U.S. DEPARTMENT OF HOMELAND SECURITY

OFFICE OF INSPECTOR GENERAL

OIG-25-46

September 26, 2025

FINAL REPORT

CISA Has Not Finalized Plans for Automated Cyber Threat Information Sharing Beyond Cybersecurity Act of 2015 Expiration

OFFICE OF INSPECTOR GENERAL
U.S. Department of Homeland Security
Washington, DC 20528 | www.oig.dhs.gov

September 26, 2025

MEMORANDUM FOR: Madhu Gottumukkala, Ph.D.
Acting Director
Cybersecurity Infrastructure and Security Agency

FROM: Joseph V. Cuffari, Ph.D.
Inspector General

JOSEPH V CUFFARI
Digitally signed by JOSEPH V CUFFARI
Date: 2025.09.26 07:56:36 -07'00'

SUBJECT: *CISA Has Not Finalized Plans for Automated Cyber Threat Information Sharing Beyond Cybersecurity Act of 2015 Expiration*

Attached for your action is our final report, *CISA Has Not Finalized Plans for Automated Cyber Threat Information Sharing Beyond Cybersecurity Act of 2015 Expiration*. We incorporated the formal comments provided by your office.

The report contains one recommendation aimed at improving information sharing under the *Cybersecurity Information Sharing Act of 2015*. Your office concurred with the recommendation. Based on information provided in your response to the draft report, we consider recommendation 1 open and resolved. Once your office has fully implemented the recommendation, please submit a formal closeout letter to us within 30 days so that we may close the recommendation. 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 Craig Adelman, Deputy Inspector General, Office of Audits, at (202) 981-6000.

Attachment

DHS OIG HIGHLIGHTS

CISA Has Not Finalized Plans for Automated Cyber Threat Information Sharing Beyond Cybersecurity Act of 2015 Expiration

September 26, 2025

Why We Did This Review

The *Cybersecurity Information Sharing 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 select agencies to submit a joint report to Congress every 2 years on actions to share cyber threat information.

We conducted this review to determine the extent of DHS' progress to meet the Act's cybersecurity information-sharing requirements for calendar years 2023 and 2024.

What We Recommend

We made one recommendation for CISA to determine whether to maintain AIS beyond September 30, 2025.

For Further Information:
Contact OIG Public Affairs at (202) 981-6000 or DHS-OIG.OfficePublicAffairs@oig.dhs.gov.

What We Found

The Cybersecurity and Infrastructure Security Agency (CISA) met requirements of the *Cybersecurity Information Sharing Act of 2015.* However, CISA has not finalized its plans for the continued use of Automated Indicator Sharing (AIS). Without finalizing this plan, CISA could be hindered in how it shares information on cyber threats, which would reduce its ability to protect the Nation's critical infrastructure from cyber threats.

Since our 2024 review, CISA made progress to meet the requirements of the Act by maintaining its guidance for information sharing, properly classifying cyber threat indicators and defensive measures, and accounting for security clearances of private-sector individuals.

Although AIS resulted in increased sharing of cyber threat indicators from approximately 1 million in 2023 to more than 10 million in 2024, this increase was primarily from one private-sector participant's contributions, which accounted for 89 percent of the public collection and 83 percent of the Federal collection. This unevenness in reporting indicates potential overreliance on one partner. Moreover, CISA did not conduct adequate outreach to add AIS participants and reduce reliance on certain partners. The number of Federal and non-Federal AIS users decreased by 65 percent since peaking in 2020. To address this challenge, CISA continues to implement our previous recommendation to develop and implement a new strategy to recruit and retain AIS participants.

CISA Response

CISA concurred with our recommendation and noted it does not have immediate or near-term plan to discontinue AIS, even if the Act expires. Appendix B contains CISA's management comments in their entirety.

Background

The Department of Homeland Security has a critical mission to protect the Nation's cyberspace, including its own computer systems and as well as those belonging to other Federal civilian agencies. 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.

On December 18, 2015, the President enacted the *Cybersecurity Information Sharing Act of 2015* (Act) [1] to establish a voluntary process between public and private-sector entities to share cyber threat information. The Act requires the Director of National Intelligence, the Secretaries of Homeland Security and Defense, and the U.S. Attorney General, in consultation with the heads of other appropriate Federal entities, to develop and issue procedures jointly to facilitate and promote sharing of:

- classified and unclassified cyber threat indicators (CTI)[2] and defensive measures (DM)[3] by the Federal Government; and
- other information and best practices to mitigate cyber threats.

The Act requires the Inspectors General from the Intelligence Community and the Departments of Commerce, Defense, Energy, Justice, Homeland Security, and Treasury to submit a joint report to appropriate congressional oversight committees, beginning in December 2017, and biennially thereafter until September 30, 2025. In the biennial joint report, the participating Offices of Inspector General must provide an overall assessment of:

- the policies, procedures, and guidelines to share CTIs and DMs within the Federal Government, including removing personal information that is not directly related to CTIs and DMs;
- whether CTIs or DMs have been properly classified and an accounting exists for the number of security clearances granted to private-sector users receiving classified information under the Act;
- actions taken by Federal agencies based on CTIs or DMs shared within the Federal Government; and

[1] *Cybersecurity Information Sharing Act of 2015*, Pub. L. 114-113, Div. N, December 18, 2015.
[2] CTIs are defined by the Act 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.
[3] DMs are defined by the Act to generally mean an action, device, procedure, technique, or other measure applied to an information system or information that is stored on, processed by, or transiting an information system that detects, prevents, or mitigates a known or suspected cybersecurity threat or vulnerability.

- barriers to sharing CTIs or DMs among Federal agencies.

In 2016, CISA created the Automated Indicator Sharing (AIS) capability to enable real-time exchange of unclassified machine-readable CTIs and DMs to help protect participants of the AIS community[4] and reduce the prevalence cyberattacks. The AIS program provides participants a no-cost, voluntary information-sharing service to identify cyber threats.

Additionally, White House Memorandum 005632[5] requires the Federal Government to ensure rapid expansion of this capability. According to the memorandum, all recipient departments and agencies should actively participate in the AIS capability and allocate necessary resources to make it operational.

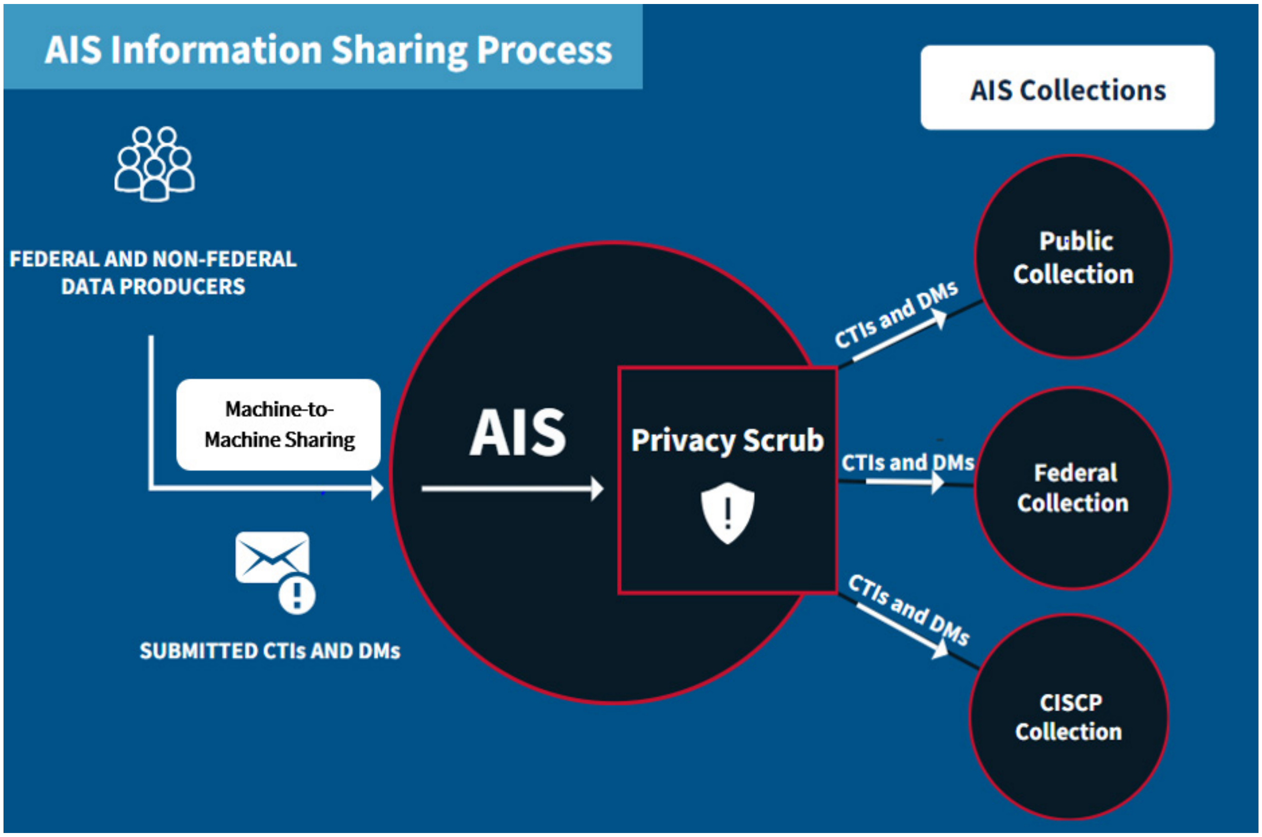
AIS is composed of three information collections (depicted in Figure 1) that enable sharing and receipt of CTIs and DMs:

1. The Federal collection is available to all departments and agencies that sign the Multilateral Information-Sharing Agreement.
2. The Public collection is available to all participants. All non-Federal users must sign the AIS Terms of Use to participate.
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.

[4] The AIS community includes Federal agencies; state, local, tribal, and territorial governments; private-sector entities; information-sharing and analysis centers and organizations; and foreign government partners and companies.

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

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



Source: Generated by DHS OIG based on CISA documentation

We completed four previous reviews to assess CISA's progress to meet the Act's requirements. Our most recent report[6] contained two recommendations. One of these is for CISA to implement a strategy and performance metrics to actively recruit and retain AIS participants. This recommendation remains open at the time of this report, but the other recommendation has been closed.

We conducted this review to determine the extent of DHS' progress in meeting the cybersecurity information-sharing requirements of the *Cybersecurity Information Sharing Act of 2015* for calendar years 2023 and 2024.

[6] *CISA Faces Challenges Sharing Cyber Threat Information as Required by the Cybersecurity Act of 2015,* OIG-24-60, September 25, 2024.

Results of Review

CISA Addressed Information-Sharing Requirements

We determined CISA addressed the requirements of the Act by (1) developing and maintaining policies and procedures to share CTIs and DMs with Federal and non-Federal entities; (2) classifying CTIs and DMs; and (3) accounting for security clearances authorized for private-sector users to receive this information.

CISA's Information-Sharing Policies and Procedures Are in Accordance with the Act

CISA's policies and procedures are still in accordance with the Act. In April 2025, CISA and the Department of Justice updated the *Privacy and Civil Liberties Final Guidelines: Cybersecurity Information Sharing Act of 2015*, which 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.[7] The guidelines provide for the removal of personal information that is not directly related to CTIs and DMs.

CISA Properly Classified CTIs and DMs

CISA properly classified CTIs and DMs as required by the Act. According to CISA officials, specifically, cyber analysts obtained sections from the original CTIs and DMs, included this information in a new indicator, and marked it with the same classification as the source.[8] CISA classified most CTIs and DMs based on the original classification authority.[9]

CISA Accounted for Security Clearances for Private-Sector Individuals to Receive Classified Information

CISA accurately accounted for the security clearances granted to private-sector individuals to receive classified information. In total, CISA maintained 1,819 active security clearances in CY 2023 and 1,991 in CY 2024, which included 256 and 396 security clearances it granted in 2023 and 2024, respectively.

[7] 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*.

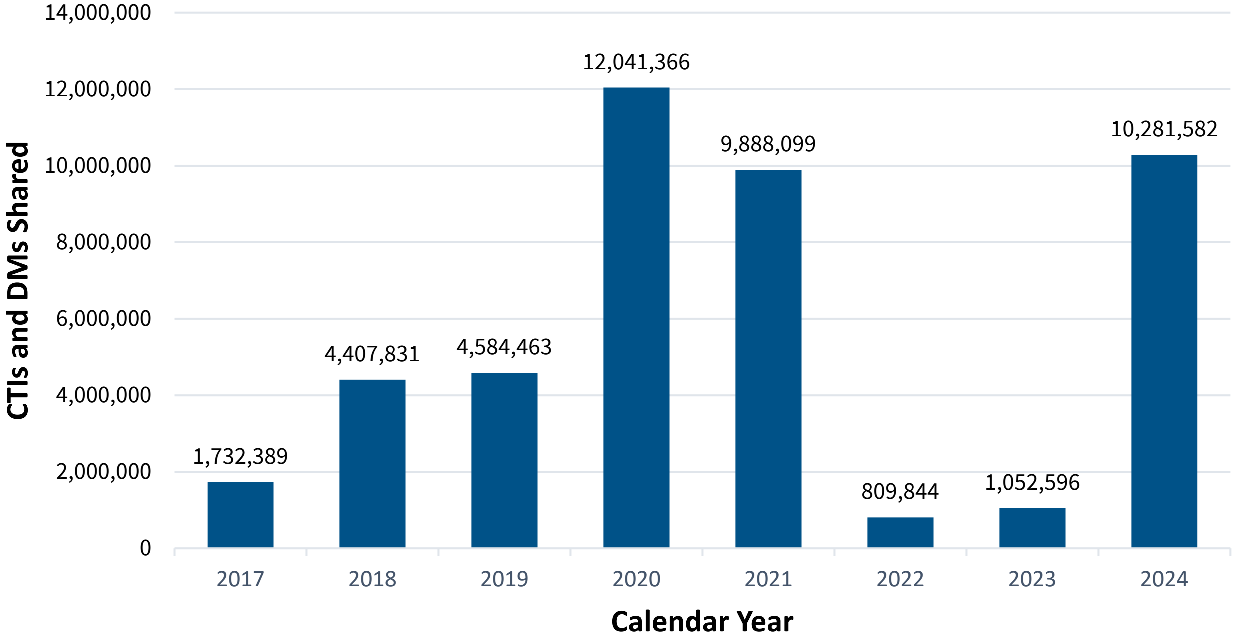
[8] Appendix C, question 11a.

[9] An initial determination that information requires protection against unauthorized disclosure, *Executive Order 13526,* December 29, 2009.

The Number of Indicators Shared via AIS Varied Significantly Each Year due to Overreliance on One Participant

The number of CTIs and DMs shared increased significantly in CY 2024. According to CISA officials, the effectiveness of AIS' capabilities relied on the participation of data producers to share information, including with CISA. The more data producers participate and share information, the more CTIs and DMs are available, leading to an increase in CTIs and DMs shared. From CYs 2023 to 2024, the number of indicators shared increased significantly from approximately 1 million in CY 2023 to more than 10 million in CY 2024 (see Figure 2).

Figure 2. Number of Shared CTIs and DMs, CYs 2017–2024



Source: DHS OIG–created from CISA data on the collection of CTIs and DMs.

Although the number of CTIs and DMs increased in 2024, CISA continues to rely on a small number of partners to share information. CISA officials attributed recent increases in shared CTIs and DMs to a private-sector partner's[10] significant contribution. In 2024, this private-sector partner added more than 4 million CTIs and DMs to each of the Federal and public collections — accounting for 89 percent of the public collection and 83 percent of the Federal collection. In our previous review,[11] we identified a significant decrease in shared CTIs and DMs in 2022 because a

[10] The private-sector partner is a cybersecurity platform that joined AIS in March 2024. As its tenants contribute data, it shares those indicators with AIS.

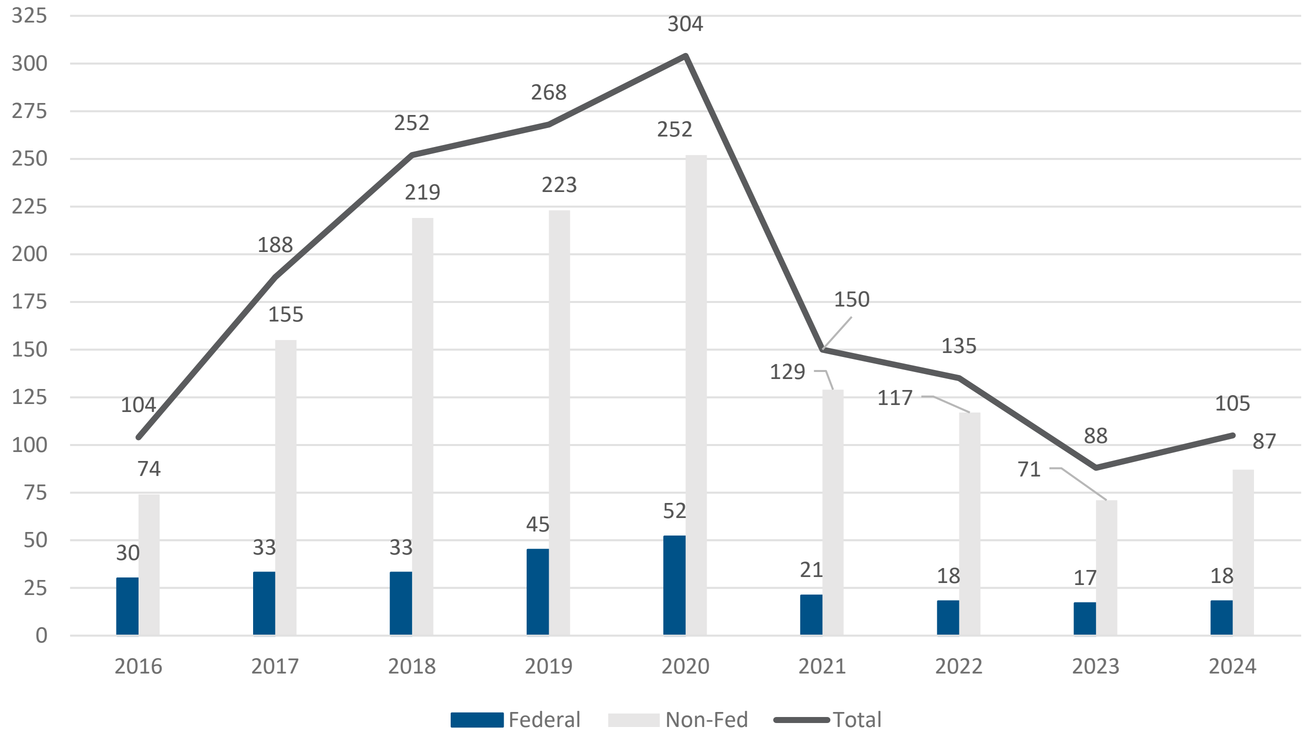
[11] In our previous report, OIG 24-60, we found a major Federal participant stopped sharing CTIs in 2022, decreasing the number of CTIs and DMs shared in the Federal collection by 99 percent.

Federal partner that shared approximately 9 million CTIs and DMs had stopped participating in AIS. CISA's overreliance on information shared by specific participants may lead to inconsistent results and prevent long-term program growth if top contributing partners stop participating.

The Number of AIS Participants Has Declined

The number of AIS participants grew over the first 4 years of the program but has declined since 2020. In 2022, the number of Federal participants decreased from 18 to 17; the number increased back to 18 for 2024. This remains lower than the period of 2017 through 2020, when AIS averaged more than 40 Federal participants. The number of non-Federal AIS participants has fluctuated since the system was created in 2016. The non-Federal participants[12] we interviewed stated that they find AIS useful and an effective tool for protecting their systems from cyber threats. However, the number of non-Federal participants remained lower in 2023 and 2024 than in previous years (see Figure 3). AIS now has 87 non-Federal participants compared to 252 in 2020.

Figure 3. Number of AIS Participants, CYs 2016–2024



Source: DHS OIG–created from CISA data on AIS participants

CISA did not conduct adequate outreach to add AIS participants and reduce reliance on certain partners. At the time of our review, CISA had not completed all corrective actions to address our prior recommendation to develop and implement a strategy to actively recruit and retain AIS

[12] We interviewed and surveyed 10 AIS participants, all from private entities.

participants. In response to this recommendation, in September 2024, CISA began developing the Threat Intelligence Enterprise Services (TIES) strategy to increase recruitment of participants and implement metrics for the quality of information shared on AIS.

According to CISA, AIS will leverage the TIES strategy, targeting specific groups for bidirectional information sharing. This strategy prioritizes focusing on continuing efforts to ensure CTIs and DMs are relevant to participants and engaging with partners that represent critical infrastructure and international cyber defense. AIS program officials said the strategy will improve quality from previous AIS upgrades and foster collaboration between Federal and private-sector entities, enabling analysts to enrich CTIs and DMs.

CISA Has Not Finalized Plans to Continue AIS Use after Act Expiration

CISA has not finalized plans for continued AIS use when Title 1 of the Act expires on September 30, 2025. During our review, CISA program officials could not provide documentation on CISA's plan for continued use of AIS after the Act's expiration. After the completion of our fieldwork, CISA program officials provided us with an outline documenting the upcoming steps for AIS and TIES. However, CISA program officials stated that CISA's senior leadership has yet to approve the outline.

Program officials stated that although CISA continues to be committed to sharing CTIs and DMs in an automated, unclassified machine-readable format such as AIS, the decision on whether to maintain the capability will be based on available resources and leadership's priorities. CISA officials said if the Act were to expire, they would analyze the value of AIS, including the average operational cost of $1 million per month and a likely reduction in CTI and DM volume, to determine whether resources could be redirected from other agency priorities to support AIS. Should CISA continue operating AIS, officials plan to integrate AIS into the TIES exchange platform to expand AIS capabilities beyond traditional indicator sharing. The TIES platform will support integration with other Government systems, such as AIS, other threat intelligence platforms, and commercial threat feeds.

Conclusion

Increased information sharing is essential to protect the Nation's networks and critical infrastructure from cyberattacks. CISA has increased the number of indicators it shared since our last review, increasing the ability to facilitate the sharing of cyber threats in real time. CISA has not determined whether AIS will remain operational beyond September 30, 2025, when the Act expires. Without finalized plans for future AIS use, CISA may not have an automated process for sharing cyber threat information among its partners, including Federal agencies and those responsible for the Nation's critical infrastructure.

Recommendation

Recommendation 1: We recommend the Director of CISA evaluate Automated Indicator Sharing and its associated costs and benefits to determine whether to maintain the system's information-sharing capabilities beyond September 30, 2025.

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 our recommendation. We consider recommendation 1 open and resolved. A summary of CISA's response and our analysis follows.

CISA Comments to Recommendation 1: Concur. Although there are no immediate or near-term plans to discontinue the AIS service, CISA's Cybersecurity Division will continue evaluating AIS and its associated costs and benefits to determine whether to maintain the system's information-sharing capabilities in the long term if Title I of the *Cybersecurity Information Sharing Act of 2015* expires. Once this evaluation is concluded, if the Act is not reauthorized, findings will be presented to CISA leadership for appropriate action. Estimated completion date: June 30, 2026.

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.

Appendix A:
Objective, Scope, and Methodology

Our objective was to determine the extent of DHS' progress in meeting the cybersecurity information-sharing requirements of the *Cybersecurity Information Sharing Act of 2015* for CYs 2023 and 2024.

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

- 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 adequacy 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 CISA. 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 135 AIS participants (25 Federal entities and 110 non-Federal entities) to obtain their perspectives on the effectiveness of the AIS program. Only 10 of the 135 participants (7.4 percent), none of which were Federal entities, provided feedback. We judgmentally selected 17 unclassified CTIs and DMs a year for both 2023 and 2024 (i.e., a total of 34) to determine if they were properly classified. Additionally, we selected 30 classified CTIs and DMs for 2023 to determine if the CTIs and DMs sampled were properly classified; no classified CTIs and DMs were shared in 2024.

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

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.

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 28, 2025

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

FROM: Madhu Gottumukkala, Ph.D.
Acting Director
Cybersecurity Infrastructure and Security Agency

SUBJECT: Management Response to Draft Report: "CISA Has Not Finalized Plans for AIS Beyond the Expiration of the Cybersecurity Act of 2015"
(Project No. 25-010-AUD-CISA)

Thank you for the opportunity to comment on this draft report. The Cybersecurity Infrastructure and 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 made progress to meet the requirements of the Cybersecurity Act of 2015 by updating its guidance for information sharing; properly classifying cyber threat indicators and defensive measures; and accounting for security clearances of private-sector individuals. CISA remains fully committed to advancing its cyber threat information-sharing capabilities.

However, it is important for readers of this report to understand that automated threat intelligence and information sharing with our global partners and stakeholders remains a priority for CISA, and that there are no immediate or near-term plans to discontinue the Automated Information Sharing service, regardless of the status of the Cybersecurity Act of 2015. Subject to available appropriations, CISA remains authorized to operate Automated Information Sharing irrespective of the possible sunset of the Cybersecurity Information Sharing Act of 2015 on September 30, 2025, and CISA will continue to modernize and evolve Automated Information Sharing to meet the needs of its partners and stakeholders.

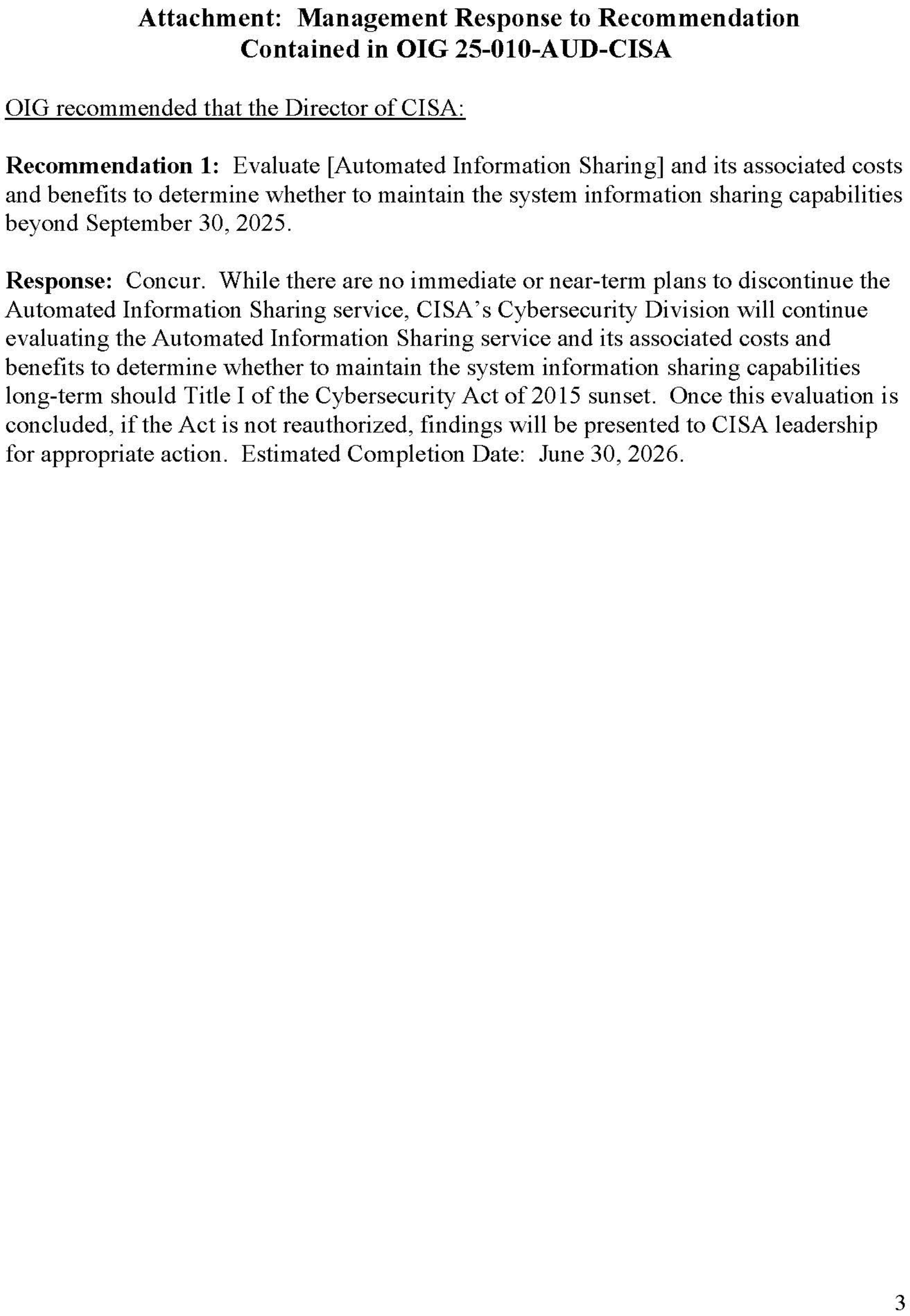
Furthermore, CISA is actively exploring opportunities to evolve and modernize Automated Information Sharing and better integrate the service with other existing systems, including the future-state Threat Intelligence Enterprise Services[1] platform, to enhance the quality, relevance, and timeliness of shared cyber threat indicators. CISA will continue to evaluate Automated Information Sharing to ensure it remains a valuable and effective tool for protecting the Nation's critical infrastructure and networks.

The draft report contained one recommendation with which CISA concurs. Attached find our detailed response to the 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.

Attachment

[1] CISA's Threat Intelligence Enterprise Services is a project to modernize how the agency shares cyber threat information. It aims to simplify, improve, and streamline CISA's customer-facing cyber threat intelligence offerings. TIES will focus on a partner-centered design, ensuring the platform is built with human-centered design principles, and will learn from the challenges of the legacy Automated Indicator Sharing system.



Attachment: Management Response to Recommendation Contained in OIG 25-010-AUD-CISA

OIG recommended that the Director of CISA:

Recommendation 1: Evaluate [Automated Information Sharing] and its associated costs and benefits to determine whether to maintain the system information sharing capabilities beyond September 30, 2025.

Response: Concur. While there are no immediate or near-term plans to discontinue the Automated Information Sharing service, CISA's Cybersecurity Division will continue evaluating the Automated Information Sharing service and its associated costs and benefits to determine whether to maintain the system information sharing capabilities long-term should Title I of the Cybersecurity Act of 2015 sunset. Once this evaluation is concluded, if the Act is not reauthorized, findings will be presented to CISA leadership for appropriate action. Estimated Completion Date: June 30, 2026.

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

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 unclassified cyber threat intelligence available to Federal Government and private partners. CISA does this using an automated system:

- According to officials in DHS' CISA, the AIS service provides participating Federal agencies and non-Federal entities the capability to share unclassified cyber threat information with each other. Participation in the service and any contribution of cyber threat information is completely voluntary.
    - Officials also publish Indicator Bulletins, Malware Analysis Reports, and Cybersecurity Advisories to share information with AIS participants.

For classified sharing, CISA used Enhanced Cybersecurity Services which is an intrusion detection, prevention, and analysis capability. CISA also used Einstein 3 Accelerated, which is a system used to detect cyberattacks targeting Federal Civilian Executive Branch networks and actively prevents potential compromises. Both were decommissioned on December 2023. CISA's Protective Domain Name System replaced Einstein 3 Accelerated service after its decommission. During 2024, CISA did not share classified CTIs and DMs because it deliberately 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.

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

DHS developed or assisted in developing the following four policies and procedures for sharing CTIs:

- *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, The Department of Justice, The Office of the Director of National Intelligence,* February 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,* April 2024.

- *Final Procedures Related to the Receipt of CTIs and DMs by the Federal Government, The Department of Homeland Security, The Department of Justice,* October 2023.

- *Privacy and Civil Liberties Final Guidelines: Cybersecurity Information Sharing Act of 2015, The Department of Homeland Security, The Department of Justice,* April 2025.

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. According to CISA officials, Federal policies[13] require the removal of personal information not directly related to a cybersecurity threat before sharing CTIs. The *Privacy and Civil Liberties Final Guidelines: Cybersecurity Information Sharing Act of 2015* ensures information identifying individuals that are not directly related to a cybersecurity threat is removed from shared indicators, safeguarding privacy and civil liberties.

4. **If the four procedure documents created as a result of the Cybersecurity Information Sharing Act were not provided for question 2, is the agency aware of the documents?**

This question is not applicable to DHS.

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. According to CISA officials, the AIS service aligns with the policies, procedures, and guidelines from question 2 by integrating automated checks for data sanitization, manual reviews, and secure transmission methods.

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

According to CISA officials, this question is not applicable to DHS.

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

[13] *Sharing of CTIs and DMs by the Federal Government under the Cybersecurity Information Sharing Act of 2015, The Department of Homeland Security, The Department of Justice, The Office of the Director of National Intelligence,* February 2016*.*

According to CISA officials, this question is not applicable to DHS.

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 for AIS are sufficient.

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

Yes. According to CISA officials, CISA has shared unclassified CTIs and DMs with non-Federal entities through the AIS service as CISCP packages. CISA has shared machine-readable versions of various CISA-published products (e.g., Indicator Bulletins, Activity Alerts, and Analysis Reports). CISA's implementation of the AIS service allows other Federal agencies to share their unclassified CTIs and DMs with non-Federal entities.

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

Yes. In 2023, through Enhanced Cybersecurity Services program, CISA shared a total of 2,315 classified CTIs and DMs with a small number of critical infrastructure partners. There were no classified CTIs or DMs shared in 2024.

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

According to CISA officials, CTIs and DMs are classified according to their sensitivity, relevance, and potential risks. The process includes reviews by threat analysts, compliance teams, and, when needed, interagency security officers. However, CISA is not the original classifier.

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

The audit team reviewed a sample of 17 unclassified CTIs and DMs for each year (CYs 2023 and 2024) and concluded they were classified correctly. The team sampled 30 classified CTIs and DMs for CY 2023 and concluded they were classified correctly. According to CISA officials, there were no classified CTIs or DMs shared for 2024.

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

Yes. According to CISA officials, CISA's process resulted in proper classification.

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

Yes. According to CISA officials, CISA authorized 256 security clearances in 2023 and 396 security clearances in 2024 to private-sector partners under various DHS information-sharing programs.

12a. If yes, how did the agency account for the number of security clearances and how many security clearances were active in CYs 2023 and 2024?

According to CISA officials, the Department maintains active security clearance information in the Integrated Security Management System. In 2023 and 2024, DHS maintained 1,819 and 1,991 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?

Yes. According to CISA officials, the number of active security clearances is sufficient.

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

Yes. According to CISA officials, CISA uses and disseminates CTIs and DMs on a case-by-case basis. CISA receives ad-hoc threat information and cybersecurity-related documents directly from Federal Civilian Executive Branch stakeholders. The information received from Federal agencies is coordinated and cleared for wider dissemination to the broader Federal Civilian Executive Branch community through information-sharing channels. DMs and CTIs received from other Federal agencies have been used to bolster various CISA products, such as cybersecurity advisories and mitigation guidance. This dissemination process is coordinated through various entities across CISA's Cybersecurity Division and cleared with personnel from the sharing agency to confirm the dissemination guidance, clearance level, and unique agency information used in the CISA publication.

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

According to CISA officials, CISA shares unclassified CTIs and DMs via the AIS program according to the Traffic Light Protocol. According to the AIS Terms of Use, CISA anonymizes the source identities of the indicators. CISA shares all indicators received in AIS on a real-time, machine-to-machine basis.

Officials also stated CISA analysts share Indicator Bulletins by anonymizing source information, which is then turned into machine-readable files, such as Structured Threat Information

Expression, text, Extensible Markup Language, and JavaScript Object Notation that are shared with authorized partners through DHS-approved platforms/portals, such as AIS, Homeland Security Information Network, and Joint Cyber Defense Collaborative. For content disseminated to Federal subscribers, the system adheres to the package marking, and CISA expects Federal clients to honor the marking as well.

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

Yes. According to CISA officials, information received from Federal agencies is used or disseminated further by CISA to better protect the Federal cybersecurity landscape from potential threats.

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

Yes. According to CISA officials, CISA regularly shares CTIs and DMs within DHS, and with the Federal Bureau of Investigation, the National Security Agency, and others through automated and manual mechanisms.

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.

Yes. DHS OIG reviewed a random sample of unclassified CTIs and DMs, 17 for 2023 and 17 for 2024, and determined they were shared timely and adequately.

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

In 2024, CISA reported 18 Federal agencies and 3 DHS components directly connect to AIS to receive CTIs. Federal agencies also receive AIS data indirectly from CISA's Shared Cybersecurity Services program.

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

Yes. According to CISA officials, the Department of Defense Cyber Crime Center, the Department of Energy, and the National Security Agency share information with AIS subscribers. Also, within DHS, U.S. Customs and Border Protection, which is treated as a separate Federal entity in AIS, shared CTIs and DMs.

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

Yes. DHS OIG reviewed a random sample of 17 unclassified CTIs and DMs for 2023 and 17 for 2024 and determined they were shared timely, adequately, and in an appropriate manner.

18. How many CTIs and DMs did entities share with the Department of Homeland Security through the AIS capability in CYs 2023 & 2024? Provide results.

According to CISA officials, the number of CTIs and DMs made available for CYs 2023 and 2024 were as follows:

- For CY 2023:
  - AIS 1.0:[14]
    - Public collection: 17,862
    - Federal collection: 21,418
    - CISCP collection: 2,035
  - AIS 2.0:
    - Public collection: 496,053
    - Federal collection: 503,481
    - CISCP collection: 11,747
- For CY 2024:
  - AIS 2.0:
    - Public collection: 4,955,678
    - Federal collection: 5,319,753
    - CISCP collection: 6,151

19. (For DHS only) How many of those CTIs and DMs reported for question 18 did the Department of Homeland Security share with other Federal entities CYs 2023 & 2024? Provide results.

According to CISA officials, all CTIs and DMs reported in question 18 for CYs 2023 and 2024 were made available to all participating Federal entities.

20. (Agencies other than DHS) How many CTIs and DMs did the Department of Homeland Security relay to the agency via AIS CYs 2023 & 2024?

Not applicable.

[14] According to CISA officials, CISA decommissioned AIS 1.0 in May 2023.

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

Not applicable.

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. According to CISA officials, the AIS service uses an automated PII detection capability that moves any potential PII to a human review process for analysis and remediation, if applicable. CISA's Office of Privacy officials stated that any PII found during the AIS Privacy Oversight Review was directly related to a cybersecurity threat and verified with Mission Engineering after completion of the review.

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. According to CISA officials, there were no individual's privacy and civil liberties were affected due to the agency sharing CTIs and DMs reported.

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

Not applicable; see response to above question.

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

No. According to CISA officials, the agency 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; see response to above question.

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. According to CISA officials, there were no adverse effects on the privacy and civil liberties of U.S. persons due to the activities carried out under this title by the agency.

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

Not applicable; see response to above question.

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. Examples of barriers could include:

Yes. According to CISA officials, barriers continue to include:

- lack of adherence to Federal cyber information-sharing interagency policy recommendations;
- lack of dedicated funding for implementing those interagency policy recommendations;
- lack of organizational resources to support machine-readable indicator sharing;
- lack of widespread commercial vendor support for generating and sharing AIS-compliant STIX[15] files; and
- Federal organizations tend to be reluctant 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, CISA has undertaken efforts, such as automating the ingestion of CTIs and DMs, improving classification protocols, and fostering trust and collaboration among sharing partners to mitigate potential barriers. However, according to CISA officials, there continues to be inconsistent vendor support for the latest STIX and TAXII[16] specifications, which hinders Federal entities from deploying shared indicators 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/services to improve operational collaboration using common-structured, CTI-sharing formats.

[15] STIX is a computing language that enables organizations to share structured cyber threat information.
[16] TAXII is a standard for exchanging structured cyber threat information in a trusted manner for the detection, prevention, and mitigation of cyber threats.

Threat intelligence platform tools are more likely to include sharing capabilities than other limited purpose security sensors like firewalls. 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. According to CISA officials, the AIS service does not receive or share classified CTIs or DMs.

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

According to CISA officials, Federal entities continue to be reluctant to share information into the public collection. Some prefer to share exclusively within the Federal community collection. Others may have policy requirements to share only within their relevant sector among eligible stakeholders, where AIS does not offer a current narrow sector-specific community collection. Some Federal entities expressed reluctance toward dedicating resources to prepare internal CTI and DM knowledge for external consumption. Others state they do not have the maturity to produce unique CTIs and DMs of value to the broader community.

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

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

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

Yes. According to CISA officials, 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.

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

Yes, according to CISA officials, 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 increase adoption of the latest specifications and the number of sharing tools that are interoperable with DHS' capabilities. CISA also continues to engage with Federal and non-Federal entities to encourage sharing and document feedback to introduce future features and capabilities to 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)]

According to CISA officials, CISA sponsored a *STIX 2.1 Best Practice Guide* developed by industry partners and approved and released by the Organization for the Advancement of Structured Information Standards CTI Technical Committee. The guide suggests best practices to use for STIX content, both for some "non-MUST"[17] normative statements and for considerations beyond the specification. CISA regularly analyzes CTIs to identify best practices for threat hunting, DMs, and mitigation strategies. These are shared with Federal and private-sector entities through collaboration programs.

CISA also produces a wide range of cybersecurity advisories, technical guides, and fact sheets to disseminate actionable best practices to Federal agencies, critical infrastructure organizations, and the broader cybersecurity community. These resources incorporate insights from ongoing threat intelligence analysis, operational collaboration, and incident response activities.

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?

According to CISA officials, AIS is a service 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 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

[17] Non-MUST refers to items not essential or absolutely required, but that are considered optional or desirable. The term is often used in the context of requirements or features.

for, or meant to, capture the usefulness or usage of CTIs that have been made available to end users (i.e., CISA analysts).

29. Does the agency receive unclassified cyber threat information from the Intelligence Community Analysis and Signature Tool (ICOAST)? If not, why? (Resources, system incompatibility, lack of information?)

According to CISA officials, CISA's unclassified threat intelligence platform ingests unclassified data into ICOAST for analysts to use operationally. The AIS service does not receive ICOAST data in AIS 2.0 due to using different CTI technologies, which are incompatible.

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

Yes. The biennial review of the *Privacy and Civil Liberties Final Guidelines: Cybersecurity Information Sharing Act of 2015* was completed on April 24, 2025, by DHS and the Department of Justice.

Appendix D:
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

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