implementing Key Practices Could Help DHS Ensure Responsible Use for Cybersecurity*, GAO-24-106246, February 2024.

⁶ STIX is a computing language that enables organizations to share structured cyber threat information.

⁷ TAXII is a standard for exchanging structured cyber threat information in a trusted manner for the detection, prevention, and mitigation of cyber threats. *Final Procedures Related to the Receipt of Cyber Threat Indicators and Defensive Measures by the Federal Government*, June 15, 2016, Appendix A, Glossary.



Figure 1. AIS Distribution Process to Public, Federal, and CISC Collections



Source: Generated by DHS Office of Inspector General based on CISA documentation on AIS indicator-sharing process

Cybersecurity Act Reporting Requirements in Relation to Previous DHS OIG Reports

Title I, Section 107(b) of the Act requires the Inspectors General from the Intelligence Community and the Departments of Commerce, Defense, Energy, Homeland Security, Justice, and Treasury to submit a biennial joint report⁸ to appropriate congressional oversight committees. This report includes an overall assessment⁹ of:

- the policies, procedures, and guidelines for sharing CTIs within the Federal Government, as well as for removing personal information that is not directly related to CTIs;

⁸ *Joint Report on the Implementation of the Cybersecurity Information Sharing Act of 2015*, OIG of the Intelligence Community, AUD-2023-002, December 12, 2023.

⁹ *Section 107 (b) Joint Project Steps*, April 26, 2023.



OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

- whether CTIs and DMs have been properly classified and an accounting exists for the number of security clearances authorized by the Federal Government under the Act;
- actions taken by Federal agencies based on CTIs or DMs shared within the Federal Government; and
- any inappropriate barriers to sharing CTIs or DMs among Federal agencies.

According to the Office of the Inspector General of the Intelligence Community's *Section 107 (b) Joint Project Steps*, the OIG for each responsible agency is required to submit responses to 30 questions on the actions the agency has taken to implement the Act. See Appendix C for DHS' responses to these questions.

DHS OIG has published three prior reports¹⁰ over the past 7 years assessing AIS functionality. In calendar years 2020 and 2022,¹¹ we disclosed that limited contextual information shared with AIS participants was not adequate for identifying and addressing cyber threats. We concluded that these deficiencies stemmed from limitations in AIS functionality, staffing inadequacies, and external factors. In 2017,¹² we reported on insufficient contextual information for CTIs and DMs, inadequate automated analytical tools, limited outreach efforts, and security-control deficiencies. At the time of this review, all recommendations from these three reports were closed.

We conducted this review to evaluate DHS's progress¹³ in meeting the Act's cybersecurity information-sharing requirements for CYs 2021 and 2022.

Results of Review

CISA addressed the basic information-sharing requirements of the *Cybersecurity Act of 2015*. In CYs 2021 and 2022, CISA updated its guidance, properly classified CTIs and DMs, and accurately accounted for security clearances to address the basic information-sharing requirements of the Act. In March 2022, CISA completed upgrades to its AIS 2.0 capability to address information-sharing limitations.

Despite these improvements, the number of participants using AIS to share cyber threat information has declined to its lowest level since 2017. The overall number of AIS participants

¹⁰ *Additional Progress Needed to Improve Information Sharing under the Cybersecurity Act of 2015*, OIG-22-59, August 16, 2022; *DHS Made Limited Progress to Improve Information Sharing under the Cybersecurity Act in Calendar Years 2017 and 2018*, OIG-20-74, September 25, 2020; and *Biennial Report on DHS' Implementation of the Cybersecurity Act of 2015*, OIG-18-10, November 1, 2017.

¹¹ See OIG-22-59 and OIG-20-74.

¹² See OIG-18-10.

¹³ DHS progress is evaluated by CISA's progress in implementing the cybersecurity information-sharing requirements within the Act.



OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

fell from 304 in CY 2020 to 135 in CY 2022. Among other factors, overall participation in AIS declined because CISA did not have an outreach strategy to recruit and retain data producers. Concurrently, sharing of CTIs through AIS declined by 93 percent from CY 2020 to CY 2022. This decline occurred because a key Federal agency stopped sharing CTIs due to unspecified security concerns with transferring information from its current system to AIS.

CISA could not identify specific AIS program costs for the amount spent on upgrades and operations because it did not maintain expenditure data to readily allow auditing of AIS-related costs. Insufficient participation in AIS, along with the reduction in CTIs, has impeded CISA's ability to facilitate the sharing of cyber threats in real time. As a result, AIS stakeholders may be unable to identify and mitigate new cyber threats, potentially putting the Nation's critical infrastructure at risk. Also, CISA's inability to determine AIS costs limited our ability to identify whether taxpayer funds could have been put to better use.

CISA Addressed Basic Information-Sharing Requirements of the Act and Completed AIS Upgrades

During our review, we found that CISA addressed the key requirements of the Act, which requires CISA to (1) develop and update policies and procedures needed for sharing CTIs and DMs with Federal and private entities, (2) classify CTIs and DMs, and (3) account for security clearances authorized for private-sector users to receive this information. CISA took steps to meet these requirements by updating its guidance for information sharing, classifying CTIs and DMs, and accounting for security clearances of private-sector individuals.

Information-Sharing Policies and Procedures

CISA updated its policies and procedures in accordance with the Act. For example, in November 2022, CISA and the Department of Justice updated the *Privacy and Civil Liberties Final Guidelines: Cybersecurity Information Sharing Act of 2015*. This document establishes privacy and civil-liberties guidelines governing the receipt, retention, use, and dissemination of CTIs and DMs by a Federal entity obtained in connection with activities authorized by the Act.¹⁴

Classification of CTIs and DMs

CISA properly classified CTIs and DMs as required by the Act. Specifically, cyber analysts used derivative classification for CTIs and DMs. As part of our review, we checked 30 unclassified and 30 classified CTIs that were randomly selected from CY 2021 and CY 2022. From this review, we

¹⁴ The Act requires the Attorney General and the Secretary of Homeland Security to conduct a joint, periodic review (not less frequently than once every 2 years) of the *Privacy and Civil Liberties Final Guidelines: Cybersecurity Information Sharing Act of 2015*.



OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

determined CISA properly classified the sampled CTIs. We determined CISA timely, adequately, and appropriately shared and received CTIs with Federal and non-Federal entities.

CISA classified most CTIs based on the original classification authority.¹⁵ There were 9,313 classified CTIs and DMs for CY 2021 and 9,853 for CY 2022. CISA shared 464 classified CTIs with non-Federal entities in 2021, and 441 in 2022. CISA completed these actions through its Enhanced Cybersecurity Services program, which, unlike the AIS capability, can share sensitive and classified cyber threat information to detect and block malicious cyber activity.¹⁶

Security Clearances for Private Sector to Receive Classified Information

CISA accurately accounted for security clearances of private-sector individuals authorized to receive classified information. Under various information-sharing programs, the Department granted 236 security clearances in CY 2021 and 506 in CY 2022 to private-sector partners. In total, CISA maintained 1,559 active security clearances in CY 2021 and 2,065 in CY 2022. CISA does not track clearances granted under the Act, as the AIS capability only deals with unclassified information.

Similarly, in its biennial report¹⁷ on the Act, the Office of the Inspector General of the Intelligence Community found appropriate Federal entities, including CISA in its role within DHS, continue to implement the Act. According to the report, the key elements of the Act were addressed, including sufficiency of policies and procedures; proper classification of CTIs; appropriate, adequate, and timely sharing and receipt of CTIs; removal of any personally identifiable information (PII); and proper accounting for security clearances for sharing CTIs and DMs.

CISA Completed AIS Upgrades

According to CISA officials, they completed upgrades from AIS 1.0 to AIS 2.0 in March 2022 to increase participation and improve the sharing and receipt of CTIs and DMs. The upgrade to AIS 2.0 included:

- a single ingest point for submissions—previously, there were different ingest points for different AIS participants (e.g., Federal versus non-Federal entities);
- a new status feature that enables submitters to determine the status of their submission (validation accuracy and completeness, pending human review, etc.);

¹⁵ An initial determination that information requires protection against unauthorized disclosure as well as the level of protection required, *Executive Order 13526*, December 29, 2009.

¹⁶ CISA's Enhanced Cybersecurity Services program shares sensitive and classified cyber threat information with accredited commercial service providers to detect and block malicious cyber activity from entering or exiting customer networks.

¹⁷ See AUD-2023-002.



OFFICE OF INSPECTOR GENERAL

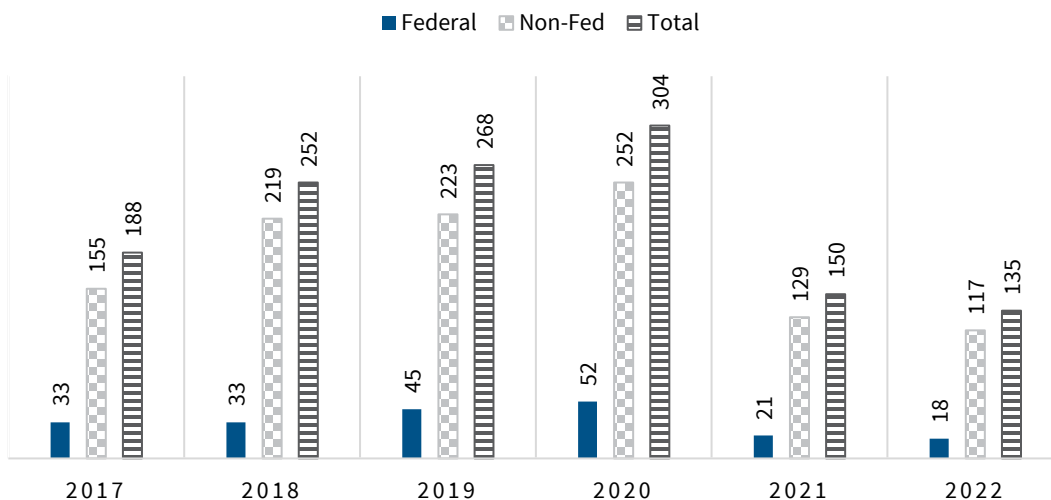
U.S. Department of Homeland Security

- a filtering capability for participants to identify objects of interest; and
- a function enabling organizations to remain anonymous when making submissions— organizations that want to remain anonymous are assigned unique identities allowing other entities to track submissions from the same anonymized organization over time.

Despite CISA’s Upgrades, Overall Participation and Information Sharing Declined

Although CISA upgraded AIS to version 2.0 in 2022, the overall participation and volume of CTIs shared in AIS have declined. AIS’ overall participation dropped from 304 participants in CY 2020 to 135 participants in CY 2022. Of the 135 participants in CY 2022, only 10 upgraded to AIS 2.0, and only 17 new participants began using AIS 2.0. Overall, the number of AIS participants has declined to its lowest number since CISA first began reporting AIS metrics in 2017, as depicted in Figure 2.

Figure 2. Number of AIS Participants Declined from CY 2017 to CY 2022



Source: CISA data on AIS participants

According to CISA officials, the effectiveness of AIS’ capabilities relies on data producers sharing information. From CYs 2021 to 2022, the number of AIS 1.0 external data producers sharing information into AIS decreased from 13 to 11. None of the 11 external data producers in CY 2022 used AIS 2.0. Also, multiple non-Federal participants chose to be indicator recipients only and opted not to function as external data producers.



OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

Overall participation in AIS declined because CISA did not have an outreach strategy to recruit and retain data producers. According to the Act,¹⁸ the Secretary of Homeland Security shall facilitate and promote “periodic sharing, through publication and targeted outreach, of cybersecurity best practices that are developed based on ongoing analyses of CTIs, DMs, and information relating to cybersecurity threats or authorized uses under this title, in the possession of the Federal Government, with attention to accessibility and implementation challenges faced by small business concerns.” Without explanation, CISA paused outreach efforts for promoting AIS in May 2022. CISA’s lack of outreach led to at least one major stakeholder being unaware of AIS. This stakeholder only became aware of the information-sharing capability by conducting its own research and contacting CISA directly to become a participant.

According to CISA officials, it did not continue targeted outreach efforts after the launch of AIS 2.0. Specifically:

- One of CISA’s outreach efforts was to establish the Quality Service Management Office to create an online marketplace so CISA could advertise AIS to potential data producers. However, CISA reorganized its offices and never launched the marketplace. After numerous unsuccessful attempts to interview CISA senior executive management, we could not determine the rationale for why CISA officials stopped actively promoting AIS.
- After pausing outreach activities,¹⁹ CISA management subsequently halted drafting an external affairs guide intended to be part of CISA’s outreach strategy.

CISA could not conduct adequate outreach because its contact information for current AIS participants was inaccurate. Of the 70 AIS participants we attempted to email for an interview, 17 attempts (24 percent) were returned as undeliverable.

Decline in the Number of Shared Indicators

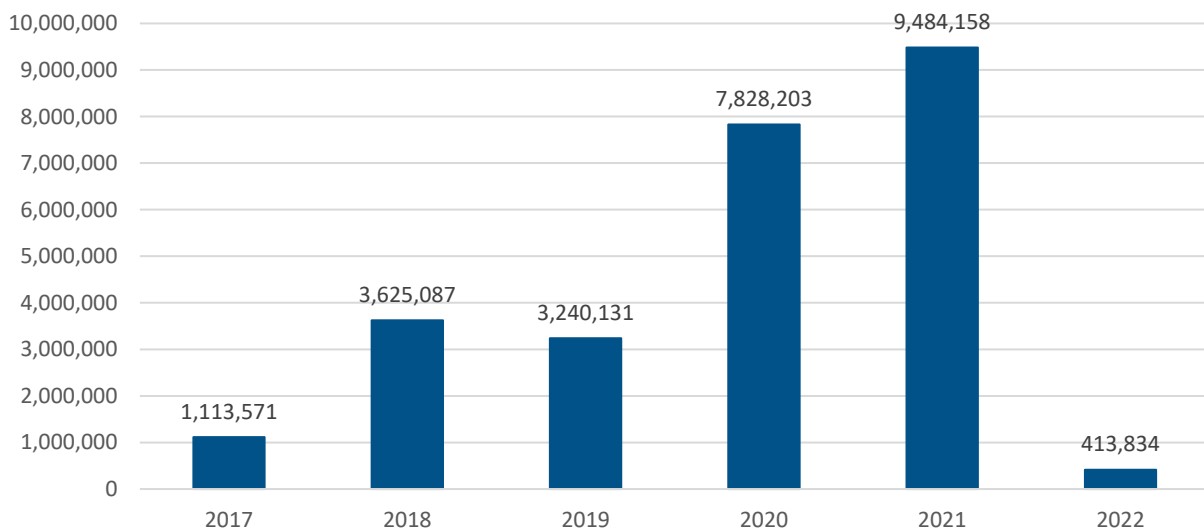
The Federal collection of CTIs significantly declined from CY 2021 to CY 2022. In CY 2021, the Federal collection shared a total of 9,484,158 CTIs. However, the number of CTIs shared decreased significantly to 413,834, an approximately 96 percent decline, in CY 2022, as depicted in Figure 3. The upgrade to AIS 2.0 did not improve the sharing of CTIs by Federal entities, as CISA intended. After the AIS 2.0 upgrade, CISA reported only 173,177 CTIs shared between March and December 2022.

¹⁸ Section 103 of the *Cybersecurity Information Sharing Act of 2015*.

¹⁹ Information on AIS was available on <https://www.cisa.gov> during the outreach pause.



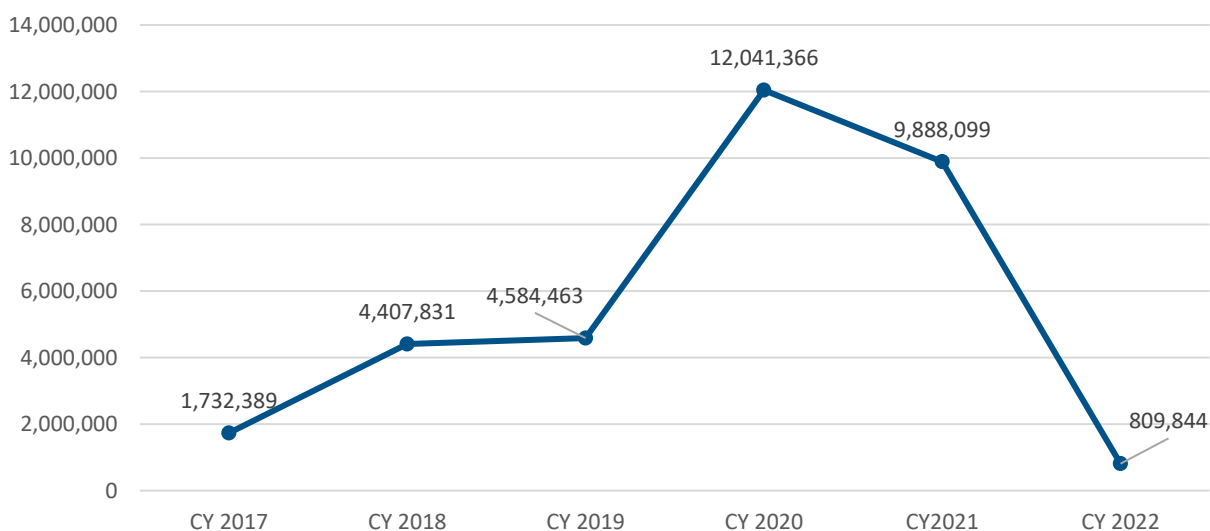
Figure 3. Federal Collection of Shared CTIs Declined from CYs 2021 to 2022



Source: CISA data on the Federal collection CTIs

Just as with the Federal collection, the total number of shared CTIs significantly declined from CY 2020 to CY 2022. In CY 2020, a total of 12,041,366 CTIs were shared, but only 809,844 (approximately a 93 percent reduction) were shared in CY 2022, as depicted in Figure 4.

Figure 4. Total Shared CTIs Declined from CYs 2020 to 2022



Source: CISA data on shared CTIs



OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

The significant decrease in CTIs shared occurred because a system²⁰ used to share CTIs with AIS changed ownership from one Federal partner to another due to requirements in the National Defense Authorization Act.²¹ In CY 2021, the outgoing Federal partner shared approximately 9 million CTIs in AIS. But in CY 2022, after the incoming Federal partner took ownership of the system, this number fell to 16,697, representing a decrease of more than 99 percent. The incoming Federal partner previously shared more than 5,000 CTIs with AIS in CY 2021, but it stopped sharing CTIs in AIS altogether in CY 2022. According to CISA officials, the incoming Federal partner stopped sharing information based on unspecified security concerns with transferring information from its current system to AIS.

CISA Cannot Identify Funding Expenditures for the AIS Capability

CISA could not identify detailed FY 2021 and FY 2022 funding expenditures for the AIS capability. We requested the cost information for the AIS 2.0 upgrade, but CISA officials said the AIS funding falls under the National Cybersecurity Protection System (NCPS) budget.²² The NCPS budget included five capability areas,²³ of which funding for AIS falls under the information-sharing capability category. According to a senior CISA official, CISA spent \$31 million and \$35 million on its information-sharing capability costs for FYs 2021 and 2022, respectively. Within the broader category of information sharing, AIS expenditures are categorized under indicator management, which according to CISA officials was budgeted to spend approximately \$10 million each year. CISA could not provide further details of AIS expenditures for FYs 2021 and 2022. Further, because the budget for AIS was combined with other information-sharing capabilities under NCPS, CISA could not determine the costs for capability upgrades and program operations.

Conclusion

Insufficient participation in AIS 2.0 along with the reduction in CTIs has impeded CISA's ability to facilitate the sharing of cyber threats in real time. The limited sharing of CTIs creates information silos and gaps and may make it difficult for Federal and non-Federal entities to identify and address new cyber threats, putting the Nation's networks and critical infrastructure at risk. Due to the voluntary nature of AIS and the decrease in data producers, continued operation of AIS is ineffective and therefore a potential waste of taxpayer funding. Merging the budget for AIS with

²⁰ This system monitors emails, documents, and incoming traffic that could infect U.S. Department of Defense networks.

²¹ *Public Law 115-232, John S. McCain National Defense Authorization Act for Fiscal Year 2019*, August 13, 2018.

²² NCPS is an integrated system-of-systems that provides intrusion detection and prevention capabilities, advanced analytics, and information-sharing mechanisms that mitigate cyber threats to Federal Civilian Executive Branch networks and augment their internal cyber capabilities. AIS is a capability that was delivered under the scope of the NCPS program.

²³ The NCPS capability areas are intrusion detection, intrusion prevention, information sharing, analytics, and core infrastructure.



OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

other information-sharing capabilities under NCPS impedes CISA's ability to directly track and assess expenditures dedicated to maintaining and upgrading AIS. Therefore, we cannot determine whether the funds CISA spent for the AIS upgrade and continued operations could have been put to better use.

Recommendations

Recommendation 1: We recommend that the Director of CISA develop and implement a strategy and performance metrics to actively recruit and retain Automated Indicator Sharing participants, including Federal data producers.

Recommendation 2: We recommend the Director of CISA, in conjunction with its Chief Information Officer and Chief Financial Officer, maintain spend plans for documenting future costs related to the Automated Indicator Sharing capability.

Management Comments and OIG Analysis

CISA provided management comments on a draft of this report. We included the comments in their entirety in Appendix B. We also received technical comments to the draft report and revised the report as appropriate. CISA concurred with both of our recommendations. We consider recommendation 1 open and unresolved, and recommendation 2 open and resolved. A summary of CISA's response and our analysis follows.

CISA Comments to Recommendation 1: Concur. CISA's Cybersecurity Division (CSD) is conducting an independent evaluation of the AIS service, which includes exploring alternative approaches to its automated threat intelligence and information-sharing capabilities to align with the new long-term Threat Intelligence Enterprise Services strategy. CSD is exploring a long-term vision for Threat Intelligence Enterprise Services, which seeks to address the challenges identified in the audit, build on existing capabilities for AIS, and provide a platform for future growth and evolution, including recruiting and retaining participants and Federal data producers. This evaluation will culminate in a series of recommendations for CISA leadership consideration. CISA will develop tailored communications for its customer base regarding any leadership-approved changes, as appropriate. Estimated Completion Date: July 31, 2025.

OIG Analysis of CISA Comments: We agree with CISA's actions to conduct an independent evaluation of the AIS service and create a new long-term Threat Intelligence Enterprise Services strategy. However, CISA did not include implementing performance metrics in its response. Therefore, this recommendation will remain open and unresolved until CISA provides documentation that it has developed and implemented a performance metric to actively recruit and retain AIS participants.



OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

CISA Comments to Recommendation 2: Concur. CISA CSD’s Mission Engineering subdivision will develop and maintain an activity-based spend plan specific to AIS to document future AIS costs. Estimated Completion Date: December 31, 2024.

OIG Analysis of CISA Comments: CISA’s actions are responsive to the recommendation. This recommendation will remain open and resolved until CISA provides documentation to support that all planned corrective actions are completed.



OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

Appendix A: Objective, Scope, and Methodology

The Department of Homeland Security Office of Inspector General was established by the *Homeland Security Act of 2002* (Pub. L. No. 107–296) by amendment to the *Inspector General Act of 1978*.

Our objective was to determine the extent of DHS’ progress in meeting the cybersecurity information-sharing requirements of the *Cybersecurity Act of 2015* for CYs 2021 and 2022.

To answer our objective, we assessed CISA’s progress implementing the cybersecurity information-sharing requirements according to Section 107 of the Act. Our evaluation focused on the progress CISA has made since our last review in CYs 2021 and 2022. Specifically, we determined whether DHS and its components have:

- revised existing policies and procedures or issued additional guidance to improve the sharing of CTIs within the Federal Government;
- enhanced the information-sharing mechanisms and methodology used to receive and share CTIs and DMs and remove unrelated personal information;
- increased the number of participants that share and receive CTIs;
- improved the timeliness and quality of the CTIs that CISA shares and receives with its partners; and
- established new guidance or revised existing procedures to ensure CTIs and DMs are properly classified.

Our fieldwork consisted of interviewing selected personnel from DHS components and offices including CISA, U.S. Immigration and Customs Enforcement, and U.S. Customs and Border Protection. We also met with non-Federal AIS participants. Under AIS’ publicly available sharing guidance, a non-Federal entity sharing information with CISA must provide consent before its identity can be shared with other Federal entities. We non-statistically selected and solicited feedback from a total of 70 AIS participants (20 Federal agencies and 50 non-Federal entities) to obtain their perspectives on the effectiveness of the AIS program. Only 13 of 70 participants (19 percent) provided their feedback, including 9 non-Federal entities. Additionally, we judgmentally selected 30 unclassified and 30 classified CTIs for both 2021 and 2022 to determine if the CTIs sampled were properly classified.

We conducted this review under the authority of the *Inspector General Act of 1978, as amended*, 5 U.S.C. §§ 401–424, and according to the *Quality Standards for Inspections and Evaluations*, issued by the Council of the Inspectors General on Integrity and Efficiency.



OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

DHS OIG's Access to DHS Information

During this review, CISA provided timely responses to our requests for information and did not delay or deny access to information we requested.



OFFICE OF INSPECTOR GENERAL
U.S. Department of Homeland Security

Appendix B:
CISA Comments on the Draft Report

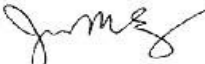


U.S. Department of Homeland Security
Cybersecurity & Infrastructure Security Agency
Office of the Director
Washington, DC 20528

BY ELECTRONIC SUBMISSION

August 16, 2024

MEMORANDUM FOR: Joseph V. Cuffari, Ph.D.
Inspector General

FROM: Jen Easterly 
Director
Cybersecurity and Infrastructure Security Agency

SUBJECT: Management Response to Draft Report: "CISA Faces
Challenges Sharing Cyber Threat Information as Required by
the Cybersecurity Act of 2015"
(Project No. 23-025-AUD-CISA)

Thank you for the opportunity to comment on this draft report. The Cybersecurity and Infrastructure Security Agency (CISA) appreciates the work of the Office of Inspector General (OIG) in planning and conducting its review and issuing this report.

CISA leadership is pleased to note OIG's positive recognition that CISA addressed the basic information sharing requirements of the Cybersecurity Act of 2015, including CISA's efforts to update its guidance, properly classify cyber threat indicators and defensive measures, and accurately account for security clearances. CISA remains committed to strengthening the sharing of cyber threat information and tracking of costs for Automated Indicator Sharing (AIS) through the development of activity-based spend plans to document future costs related to AIS.

The draft report contained two recommendations with which CISA concurs. Enclosed find our detailed response to each recommendation. CISA previously submitted technical comments addressing several accuracy, contextual, and other issues under a separate cover for OIG's consideration, as appropriate.

Again, thank you for the opportunity to review and comment on this draft report. Please feel free to contact me if you have any questions. We look forward to working with you again in the future.

Enclosure



OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

Enclosure: Management Response to Recommendations Contained in OIG 23-025-AUD-CISA

OIG recommended that the Director of CISA:

Recommendation 1: Develop and implement a strategy and performance metrics to actively recruit and retain Automated Indicator Sharing participants, including Federal data producers.

Response: Concur. The CISA Cybersecurity Division (CSD) is currently conducting an independent evaluation of the AIS service, which includes exploring alternative approaches to its automated threat intelligence and information sharing capabilities that will align with the new long-term Threat Intelligence Enterprise Services (TIES) strategy.¹ CSD is exploring a long-term vision for TIES, which seeks to address the challenges identified in the audit and build on existing capabilities (e.g., AIS), and provide a platform for future growth and evolution including in recruitment and retention of participants and Federal data producers. This evaluation will culminate in a series of recommendations for CISA leadership consideration with tailored communications to be developed for our customer base informing them of any leadership-approved changes, as appropriate. Estimated Completion Date (ECD): July 31, 2025.

Recommendation 2: In conjunction with its Chief Information Officer and Chief Financial Officer, maintain spend plans for documenting future costs related to the Automated Indicator Sharing capability.

Response: Concur. Historically, costs for AIS were tracked under a program-level spend plan for the National Cybersecurity Protection System. Using that spend plan, CISA's Cybersecurity Division (CSD), Mission Engineering (ME) subdivision would continually estimate project expenditures throughout the year of execution based on priorities. Even though CISA did not develop a standalone AIS spend plan, CISA CSD ME reviewed previous spend plans for work aligned to Information Sharing, which included AIS. Moving forward, CISA CSD ME will develop and maintain an activity-based spend plan specific to AIS to document future AIS costs. ECD: December 31, 2024.

¹ Blog Post: Enabling Threat-Informed Cybersecurity: Evolving CISA's Approach to Cyber Threat Information Sharing
December 18, 2023, Michael Duffy, Associate Director, CISA

[Enabling Threat-Informed Cybersecurity: Evolving CISA's Approach to Cyber Threat Information Sharing | CISA](#)



OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

Appendix C:

DHS' Responses to the Office of the Inspector General of the Intelligence Community Questionnaire

Policies, Procedures, and Guidelines

1. What is the agency's process in practice for sharing CTIs within the Federal Government? Define "sharing" for the purposes of your agency.

CISA defines sharing as making both unclassified and classified CTIs and DMs available to Federal Government and private partners. CISA does this using automated systems:

- For unclassified sharing, CISA created the AIS capability in 2016 to enable the real-time exchange of unclassified CTIs and DMs to participants of the AIS community. CISA offers the AIS service at no cost to participants as part of CISA's mission to work with public and private sector partners to identify and help mitigate cyber threats through information sharing. The fundamental concept of the AIS capability is to promote interaction among participants. AIS conducts the following automated sharing:
 - The Public collection shares CTIs with all AIS participants. Non-Federal participants must sign the AIS Terms of Use.
 - The Federal collection also shares CTIs with Federal departments and agencies. Federal departments and agencies must sign the Multilateral Information Sharing Agreement.
 - The CISCPC collection shares CTIs with non-Federal entities that have also signed the Cyber Information Sharing and Collaboration Agreement with CISA. The CISCPC collection is also available to Federal departments and agencies.
- For classified sharing, CISA uses Enhanced Cybersecurity Services, which is an intrusion detection, prevention, and analysis capability. CISA also uses Einstein 3 Accelerated, a system that detects cyberattacks targeting Federal Civilian Executive Branch networks and that actively prevents potential compromises.

2. What are the agency's policies, procedures, and guidelines for sharing CTIs within the Federal Government?

DHS has policies, procedures, and guidelines for sharing CTIs. Specifically, DHS developed or assisted in the development of the following four policies and procedures:

- *Sharing of CTIs and DMs by the Federal Government under the Cybersecurity Information Sharing Act of 2015, The Department of Defense, The Department of Homeland Security,*



OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

The Department of Justice, The Office of the Director of National Intelligence, February 16, 2016;

- *Guidance to Assist Non-Federal Entities to Share CTIs and DMs with Federal Entities under the Cybersecurity Information Sharing Act of 2015, The Department of Homeland Security, The Department of Justice, October 2020;*
- *Final Procedures Related to the Receipt of CTIs and DMs by the Federal Government, The Department of Homeland Security, The Department of Justice, June 15, 2016; and*
- *Privacy and Civil Liberties Final Guidelines: Cybersecurity Information Sharing Act of 2015, The Department of Homeland Security, The Department of Justice, November 30, 2022.*

3. Do the policies, procedures, and guidelines include guidance for removing information not directly related to a cybersecurity threat that is personal information of a specific individual or information that identifies a specific individual?

Yes. Specifically, Section 9.5 of *Sharing of CTIs and DMs by the Federal Government under the Cybersecurity Information Sharing Act of 2015* contains guidance for Federal entities relating to personal information review and removal. Section 3 of the AIS Terms of Use contains guidance for AIS data producers regarding removal of any unclassified CTIs or DMs that are not directly related to a cybersecurity threat.

4. If the four procedure documents created as a result of CISA²⁴ were not provided for question 2, is the agency aware of the documents?

Not applicable.

5. Does the process for sharing CTIs within the Federal Government determined from question 1 align with the policies, procedures, and guidelines from question 2?

Yes.

6. Are the agency's policies, procedures, and guidelines (if different from the four CISA procedure documents) sufficient and compliant with the guidance in CISA Section 103(a) and (b) and 105(a), (b), and (d)?

Not Applicable.

7. If there are differences in the policies, procedures, and guidelines implemented among the agencies, does it impact the sharing of cyber threat information? (OIGs can first determine

²⁴ The four documents are detailed in question 2.



OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

whether not using the four procedure documents impacts the sharing – Intelligence Community Inspector General will coordinate additional follow-up, if necessary.)

Not Applicable.

8. Does the agency believe the policies, procedures, and guidelines are sufficient, or are there any gaps that need to be addressed?

According to CISA officials, the policies, procedures, and guidelines referenced in question 2 sufficiently address the sharing of unclassified CTIs and DMs. However, officials acknowledged interagency noncompliance with the agreed-upon standardized sharing policies and recommendations included in approved Multilateral Information Sharing Analysis.

Sharing CTIs and DMs with Private Sector

9. Has the agency shared CTIs and DMs with the private sector?

Yes, CISA has shared unclassified CTIs and DMs with non-Federal entities through the AIS service as CISCP packages. Specifically, it shared machine-readable versions of various CISA-published products (e.g., indicator bulletins, activity alerts, and analysis reports). Additionally, CISA's implementation of the AIS service allows other Federal agencies to share their unclassified CTIs and DMs with non-Federal entities. CISA shares classified CTIs and DMs via the Enhanced Cybersecurity Services and Einstein 3 Accelerated programs. According to the *Cybersecurity Act of 2015*, individuals within non-Federal entities with the appropriate security clearances can receive classified CTIs and DMs.

10. If yes for question 9, are any of the shared CTIs and DMs classified?

Yes, CISA shared classified CTIs and DMs. CISA shared a total of 9,313 classified CTIs and DMs for 2021 and 9,853 for 2022. In 2021 and 2022, respectively, CISA shared 464 and 441 classified CTIs with the private sector.

11. If yes for question 10, what was the process used by the agency to classify the shared CTIs and DMs?

CTIs are classified using derivative classification. The original classification of the CTIs remains with the original classification authority. CISA uses additional security classification guides to derivatively classify CTIs.

Specifically, cyber analysts used derivative classification for CTIs and DMs. CISA classified most CTIs based on the original classification authority. This was done through its Enhanced



OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

Cybersecurity Services program, which, unlike the AIS capability, can share sensitive and classified cyber threat information to detect and block malicious cyber activity.

11a. Review a sample of the shared CTIs and DMs and determine whether the cyber threat information was properly classified.

The audit team sampled 30 unclassified and 30 classified CTIs and DMs for CYs 2021 and 2022 and concluded that they were classified correctly.

11b. Did the agency's process result in the proper classification?

Yes, CISA's process resulted in proper classification.

Accounting of Security Clearances

12. Has the agency authorized security clearances for sharing CTIs and DMs with the private sector?

Yes, CISA granted 236 security clearances in 2021 and 506 in 2022 to private-sector partners under various DHS information-sharing programs. However, CISA does not track the number of security clearances that have been issued under the Act. Since CISA shares unclassified CTIs via AIS, a security clearance is not required to receive the information.

12a. If yes, how did the agency account for the number of security clearances and how many security clearances were active in CYs 2021 and 2022?

The Department maintains active security clearance information in the Integrated Security Management System. In 2021 and 2022, DHS maintained 1,559 and 2,065 active security clearances, respectively.

13. Are the number of active security clearances sufficient, or are there barriers to obtaining adequate number of cleared personnel to receive cyber threat information?

CISA identified no barriers.

Using and Disseminating CTIs and DMs Shared by Other Federal Agencies

14. Has the agency used and disseminated CTIs and DMs shared by other Federal agencies?



OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

Yes, CISA uses AIS to share the CTIs and DMs contained within its Public and Federal collections with CISA's threat-intelligence platform (Analyst1). AIS also enables CTIs from Analyst1 and other internal CTI-generation sources to be disseminated to the AIS TAXII collections.

CISA analysts review cyber threat intelligence from various sources for the primary purpose of sharing unclassified CTIs for CISA-published products (e.g., indicator bulletins, activity alerts, and analysts reports).

14a. If yes, determine whether the agency used and disseminated the shared cyber threat information appropriately? Provide results.

CISA shares unclassified CTIs via the AIS program according to the Department's Traffic Light Protocol and classified CTIs under the business rules of the Enhanced Cybersecurity Services programs. According to the AIS Terms of Use, CISA anonymizes the identities of the sources of the CTIs. CISA shares all CTIs received in AIS on a real-time, machine-to-machine basis.

CISA analysts also share indicator bulletins by anonymizing source information, which is then turned into machine-readable files that are shared with authorized partners through DHS-approved platforms or portals.

For content disseminated to Federal subscribers, the system adheres to the package marking. All Federal clients are expected to comply with the marking as well.

14b. If yes, did the agency use the shared cyber threat information to mitigate potential threats? Please explain.

CISA is in the process of providing examples of how CTIs were used to mitigate potential threats.

Sharing CTIs and DMs with Other Federal Agencies

15. Has the agency shared CTIs and DMs with other Federal agencies?

Yes, Federal agencies participating in the AIS service can access CISA-sourced CTIs contained within the Public, Federal, and CISCP collections. CISA's implementation of the AIS service also allows other Federal and non-Federal entities to share their unclassified CTIs and DMs with participating Federal agencies.

15a. If yes, determine whether the agency shared the cyber threat information in a timely and adequate manner with appropriate entities or, if appropriate, made publicly available. Provide results.



OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

Yes, a sample of 30 unclassified CTIs and DMs for 2021 and 2022 were reviewed and found to be shared in a timely and adequate manner.

16. With which Federal agencies and what capabilities or tools were used to share the cyber threat information?

CISA reported 23 Federal agencies directly connect to AIS to receive CTIs. AIS also supports indirect connections to the service via third-party providers.

17. Have other Federal entities shared CTIs and DMs with the agency?

Yes, four Federal agencies shared CTIs and DMs directly into AIS.

17a. If yes, determine if cyber threat information was shared and/or received in a timely, adequate, and appropriate manner. Provide results.

Yes, we reviewed a sample of 30 unclassified CTIs and DMs for 2021 and 2022 and determined they were shared in a timely and adequate manner. Note: The sample of 30 unclassified CTIs and defensive measures is not limited to the four Federal agencies referenced above.

DHS' Sharing Capability and Processes (To be answered by DHS only)

18. How many CTIs and DMs did entities share with DHS through the AIS capability in CYs 2021 and 2022? Provide results.

According to CISA officials, the number of CTIs and DMs shared with DHS for CYs 2021 and 2022 were:

- For CY 2021:
 - Public collection: 397,218
 - Federal collection: 9,484,158
 - CISCP collection: 6,723

- For CY 2022:
 - AIS 1.0:
 - Public collection: 227,459
 - Federal collection: 240,657
 - CISCP collection: 3,040



OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

- AIS 2.0:²⁵
 - Public collection: 163,032
 - Federal collection: 173,177
 - CISCP collection: 2,479

19. How many of those CTIs and DMs reported for question 18 did DHS share with other Federal entities in CYs 2021 and 2022? Provide results.

DHS shares all CTIs and DMs reported. AIS uses a client-server TAXII model that has three different TAXII collections (data repositories) that allow participants to share and receive CTIs. Participating Federal agencies have access to all AIS TAXII collections and can retrieve CTIs as desired.

CTIs and DMs Received from Other Federal Agencies

20. (Agencies other than DHS) How many CTIs and DMs did DHS relay to the agency via AIS in CYs 2021 and 2022?

Not applicable.

21. If there are differences in the numbers reported by DHS and the agencies, what is the cause? (Intelligence Community Inspector General will coordinate follow-up)

Not applicable.

Personal Information Violations

22. Did any Federal or non-Federal entity share information with the agency that was not directly related to a cybersecurity threat that contained personally identifiable information (PII)?

No, AIS participants (Federal and non-Federal) have a responsibility to not share information with the AIS service that is not directly related to a cybersecurity threat. As an additional layer of protection, CISA has implemented automated controls in AIS to identify, for additional review, any free text fields that may contain potential PII. Analysts within CSD/Threat Hunting perform a human review, and if necessary, will redact any PII and subsequently send the approved information through AIS. CISA's Office of the Chief Privacy Officer conducts regular privacy reviews of the AIS PII check process.

²⁵ CISA completed upgrades from AIS 1.0 to AIS 2.0 and started using this updated version March 4, 2022. AIS 2.0 includes CTIs and DMs shared from March 2022 to December 2022.



OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

22a. If yes, provide a description of the violation.

Not applicable based on question above.

23. Was the privacy and civil liberties of any individuals affected due to the agency sharing CTIs and DMs?

No.

23a. If yes, how many individuals were affected? Provide a description of the effect for each individual and instance.

Not applicable based on question above.

24. Did the agency receive any notices regarding a failure to remove information that was not directly related to a cybersecurity threat?

No, the AIS service team did not receive any notices regarding a failure to remove information that was not directly related to a cybersecurity threat.

24a. If yes, how many notices were received and did any of those notices relate to personally identifiable information for any individuals?

Not applicable based on question above.

25. Was there any adverse effect on the privacy and civil liberties of U.S. persons due to the activities carried out under this title by the agency?

No.

25a. If yes, did the agency take adequate steps to reduce adverse effects? Provide results.

Not applicable.

Potential Barriers

26. Are there any barriers that affected the sharing of CTIs and DMs among Federal entities? Provide a description of the barriers and the impact the barriers have on the sharing of CTIs and DMs.

Yes, according to CISA officials, barriers continue to include:

- Federal entities not adhering to Federal cyber information-sharing interagency policy



OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

recommendations;

- a lack of dedicated funding for implementing those interagency policy recommendations;
- a shortage of organizational resources to support machine-readable indicator sharing;
- a lack of vendor support for the generation and sharing of AIS-compliant STIX files; and
- the reluctance of Federal organizations to share their cybersecurity incident data via machine-to-machine connections.

26a. Any difficulties with using a specific capability or tool to share and/or receive cyber threat information?

According to CISA officials, they continue to experience inconsistent vendor support for the latest STIX and TAXII specifications, which hinders Federal entities from deploying shared CTIs and DMs from others in the community into their vendor tools. These tools include threat-intelligence platforms, security information and event management, and other network-connected sensors and devices. CISA continues to perform proactive outreach to vendors to advocate for adoption of the latest STIX and TAXII specification into their products and services to improve operational collaboration using common-structured CTI sharing formats.

Further, threat-intelligence-platform tools are more likely to include sharing capabilities than other limited-purpose security sensors such as firewalls. In addition, CISA continues to see limited adoption of threat-intelligence-platform products among Federal entities. As part of its engagements, CISA will continue to promote adoption of free or low-cost threat-intelligence platforms that elevate stakeholders' ability to detect and respond to known threats from CTI sources as well as their ability to share structured data back to CISA via STIX and TAXII mechanisms.

26b. Any difficulties due to classification of information?

No. The AIS service does not receive or share classified CTIs or DMs.

26c. Any difficulties due to a reluctance to sharing information?

Yes, Federal entities continue to be reluctant to share information into the Public collection. Some prefer to share exclusively within the Federal collection. Others may have policy requirements to share only within their relevant sector among eligible stakeholders. Currently, AIS does not offer a narrow sector-specific community collection. Some Federal entities have expressed reluctance toward dedicating resources for preparing internal cyber threat information knowledge for external consumption. They also do not have the maturity to produce unique CTIs and DMs of value for the broader community.



OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

26d. Any difficulties due to the number of CTIs and DMs received? Too many to ingest and review?

Yes, Federal and private-sector entities indicated that volume is not as much of an issue as their ability to effectively filter and sort CTIs that are appropriate for their sector. If CTI and DM data is not categorized properly, entities cannot deploy relevant mitigation measures and disregard data not targeted for their sector. In some cases, for example, users have limited bandwidth and storage on their sensors using deployed CTIs. Therefore, stakeholders need to prioritize the CTIs that are most likely to affect their enterprise. Some stakeholders avoid deploying uncategorized datasets in favor of more highly tailored, sector-specific datasets.

26e. Any issues with the quality of the information received?

Yes, in its latest TAXII 2.1 capability, CISA responded to previously identified quality concerns by introducing a CISA opinion score of all shared CTIs, which users can filter, to make their own decisions about which CTIs to deploy for detection and mitigation measures in their environments. This capability reduces the risk of false positives and allows participants to triage which alerts to prioritize among the growing volume of alerts within operations teams.

26f. Has the agency performed any steps to mitigate the barriers identified?

Yes, CISA implemented the latest STIX 2.1 and TAXII 2.1 capability in March 2022 to improve delivery of CTIs and DMs to participants. CISA continues to work with the cybersecurity vendor community to grow adoption of the latest specifications and increase the number of sharing tools that are interoperable with DHS' capabilities. Further, CISA continues to engage with Federal and non-Federal entities to encourage sharing and document feedback to introduce future features and capabilities that best encourage sharing of CTIs and DMs for awareness of the latest cross-sector cyber threats.

27. Any cybersecurity best practices identified by the agency through ongoing analyses of CTIs, DMs, and information related to cybersecurity threats? Did the agency share or receive any cybersecurity best practices? [Section 103(a)(5)]

Yes, CISA sponsored a STIX 2.1 Best Practice Guide developed by MITRE and approved and released by the Organization for the Advancement of Structured Information Standards CTI Technical Committee on September 15, 2022. The guide suggests best practices to use for STIX content.

28. What capabilities/tools does the agency use to share and/or receive CTIs and DMs? Are the capabilities/tools providing the agency with the necessary cyber threat information?

AIS is a service that CISA provides to enable real-time exchange of machine-readable CTIs and DMs between public and private-sector organizations. Additionally, the CTI and DMs Submission



OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

System provides a secure, web-enabled method of sharing CTIs and DMs with CISA. Both capabilities provide the means to share CTIs with CISA, but are not designed for, or intended to, capture the usefulness or usage of CTIs that are made available to end users (i.e., CISA analysts).

29. Does the agency receive unclassified cyber threat information from ICOAST? If not, why? (resources, system incompatibility, lack of information)

Yes, CISA received 136,958 Intelligence Community and Analysis Tool packages in CY 2022. CISA did not receive any for 2021.

30. Has DHS and the heads of the appropriate Federal entities, in consultation with the appropriate private entities, jointly reviewed the guidelines issues? [Section 105(b)(2)(B)]

Yes, the Privacy and Civil Liberties Guidelines require a review every 2 years. The review was completed in November 2022.



OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

Appendix D: Office of Audits Major Contributors to This Report

Tarsha Cary, Director
Danny Urquijo, Audit Manager
James Diaz, Auditor-in-Charge
Robert Williams Jr., Auditor
Kiersten Godfrey, Auditor
Larry Malone, Auditor
Juan Santana, Auditor
Tom Hamlin, Communications Analyst
Jeffrey Whitaker, Independent Referencer
Javier Benton, Independent Referencer



OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

Appendix E: Report Distribution

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
Deputy Chiefs of Staff
General Counsel
Executive Secretary
Director, GAO/OIG Liaison Office
Under Secretary, Office of Strategy, Policy, and Plans
Assistant Secretary for Office of Public Affairs
Assistant Secretary for Office of Legislative Affairs

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees

External

Additional Information

To view this and any other DHS OIG reports, Please visit our website: www.oig.dhs.gov

For further information or questions, please contact the DHS OIG Office of Public Affairs via email: DHS-OIG.OfficePublicAffairs@oig.dhs.gov



DHS OIG Hotline

To report fraud, waste, abuse, or criminal misconduct involving U.S. Department of Homeland Security programs, personnel, and funds, please visit: www.oig.dhs.gov/hotline

If you cannot access our website, please contact the hotline by phone or mail:

Call: 1-800-323-8603

U.S. Mail:
Department of Homeland Security
Office of Inspector General, Mail Stop 0305
Attention: Hotline
245 Murray Drive SW
Washington, DC 20528-0305