OFFICE OF INSPECTOR GENERAL

Additional Progress Needed to Improve Information Sharing under the Cybersecurity Act of 2015

Homeland Security

August 16, 2022

OIG-22-59

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

August 16, 2022

MEMORANDUM FOR: The Honorable Jen Easterly
Director
Cybersecurity and Infrastructure Security Agency

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

JOSEPH V CUFFARI
Digitally signed by JOSEPH V CUFFARI
Date: 2022.08.16 09:40:35 -04'00'

SUBJECT: *Additional Progress Needed to Improve Information Sharing under the Cybersecurity Act of 2015*

Attached for your action is our final report, *Additional Progress Needed to Improve Information Sharing under the Cybersecurity Act of 2015*. We incorporated the formal comments provided by your office.

The report contains four recommendations aimed at improving information sharing under the *Cybersecurity Act of 2015*. Your office concurred with all four recommendations. Based on information provided in your response to the draft report, we consider recommendation 1 open and unresolved. As prescribed by the 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 each 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.

Based on information provided in your response to the draft report, we consider recommendation 4 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. Recommendations 2 and 3 are resolved and closed.

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

Consistent with our responsibility under the *Inspector General Act of 1978, as amended*, we will provide copies or 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 call me with any questions, or your staff may contact Bruce Miller, Deputy Inspector General for Audits, at (202) 981-6000.

Attachment

DHS OIG Highlights

Additional Progress Needed to Improve Information Sharing under the Cybersecurity Act of 2015

August 16, 2022

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. 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 CISA's progress meeting the Cybersecurity Act's requirements for 2019 and 2020.

What We Recommend

We recommend CISA complete system upgrades, hire needed staff, encourage compliance with information sharing agreements and develop a formal reporting process with quality controls.

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) has addressed the basic information sharing requirements of the *Cybersecurity Act of 2015* (Cybersecurity Act) but has made limited progress improving the overall quality of threat information. In 2019 and 2020, CISA continued to leverage its Automated Indicator Sharing (AIS) capability to share cyber threat information between the Federal Government and the private sector. During that time, CISA reportedly increased the number of Federal participants by more than 15 percent and increased the number of non-Federal participants by 13 percent. CISA asserted it increased the overall number of cyber threat indicators it shared and received by more than 162 percent, but it could not validate this number.

The quality of information shared with AIS participants was not always adequate to identify and mitigate cyber threats. According to Federal and private sector entities we interviewed, most of the cyber threat indicators did not contain enough contextual information to help decision makers take action. We attribute this to limited AIS functionality, inadequate staffing, and external factors. We reported on these same challenges in our Cybersecurity Act evaluation for 2017 and 2018.

Deficiencies in the quality of threat information shared among AIS participants may hinder the Federal Government's ability to identify and mitigate potential cyber vulnerabilities and threats.

CISA Response

CISA concurred with all four recommendations. We included a copy of CISA's comments in Appendix B.

Table of Contents

Background 1

Results of Review 4

DHS Addressed Key Cybersecurity Act Requirements and Reportedly Increased the Volume of Threat Information Shared.............................. 5

Cyber Threat Indicators Were Not Adequate to Identify and Mitigate Threats... 8

Recommendations... 11

Management Comments and OIG Analysis 12

Appendixes

Appendix A: Objective, Scope, and Methodology 14
Appendix B: CISA Comments to the Draft Report................................ 16
Appendix C: DHS' Responses to the Office of the Inspector General of the Intelligence Community 19
Appendix D: Major Contributors to This Report 29
Appendix E: Report Distribution 30

Abbreviations

AIS	Automated Indicator Sharing
CISA	Cybersecurity and Infrastructure Security Agency
CISCP	Cyber Information Sharing and Collaboration Program
IC IG	Office of the Inspector General of the Intelligence Community
MISA	Multilateral Information Sharing Agreement
PII	personally identifiable information
STIX	Structured Threat Information eXpression
TAXII	Trusted Automated eXchange of Indicator Information

Background

The American people increasingly depend on digital computing and connectivity for daily conveniences, essential services, and economic prosperity. Services such as electricity, finance, transportation, water, and health care are facilitated electronically, which may introduce vulnerabilities to computer systems and data. The protection of sensitive information from threats and the security of systems that process, store, or transmit information are critical. The 2021 SolarWinds Orion supply chain compromise[1] highlights the continuing need to identify and respond to the unique challenges surrounding information and information systems.

The Department of Homeland Security plays a critical role in protecting the Nation's cyber space, which includes DHS' own computer systems and information, as well as those belonging to other Federal civilian 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. CISA Central is a branch within the Integrated Operations Division that serves as a central hub for situational awareness regarding threats and emerging risks to our Nation's critical infrastructure, whether they are of a cyber, communications, or physical origin.

The *Cybersecurity Act of 2015*[2] (Cybersecurity Act or Act) established 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 Attorney General, with other Federal entities, to develop procedures designed to facilitate sharing of cyber threat indicators. According to the Act, cyber threat indicators are defined as information that describes or identifies various aspects of cybersecurity threats or security vulnerabilities, such as malicious reconnaissance, a security vulnerability, malicious cyber command and control, the actual or potential harm caused by an incident, or any other attribute of a cybersecurity threat, if disclosure is not otherwise prohibited by law.

CISA created an Automated Indicator Sharing (AIS) capability in 2016 to enable the real-time exchange of unclassified cyber threat information and defensive measures 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

[1] *Emergency Directive 21-01-Mitigate SolarWinds Orion Code Compromise,* Cybersecurity and Infrastructure Agency, updated April 15, 2021.
[2] *Cybersecurity Act of 2015,* December 18, 2015.

information sharing. The fundamental concept of the AIS capability is to promote interaction among participants.

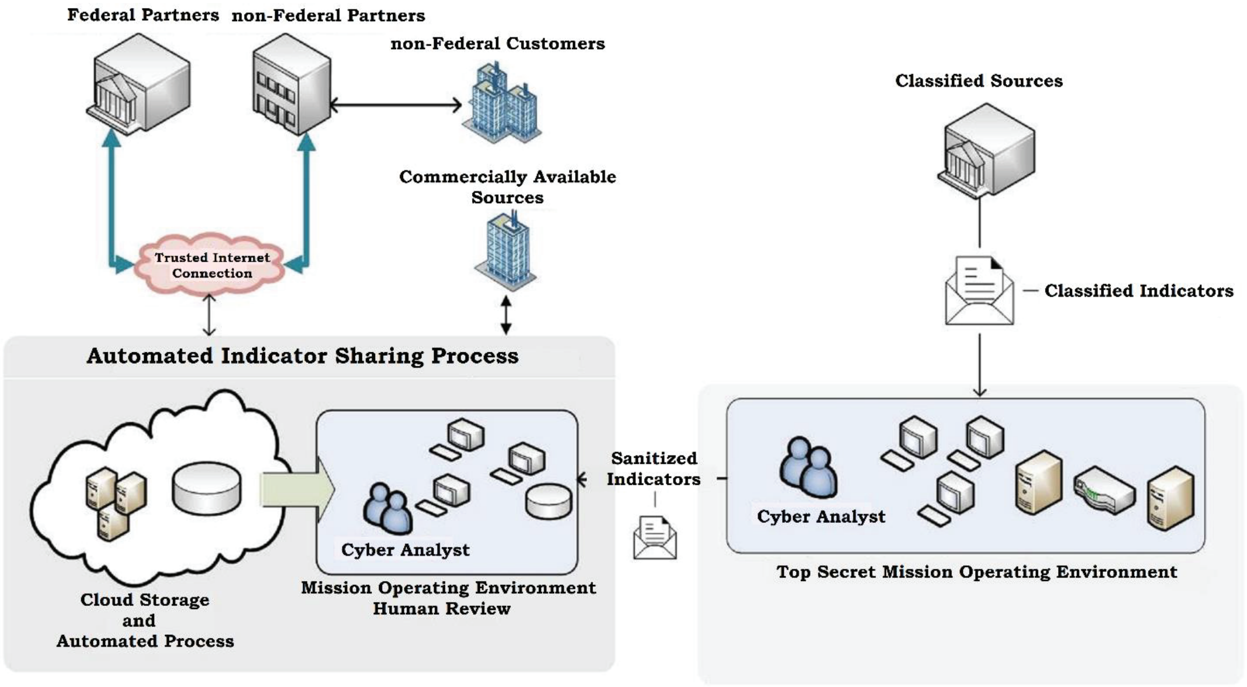
To receive unclassified cybersecurity threat information through the AIS capability, participating entities must first sign an information sharing agreement. CISA offers three separate information sharing categories, or data feeds, to AIS participants: FedGov, AIS, and Cyber Information and Sharing Collaboration Program (CISCP).

- FedGov Feed shares cyber threat information with Federal departments and agencies that have signed the January 2019 Multilateral Information Sharing Agreement (MISA).
- AIS Public Feed is available to all approved AIS participants. Non-Federal entities must have signed the AIS Terms of Use.
- CISCP Feed distributes cyber threat information to non-Federal entities that have signed the Cybersecurity Information Sharing and Collaboration Agreement.

To facilitate the protection of personally identifiable information (PII) within the information sharing process, an automated privacy review flags potential PII within submitted cyber threat indicators and defensive measures that require additional human review. CISA cyber analysts use applications within the unclassified Mission Operating Environment to review and redact PII from submitted cyber threat indicators and defensive measures if not directly related to a cybersecurity threat.

As part of this process, CISA compiles information from classified sources, then removes sensitive or private information before dissemination. Analysts enter declassified cyber threat indicators into Mission Operating Environment workstations. Nonetheless, the background information supporting the now unclassified cyber threat indicators may remain classified. Figure 1 illustrates this process.

Figure 1. AIS Information Sharing Process


Federal Partners
non-Federal Partners
non-Federal Customers
Classified Sources
Commercially Available Sources
Trusted Internet Connection
Classified Indicators
Automated Indicator Sharing Process
Sanitized Indicators
Cyber Analyst
Cyber Analyst
Cloud Storage and Automated Process
Mission Operating Environment Human Review
Top Secret Mission Operating Environment

Source: DHS Office of Inspector General-generated based on information received from CISA

In addition, entities can also share and receive AIS cyber threat indicators and defensive measures outside of AIS. This can be done through a participating Information Sharing and Analysis Center or Information Sharing and Analysis Organization or via an AIS-integrated commercial product or service.

Cybersecurity Act Reporting Requirements

Section 107 of the Act requires a biennial joint report from participating OIGs to include an overall assessment of:

- the policies, procedures, and guidelines to share cyber threat indicators within the Federal Government, including removing personal information that is not directly related to cyber threat indicators;
- whether cyber threat indicators or defensive measures 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 cyber threat indicators or defensive measures shared within the Federal Government; and
- any barriers to sharing cyber threat indicators or defensive measures among Federal agencies.

According to the Office of the Inspector General of the Intelligence Community (IC IG) reporting instruction, each OIG of the selected agencies is required to submit responses to 30 questions on the actions the agency has taken to implement the Act. In accordance with this requirement, we previously assessed DHS' progress implementing the cybersecurity information sharing requirements for 2017 and 2018. We reported in 2020[3] that DHS had addressed the basic information sharing requirements of the Act. We determined CISA had increased the number of AIS participants and cyber threat indicators shared during that time but concluded that the quality of information shared was not effective in reducing cyber threats and protecting against attacks. We recommended that CISA improve information quality by increasing participants' sharing of cyber information, completing system upgrades, and hiring the staff needed to enhance program training and outreach.

We conducted this review to evaluate CISA's progress meeting Cybersecurity Act requirements for 2019 and 2020. At the time of our review, three recommendations from our prior report remained open.

Results of Review

CISA has addressed the basic information sharing requirements of the *Cybersecurity Act of 2015* but has made limited progress improving the overall quality of threat information. In 2019 and 2020, CISA continued to leverage its AIS capability to share cyber threat information between the Federal Government and the private sector. During that time, CISA reportedly increased the number of Federal participants by more than 15 percent and increased the number of non-Federal participants by 13 percent. CISA asserted it increased the overall number of cyber threat indicators it shared and received by more than 162 percent, but it could not validate this number.

The quality of information shared with AIS participants was not always adequate to identify and mitigate cyber threats. According to Federal and private sector entities we interviewed, most of the cyber threat indicators did not contain enough contextual information to help decision makers take action. We attributed this to limited AIS functionality, inadequate staffing, and external factors. We reported on these same challenges in our Cybersecurity Act evaluation for 2017 and 2018.

Deficiencies in the quality of threat information shared among AIS participants may hinder the Federal Government's ability to identify and mitigate potential cyber vulnerabilities and threats.

[3] *DHS Made Limited Progress to Improve Information Sharing under the Cybersecurity Act in Calendar Years 2017 and 2018,* OIG-20-74, September 25, 2020.

DHS Addressed Key Cybersecurity Act Requirements and Reportedly Increased the Volume of Threat Information Shared

DHS has addressed the key requirements of Title I[4] of the Cybersecurity Act to facilitate information sharing, including via the AIS capability, between Federal and private entities. Specifically, the Act requires CISA to (1) develop and update policies and procedures needed for sharing cyber threat indicators and defensive measures with Federal and private entities, (2) classify cyber threat indicators and defensive measures, and (3) account for the security clearances of private sector users authorized to receive this information. CISA has taken the following steps to meet these requirements:

Information Sharing Policies and Guidance

CISA updated guidance as appropriate in accordance with the Act. For example, in October 2020, CISA and the Department of Justice updated the *Guidance to Assist Non-Federal Entities to Share Cyber Threat Indicators and Defensive Measures with Federal Entities under the Cybersecurity Information Sharing Act of 2015*. This guidance assists non-Federal entities with sharing cyber threat indicators and defensive measures with Federal entities.

CISA and the Department of Justice also updated the *Privacy and Civil Liberties Final Guidelines: Cybersecurity Information Sharing Act of 2015* in January 2021. This document establishes privacy and civil liberties guidelines governing the receipt, retention, use, and dissemination of cyber threat indicators and defensive measures by a Federal entity. However, this update was completed 1 month beyond the required time, as the Act[5] required the update to be completed during 2019 and 2020.

Classification of Cyber Threat Indicators and Defensive Measures

CISA properly classified cyber threat indicators and defensive measures as required by the Act. Specifically, cyber analysts used derivative classification for cyber threat indicators and defensive measures. After reviewing 30 unclassified and 30 classified indicators for both 2019 and 2020 that were judgmentally selected, we determined that the indicators sampled were properly classified. Additionally, we determined that they were received and shared timely, adequately, and appropriately.

CISA classified most cyber threat indicators based on the original classification authority. For example, CISA shared 1,347 classified cyber threat indicators

[4] Title I – *Cybersecurity Information Sharing*, which may also be cited as the *Cybersecurity Information Sharing Act of 2015*.

[5] Section 103 of the Cybersecurity Act requires an updated *Privacy and Civil Liberties Guidelines: Cybersecurity Information Sharing Act of 2015* to be completed during 2019 and 2020.

with non-Federal entities in 2019, and 13,163 in 2020. This was done 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.[6]

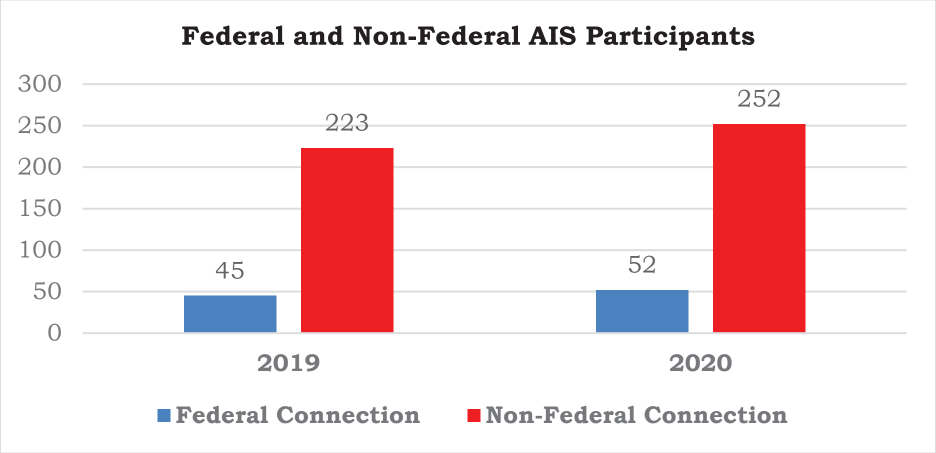
Security Clearances for Private Sector to Receive Classified Information

CISA accurately accounted for the security clearances of private sector individuals authorized to receive classified information. Under various information sharing programs, the Department granted more than 200 security clearances to private sector partners in both 2019 and 2020. In total, CISA maintained 1,845 active security clearances in 2019 and 1,906 in 2020. However, CISA does not track clearances granted under the Act, as the AIS capability only deals with unclassified information.

CISA Increased AIS Participants and Quantity of Information Shared and Received

CISA has continued to increase the number of AIS participants and the volume of cyber threat indicators shared since the capability's inception in 2016. Specifically, CISA increased the number of Federal participants by more than 15 percent and increased the number of non-Federal participants by 13 percent, as shown in Figure 2.

Figure 2. Federal and Non-Federal AIS Participants in 2019 and 2020



Source: DHS OIG-generated based on CISA-reported numbers

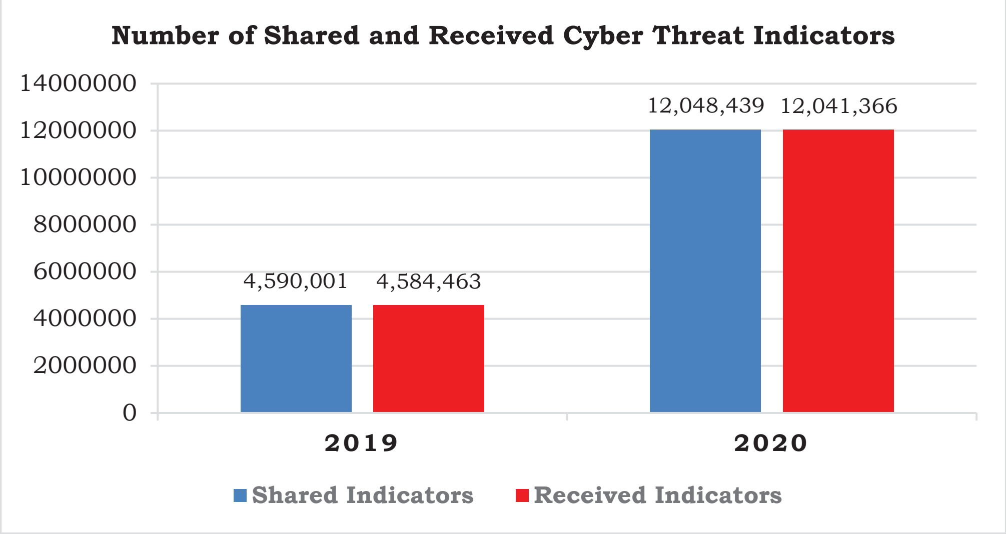
At the time of this review, DHS directly shared cyber threat information with more than 300 AIS partners. Of these, 52 were Federal departments and agencies that connect directly to AIS to receive cyber threat and defensive measure information. Additionally, DHS shares indirectly with Federal

[6] 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.

agencies and non-Federal agencies through third-party aggregators that provide a shared service connection.

During this same period, CISA reportedly increased the annual number of cyber threat indicators it shared with and received from AIS participants. Officials stated CISA increased the overall number of cyber threat indicators it shared and received by more than 162 percent, as shown in Figure 3.

Figure 3. Shared and Received Cyber Threat Indicators in 2019 and 2020



Source: DHS OIG-generated based on CISA-reported numbers

CISA attributed the increase in cyber threat indicators to outreach efforts conducted by its Quality Services Management Office. According to officials, the outreach enabled CISA to collaborate with other agencies on cyber threat information sharing goals, objectives, and standards, and to reduce information sharing challenges and barriers. In addition, CISA established the Critical Infrastructure Partnership Advisory Council on Cyber Threat Information Sharing Working Group, which helped to facilitate and engage in similar cyber threat discussions with the private sector and state and local stakeholders.

Although officials stated CISA had increased the annual number of shared and received AIS threat indicators by more than 162 percent, we could not validate the accuracy of this number. When asked to confirm the number of cyber threat indicators, CISA faced two key challenges:

(1) CISA staff did not have direct access to the indicator databases. CISA previously used a dashboard mechanism to pull such reports, but it was terminated in 2018 due to staff shortages in the AIS project management office. At the time of this review, CISA could only produce the total number of cyber threat indicators by making a request for contract support to query the system. We attempted to

recreate the data flows to validate the reported number of cyber threat indicators shared in 2019 or 2020. However, we could not trace the reported numbers back to source documents or reporting features of the various databases because we received contradictory and incomplete documentation.

(2) Officials stated the AIS capability did not have functionality to confirm the distinct number of threat indicators shared. During an initial technical demonstration, CISA staff presented two system diagrams that each showed different data flows for its archival AIS database. One diagram showed data flowing into and back out of its archival AIS database, while the other diagram showed data only going into their archival AIS database. We were not able to validate the proper data flow during this review.

Cyber Threat Indicators Were Not Adequate to Identify and Mitigate Threats

Although CISA generally increased the number of AIS participants and number of cyber threat indicators shared and received, the quality of the cyber threat indicators was not adequate for participants to take necessary actions. Limited AIS functionality, inadequate staffing, and external factors affected information quality.

Information Not Consistently Actionable

The central purpose of the Act is to share cyber threat information between the public and private sector entities to mitigate threats. Cyber threat information must contain enough contextual information to help decision makers take necessary and appropriate actions. Examples of contextual information may include Internet Protocol addresses, domain names, hash files, uniform resource locators, or anomalies in the network traffic. Real-time access to the right information is critical for mitigating risks. For example, recent sharing of cyber threat indicators, including malware information, related to the 2021 SolarWinds Orion supply chain compromise led CISA and the Department of Defense Cyber National Mission Force to analyze these malware variants and trace their origins to prevent future cyber incidents.

However, AIS participants we spoke with generally stated the cyber threat information was not consistently useful or actionable. To determine whether CISA had improved the quality of information it shared under the AIS capability, we obtained feedback from eight AIS participant entities.[7] According to Federal and private sector entities we interviewed, most of the cyber threat

[7] We met with three Federal entities and five non-Federal entities.

indicators did not contain enough contextual information to help decision makers take actions.

Stakeholders also stated that the cyber threat indicators contained false positives, which could mislead entities into believing threats were malicious, resulting in unnecessary upgrades or security protocols. Federal agency officials also noted that some participants had shared unconfirmed malware cyber threat indicator information, or low confidence threat information, that resulted in false positive alerting within security tools. Additionally, private sector feedback identified concerns with AIS customers experiencing false positives from the AIS Public Feed that were later identified as known good indicators. CISA responded to this by improving the AIS "allow list" to ensure that these types of known good indicators are not distributed via AIS to stakeholders. Federal stakeholders can filter out some of these lower confidence indicators while others may not have the expertise or intermediate tools to further refine relevant cyber threat indicators and defensive measures.

Similarly, the IC IG reported[8] quality issues with AIS because it provided raw information that was not vetted. Specifically, much of the cyber threat information received through AIS did not contain any context as to why the indicator was bad or whether it was still relevant. Consequently, most cyber threat indicators and defensive measures would require more detailed information to be usable.

Multiple Factors Impacted the Quality of Information CISA Shares

We attribute CISA's lack of progress to improve the quality of the information shared under the AIS capability to multiple factors — limited functionality in AIS, insufficient staffing, and other external factors. Collectively, these shortcomings hindered CISA's ability to improve the quality of cyber threat indicators and have thwarted efforts to increase participation and the usefulness of the AIS capability.

(1) Limited AIS Functionality

AIS contains a limited number of fields and attributes that can be used by participants sharing cyber threat information. Although AIS contains additional fields, some fields that would provide more contextual information for each cyber threat indicator were restricted or not required at the time of this audit.

CISA planned to address these limitations by upgrading AIS to version 2.0. According to CISA officials, AIS 2.0 introduces support for the latest cyber threat indicators and defensive measures sharing standards, which increase

[8] IC IG, *Joint Report on the Implementation of the Cybersecurity Information Sharing Act of 2015*, AUD-2021-002, December 9, 2021.

interoperability with more security tools enabling automated network defense. This upgrade will provide new contextual fields, an improved confidence score attribute, and an option for entities to state whether an indicator may be malicious.[9] On March 1, 2022, subsequent to our fieldwork, CISA completed its operational testing of AIS 2.0 features and functionality. According to CISA, it deployed AIS 2.0 in March 2022 to participants that would serve as early adopters of the upgraded capability.

(2) Insufficient Staffing

DHS leadership has not funded or dedicated an adequate number of full-time employees to this effort. For example, DHS has not retained or hired administrative and operational staff needed to conduct the strategic planning, coordination, analysis, and performance measurement needed to mitigate cybersecurity risks. Rather, DHS reduced the number of staff in support of AIS, as two contractor positions were terminated in August 2021 due to loss of funding. We noted in our last review, conducted in 2019, that insufficient staffing also hindered CISA's support efforts for AIS at that time.

(3) External Factors Impacted Information Quality and Sharing

CISA relies on participation from stakeholders to share cyber threat indicators and defensive measures, thereby improving the value of cyber threat information. However, some Federal entities are not adhering to using access control specification markings to identify shared cyber threat indicators (i.e., original source, last activity occurrence, and threat characteristics). CISA provides guidance on sharing cyber threat indicators and defensive measures with Federal and non-Federal entities. These markings are agreed upon in interagency policy recommendations for cyber information sharing documented in the MISA. However, a Federal agency indicated that CISA did not promptly confirm the adequacy of reported indicators or their potential impact.

Also, smaller Federal agencies and private sector companies do not have internal staff and resources to share cyber threat indicators. As a result, these agencies are not able to complete the additional automated workflows required to generate and transmit machine-to-machine information sharing. They can produce reports disseminated via email, but the technical barriers to convert this information into AIS open standard format remain high.

Lastly, some Federal entities stated they were reluctant to share information. Some Federal entity representatives expressed concerns regarding distribution of information outside of certain "communities." For

[9] AIS participants can apply automated or manual triage against the populated opinion value to identify indicator objects meeting or exceeding designated criteria and filter the remaining data.

example, some Federal entities were open to sharing with the private sector but were concerned about sharing with the international community. Both the AIS Public Feed and the CISCP Feed have some level of participation by the international community.

We reported on these same challenges during our prior Cybersecurity Act evaluation for 2017 and 2018.[10] During that timeframe, CISA had increased the number of AIS participants and cyber threat indicators, but the quality of information shared was not adequate for decision makers to mitigate and protect against attacks. We made four recommendations for CISA: improve information quality by increasing participants' sharing of cyber information, complete AIS upgrades, conduct additional training and outreach, and hire the staff needed to improve the AIS program's operational effectiveness.

To address our recommendations, CISA collaborated with the Organization for the Advancement of Structured Information Standards to expedite the approval of new standards so they could complete AIS upgrades. Therefore, this recommendation was closed in March 2022. CISA has taken steps to address the remaining three recommendations by increasing outreach for AIS through working groups, updating a public-facing website in January 2022 for AIS promotion, and acquiring temporary contractual support for AIS. Each of these recommendations remained open at the time of this review.

Conclusion

Without quality controls in place to address data reliability and reporting concerns, the data submitted through AIS may result in CISA reporting inaccurate AIS cyber threat indicators and defensive measures. More importantly, deficient information sharing among the AIS participants hinders the Department's ability to protect the Nation's networks and critical infrastructure from potential vulnerabilities and threats. Unvetted shared indicators, without appropriate context, can cause participants to take incorrect actions, such as blocking acceptable or non-malicious threats and Internet protocol addresses, which subsequently lowers the confidence level of the information provided.

Recommendations

We are administratively closing the recommendations from our prior report to issue the following new recommendations:

Recommendation 1: We recommend the Director of CISA develop and implement a formal process to verify the number of cyber threat indicators and

[10] *DHS Made Limited Progress to Improve Information Sharing under the Cybersecurity Act in Calendar Years 2017 and 2018,* OIG-20-74, September 25, 2020.

defensive measures shared through CISA's Automated Indicator Sharing capabilities to enable accurate reporting and oversight.

Recommendation 2: We recommend the Director of CISA develop and implement an approach to encourage Federal agencies and the private sector to comply with information sharing agreements and requirements, and report actions taken with information sharing agreements and requirements for Automated Indicator Sharing.

Recommendation 3: We recommend the Director of CISA complete Automated Indicator Sharing 2.0 upgrades.

Recommendation 4: We recommend the Director of CISA place priority on hiring administrative and operational staffing to conduct the strategic planning, coordination, analysis, and performance measurement needed to mitigate cybersecurity risks.

CISA Management Comments and OIG Analysis

We obtained written comments from CISA on a draft of this report. In its comments, CISA indicated it appreciated our work in planning, conducting our review, and issuing this report. CISA will continue to ensure that cyber threat indicators are shared through the real-time process according to 6 United States Code 1504(a)(3)(B).

We have reviewed CISA's comments, as well as the technical comments previously submitted under separate cover, and updated the report as appropriate. One recommendation is open and unresolved, one recommendation is open and resolved, and two recommendations are closed and resolved. A summary of the CISA's responses and our analysis follows.

DHS Response to Recommendation #1: Concur. CISA's Cybersecurity Division launched its next generation version of AIS, AIS 2.0, which created the capability to apply a CISA opinion score to cyber threat indicators. This score provides an assessment of whether the information can be corroborated with other sources available to the entity submitting the opinion to AIS. CISA publicly shared information on the opinion score methodology in the November 2021 document, *Automated Indicator Sharing (AIS) Scoring Framework Used for Indicator Enrichment*, V1.0.

OIG Analysis: CISA's actions are not responsive to this recommendation. The *Automated Indicator Sharing (AIS) Scoring Framework Used for Indicator Enrichment*, V1.0 emphasizes enriching cyber threat indicator information so that decision makers can prioritize actions and investigate indicator objects. Additionally, the document did not include any reporting or oversight capability requirements. This recommendation is open and unresolved until CISA provides documentation showing the total numbers of cyber threat indicators and defensive measures for a reporting period in support of its oversight of the AIS program.

DHS Response to Recommendation #2: Concur. CISA's Cybersecurity Division issued its *Automated Indicator Sharing (AIS) 2.0 Submission Guide*, V1.0, which was intended to increase participation in advance of the March 1, 2022, launch of AIS 2.0. Further, the submission guide can be used with the *Automated Indicator Sharing (AIS) Profile: Requirements for STIX Submissions* V1.0 document to help AIS participants understand all requirements for AIS submissions.

OIG Analysis: CISA's actions are responsive to this recommendation, after review of the *Automated Indicator Sharing (AIS) 2.0 Submission Guide*, V1.0 and the *Automated Indicator Sharing (AIS) Profile: Requirements for STIX Submissions* V1.0, we consider this recommendation closed and resolved.

DHS Response to Recommendation #3: Concur. CISA's Cybersecurity Division completed upgrades on March 1, 2022, for AIS to leverage the latest Structured Threat Information eXpression (STIX)/ Trusted Automated eXchange of Indicator Information (TAXII) 2.0 standards for capturing and communicating cyber threat intelligence. Further, on June 2, 2022, CISA demonstrated the AIS 2.0 operational capabilities for us to show that the requirements of this recommendation were met.

OIG Analysis: CISA's actions are responsive to this recommendation, after two demonstrations to the OIG showing the upgrade to AIS 2.0 and its new operational capabilities. Additionally, the *Automated Indicator Sharing (AIS) Scoring Framework Used for Indicator Enrichment*, V1.0, the supported documentation for recommendation 1, should increase the quality of information of cyber threat indicators and defensive measures. We consider this recommendation closed and resolved.

DHS Response to Recommendation #4: Concur. During the past 18 months, CISA's Cybersecurity Division has added additional contractual resources to better support these efforts and is also assessing a longer-term approach to allocate resources to fully support this critical mission area. Estimated Completion Date: January 31, 2023.

OIG Analysis: CISA's actions are responsive to this recommendation, which will remain open and resolved until CISA provides a hiring plan and a long-term approach to address strategic planning, coordination, analysis, and performance measurement needed to mitigate cybersecurity risks.

Appendix A
Objective, Scope, and Methodology

The Department of Homeland Security Office of Inspector General was established by the *Homeland Security Act of 2002* (Public Law 107−296) by amendment to the *Inspector General Act of 1978*.

Our objective was to determine to what extent DHS is making progress meeting cybersecurity information sharing requirements, pursuant to Section 107 of the *Cybersecurity Act of 2015* for 2019 and 2020.

To answer our objective, we sought to determine whether DHS had developed additional policies and procedures since our last review. The team analyzed the information-sharing mechanisms and methodology used by DHS components to receive and share cyber threat indicators and defensive measures and remove unrelated personal information.

To evaluate the progress DHS made since our last review, we determined whether DHS and its components had:

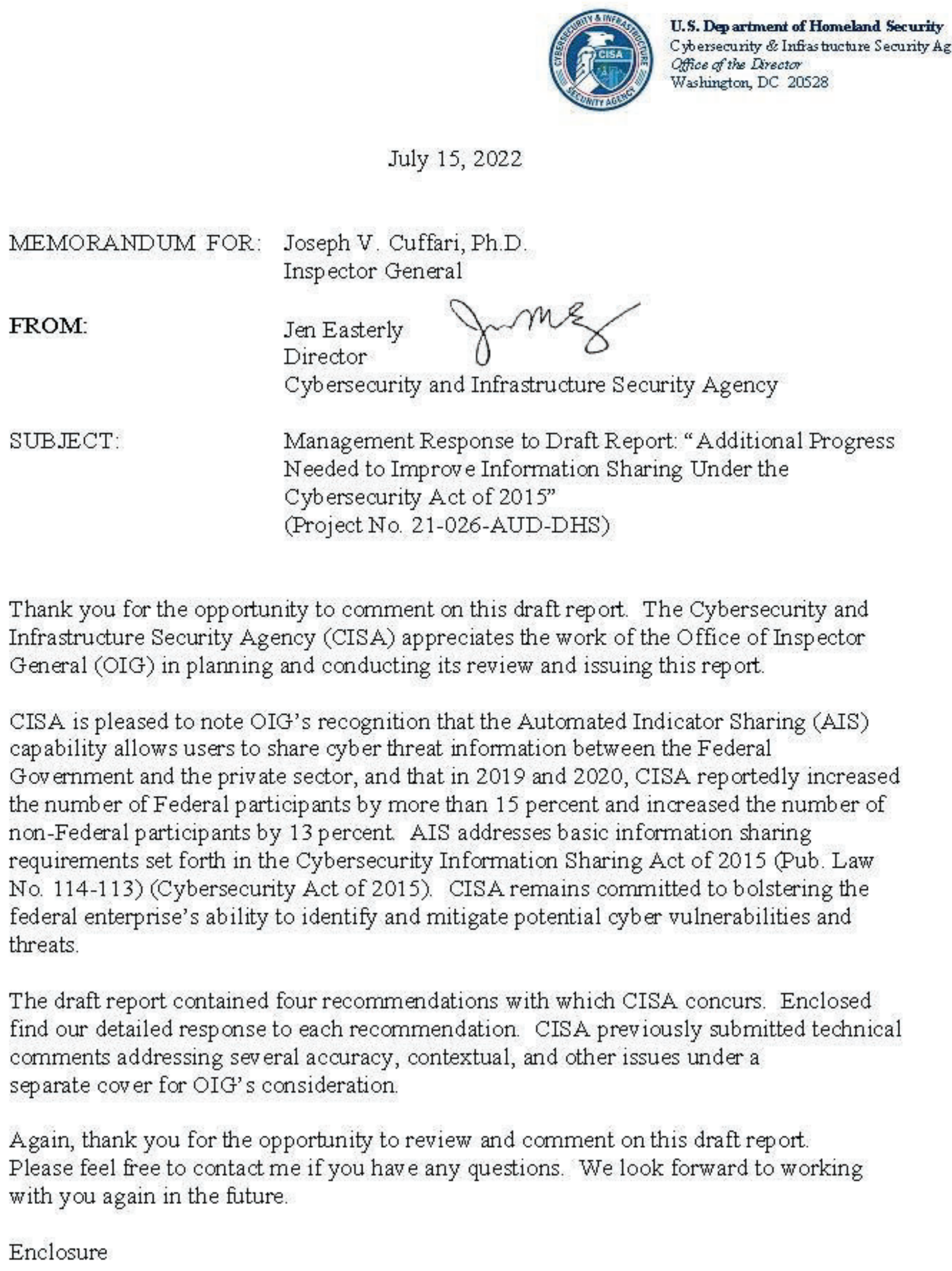
- revised existing policies and procedures or issued additional guidance to improve the sharing of cyber threat indicators and defensive measures within the Federal Government;
- properly classified cyber threat indicators or defensive measures and authorized the number of security clearances needed by the Federal Government for sharing cyber threat indicators or defensive measures with the private sector;
- taken actions along with other Federal agencies based on the cyber threat indicators or defensive measures shared under this Act. These actions included whether the cyber threat indicators or defensive measures were shared timely and adequately with appropriate entities or, if appropriate, were made publicly available; and
- determined whether all identified instances of significant internal control deficiencies, fraud, illegal acts, or violations of regulatory requirements are immediately reported to the appropriate management officials and investigative staff, if appropriate.

We interviewed selected DHS and component management and staff, as well as three Federal entities: Department of Energy, Department of Commerce, Department of Education, and five non-Federal entities. We conducted a survey to solicit feedback regarding AIS, and we received feedback from four non-Federal entities. We also reviewed applicable policies, procedures, and guidelines. We judgmentally selected 30 unclassified and 30 classified indicators for both 2019 and 2020 and determined that the indicators sampled were properly classified.

We sought to assess the reliability of AIS' data accuracy and to quantify the number of threat indicators reported as part of our review. We used the work of specialists in our Office of the Chief Data Officer as part of this review. Specifically, we used Data Analytics Specialists to assist with validating the number of cyber threat indicators and defensive measures entities shared with CISA through AIS. To do this, we requested technical demonstrations of AIS' relevant systems and underlying database structures, system and database documentation, and data extracts or database backups. Ultimately, we determined that the total number of participants that share and receive cyber threat indicators increased, but we could not validate the exact number of cyber threat indicators reported.

We conducted this review between March 2021 and January 2022 pursuant to the *Inspector General Act of 1978*, *as amended*, and according to the *Quality Standards for Inspection and Evaluation* issued by the Council of the Inspectors General on Integrity and Efficiency.

Appendix B
CISA Comments to the Draft Report



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

July 15, 2022

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

FROM: Jen Easterly
Director
Cybersecurity and Infrastructure Security Agency

SUBJECT: Management Response to Draft Report: "Additional Progress Needed to Improve Information Sharing Under the Cybersecurity Act of 2015"
(Project No. 21-026-AUD-DHS)

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 is pleased to note OIG's recognition that the Automated Indicator Sharing (AIS) capability allows users to share cyber threat information between the Federal Government and the private sector, and that in 2019 and 2020, CISA reportedly increased the number of Federal participants by more than 15 percent and increased the number of non-Federal participants by 13 percent. AIS addresses basic information sharing requirements set forth in the Cybersecurity Information Sharing Act of 2015 (Pub. Law No. 114-113) (Cybersecurity Act of 2015). CISA remains committed to bolstering the federal enterprise's ability to identify and mitigate potential cyber vulnerabilities and threats.

The draft report contained four 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.

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

Enclosure: Management Response to Recommendations Contained in 21-026-AUD-DHS

OIG recommended that the Director of CISA:

Recommendation 1: We recommend the Director of CISA develop and implement a formal process to verify the number of cyber threat indicators shared through its Automated Indicator Sharing capability to enable accurate reporting and oversight.

Response: Concur. On March 1, 2022, CISA's Cybersecurity Division launched its next generation version of AIS, "AIS 2.0," which, among other actions, created the capability to apply a CISA "opinion score" to Cyber Threat Indicators (CTI) in AIS.

This opinion score provides an assessment of whether or not the information can be corroborated with other sources available to the entity submitting the opinion to AIS. CISA publicly shares information on the opinion score methodology in the November 2021 document, "Automated Indicator Sharing (AIS) Scoring Framework Used for indicator Enrichment," V1.0. [1] This scoring can help those receiving information from AIS make informed decision in support of cyber defense.

CISA requests that the OIG consider this recommendation resolved and closed, as implemented.

Recommendation 2: Develop and implement an approach to encourage Federal agencies and the private sector to comply with information sharing agreements and requirements, and report actions taken with information sharing agreements and requirements for Automated Indicator Sharing.

Response: Concur. In November 2021, CISA's Cybersecurity Division issued its "Automated Indicator Sharing (AIS) 2.0 Submission Guide, V1.0,"[2] which was intended to increase effective sharing participation in advance of the March 1, 2022, launch of AIS 2.0 by providing guidance for AIS participants when submitting Structured Threat Information Expression (STIX) format via the Trusted Automated Exchange of Intelligence Information (TAXII). Further, the AIS 2.0 Submission Guidance V1.0 can

[1] "Automated Indicator Sharing (AIS) Scoring Framework Used for Indicator Enrichment," V1.0, November 2021 -- https://www.cisa.gov/sites/default/files/publications/AIS%20Scoring%20Framework%20Used%20for%20Indicator%20Enrichment%20V1.0_508.pdf

[2] "Automated Indicator Sharing (AIS) 2.0 Submission Guide," V1.0, November 2021 -- https://www.cisa.gov/sites/default/files/publications/AIS%202.0%20Submission%20Guide%20V1.0_508.pdf

be utilized with the AIS 2.0 Profile V1.0[3] document to help AIS participants understand all requirements for AIS submissions.

CISA requests that the OIG consider this recommendation resolved and closed, as implemented.

Recommendation 3: Complete Automated Indicator Sharing 2.0 upgrades.

Response: Concur. CISA's Cybersecurity Division completed upgrades on March 1, 2022, for AIS to leverage the latest STIX/TAXII 2.0 standards for capturing and communicating cyber threat intelligence. Furthermore, on June 2, 2022, CISA demonstrated the AIS 2.0 operational capabilities to DHS OIG to show that the requirements of this recommendation were met.

CISA requests that the OIG consider this recommendation resolved and closed, as implemented.

Recommendation 4: Place priority on hiring administrative and operational staffing to conduct the strategic planning, coordination, analysis, and performance measurement needed to mitigate cybersecurity risks.

Response: Concur. Over the past 18 months, CISA's Cybersecurity Division has added additional contractual resources to better support these efforts, and are also in the process of assessing a longer-term approach to allocate resources to fully support this critical mission area. Estimated Completion Date: January 31, 2023.

[3] "Automated Indicator Sharing (AIS) Profile: Requirements for STIX Submissions," V1.0, October 2021 -- https://www.cisa.gov/sites/default/files/publications/AIS%202.0%20Profile%20V1.0_508.pdf

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

Policies, Procedures, and Guidelines

1. What is the agency's process for sharing cyber threat indicators within the Federal Government?

First, the Department shares unclassified cyber threat indicators and defensive measures through three data feeds:

1. AIS Public Feed: This feed is available to all approved AIS participants. Non-Federal entities must have signed the AIS Terms of Use.
2. CISCP Feed: This feed distributes cyber threat information to Non-Federal entities that have signed the Cybersecurity Information Sharing and Collaboration Agreement.
3. FEDGOV Feed: This feed shares cyber threat information with Federal departments and agencies that have signed the January 2019 MISA.

Second, DHS shares classified cyber threat indicators through the Enhanced Cybersecurity Services and EINSTEIN 3 Accelerated Programs. Enhanced Cybersecurity Services is an intrusion detection, prevention, and analysis capability, while EINSTEIN 3 Accelerated is a system used to detect cyberattacks targeting Federal Civilian Executive Branch networks and actively prevents potential compromises.

2. What are the agency's policies, procedures, and guidelines for sharing cyber threat indicators within the Federal Government? (Please provide them to the IC IG.)

DHS developed or assisted in the development of the following policies and procedures:

- *Sharing of Cyber Threat Indicators and Defensive Measures by the Federal Government under the Cybersecurity Information Sharing Act of 2015* – February 2016
- *Guidance to Assist Non-Federal Entities to Share Cyber Threat Indicators and Defensive Measures with Federal Entities under the Cybersecurity Information Sharing Act of 2015* – October 2020
- *Final Procedures Related to the Receipt of Cyber Threat Indicators and Defensive Measures by the Federal Government* – June 2016
- *Privacy and Civil Liberties Final Guidelines: Cybersecurity Information Sharing Act of 2015* – June 2018

- *Automated Indicator Sharing (AIS) Brokering Between the Non-Federal Entities Sharing Community and the Federal Entities Sharing Community* – July 2016
- *Cybersecurity Information Handling Guidelines* – October 2018

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. The Automated Indicator Sharing Terms of Use directs that each AIS Producer will use reasonable efforts to remove any indicators or defensive measures that are not directly related to a cybersecurity threat provided to CISA Central. Specifically, the AIS Producer should remove any information that is not directly related to a cybersecurity threat, or that identifies personal information of a specific individual or information that identifies a specific individual.

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

Not applicable.

5. Is the agency implementing the policies, procedures, and guidelines from question 2 and does the process for sharing cyber threat indicators within the Federal Government determined from question 1 align with the process included in the policies, procedures, and guidelines?

Yes.

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)?

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 whether not using the four procedure documents impacts the sharing – IC IG will coordinate additional follow-up, if necessary)

None.

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

Yes, Department officials believe there are gaps related to Federal cyber information sharing. These gaps are related to the lack of interagency adherence to the coordinated standardized sharing policies/recommendations included in the interagency-approved MISA.

Sharing Cyber Threat Indicators and Defensive Measures with Private Sector

9. Has the agency shared cyber threat indicators and defensive measures with the private sector?

Yes. DHS shares unclassified cyber threat indicators and defensive measures with the private sector through AIS and CISCP data feeds. According to CISA, it is not able to provide us with the specific number of indicators shared with just the private sector. However, we are working with our OIG data analyst to identify exact numbers.

10. If yes for question 9, are any of the shared cyber threat indicators and defensive measures classified?

Yes. DHS shares classified indicators and defensive measures via 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 cyber threat indicators and defensive measures. The Department shared 1,347 and 13,163 classified indicators in 2019 and 2020, respectively.

11. If yes for question 10, what was the process used by the agency to classify the shared cyber threat indicators and defensive measures?

DHS classified cyber threat indicators using derivative classification. The original classification of the cyber threat indicators remained with the Original Classification Authority. Also, DHS uses additional security classification guides (e.g., the National Cybersecurity Protection System and Enhanced Cybersecurity Services) to derivatively classify cyber threat indicators.

11a. Review a sample of the shared cyber threat indicators and defensive measures and determine whether the cyber threat information was properly classified.

After reviewing 60 unclassified and 60 classified indicators that were judgmentally selected, we determined that the indicators sampled were properly classified.

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

Yes, for the classified indicators.

Accounting of Security Clearances

12. Has the agency authorized security clearances for sharing cyber threat indicators and defensive measures with the private sector?

Yes. DHS granted over 200 security clearances in both 2019 and 2020 to private sector partners under various DHS information sharing programs. However, DHS does not track the number of security clearances that have been issued under the Act. Since DHS shares unclassified cyber threat indicators 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 2019 and 2020?

The Department maintains active security clearance information in its Microsoft SharePoint application. In 2019 and 2020, DHS maintained 1,845 and 1,906 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?

A private sector company representative said that obtaining clearances has always been an issue due to Federal agencies' policies, such as National Security Adjudicative Guidelines, restricting the number of clearances issued. As a result, according to the representative, none of the company's front-line analysts have been provided clearances.

Using and Disseminating Cyber Threat Indicators and Defensive Measures Shared by Other Federal Agencies

14. Has the agency used and disseminated cyber threat indicators and defensive measures shared by other Federal agencies?

Yes, DHS has used cyber threat indicators shared by other Federal agencies and has disseminated cyber threat indicators and defensive measures shared by other Federal agencies.

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

Yes, based on our sample, DHS shares unclassified indicators via the AIS program according to the Department's Traffic Light Protocol and classified indicators under the business rules of the EINSTEIN 3 Accelerated and Enhanced Cybersecurity Services programs. According to the AIS Terms of Use, the Department anonymizes the identities of the sources of the indicators. The Department shares all indicators received in AIS on a real-time basis, machine to machine.

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

Yes, DHS shares unclassified indicators via AIS to help Federal agencies protect their networks and improve their cybersecurity posture. For example, recent sharing of the SolarWinds event cyber threat information has led CISA and the Department of Defense Cyber National Mission Force to analyze these malware variants and trace their origins so that future prevention can be remedied.

Sharing Cyber Threat Indicators and Defensive Measures with Other Federal Agencies

15. Has the agency shared cyber threat indicators and defensive measures with other Federal agencies?

Yes, DHS shares unclassified cyber threat indicators and defensive measures directly with Federal agencies and indirectly with Federal agencies via third-party data aggregators. According to CISA officials, DHS shared the following cyber threat indicators for each year from all three feeds:

2019: 4,590,001
2020: 12,048,439

15a. If yes, review a sample to 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.

We reviewed and traced a sample of indicators in the AIS capability for detailed information. Additionally, DHS shares unclassified cyber threat indicators via the AIS capability as they are received. If human review is required, DHS marks the fields as "under review" and shares all other available information.

DHS releases the other relevant information as quickly as operationally practical.

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

DHS shares cyber threat information with over 280 AIS partners. Of the AIS partners, 36 are Federal departments and agencies, such as the Departments of Agriculture, Commerce, Defense, Education, Energy, Health and Human Services, Housing and Urban Development, Transportation, Treasury, Veteran Affairs, and National Aeronautics and Space Administration, National Science Foundation, and Nuclear Regulatory Commission.

The Federal department and agency partners connected directly to the AIS Trusted Automated eXchange of Indicator Information (TAXII) server to receive AIS cyber threat and defensive measure information.

17. Have other Federal entities shared cyber threat indicators and defensive measures with the agency?

Yes, Department of Defense Cyber Crime Center (DC3), Defense Information Systems Agency, Department of Energy, and the National Security Agency shared into AIS directly.

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

We reviewed a sample of indicators and determined that they were received and shared in a timely, adequate, and appropriate manner. Additionally, DHS shares unclassified cyber threat indicators via AIS as they are received.

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

18. How many cyber threat indicators and defensive measures did entities share with the Department of Homeland Security through the Automated Indicator Sharing (AIS) capability in CYs 2019 & 2020? Provide results.

According to CISA officials, DHS received 4,584,463 indicators in 2019 and 12,041,366 indicators in 2020.

19. How many of those cyber threat indicators and defensive measures reported for question 18 did Department of Homeland Security share with other Federal entities CYs 2019 & 2020? Provide results.

According to CISA officials, DHS shared 4,590,001 indicators in 2019 and 12,048,439 indicators in 2020.

Cyber Threat Indicators and Defensive Measures Received from Other Federal Agencies

20. (Agencies other than DHS) How many cyber threat indicators and defensive measures did Department of Homeland Security relay to the agency via AIS CYs 2019 & 2020?

Not applicable to DHS.

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 to DHS.

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. To ensure that no PII is released, DHS has implemented automated controls in AIS to redact for additional review any free text fields that may contain potential PII. DHS performs a human review, and if necessary, redacts any PII and subsequently sends the approved information through AIS.

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

Not applicable.

23. Was the privacy and civil liberties of any individuals affected due to the agency sharing cyber threat indicators and defensive measures?

No.

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

Not applicable.

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

No.

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

Not applicable.

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 adversely affected the sharing of cyber threat indicators and defensive measures among Federal entities? Provide a description of the barriers and the effect the barriers have on the sharing of cyber threat indicators and defensive measures.

Yes. Barriers include Federal entities not adhering to agreed-upon interagency policy recommendations for Federal cyber information sharing documented in the MISA. Other barriers include lack of formal dedicated funding for Federal agencies to implement cyber information capabilities that follow the agreed-upon policy requirements. Some agencies also do not have internal staff resources to support sharing of indicators. As a result, these agencies are not able to complete the additional automated workflows required to generate and transmit machine-to-machine cyber information sharing. They can produce human-readable reports disseminated via email, but the technical barriers to convert this information into AIS open standard format remain high.

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

Yes, some entities stated that they had difficulty implementing the AIS platform and TAXII feeds. Due to these difficulties in setting up the TAXII, they could not share information.

26b. Any difficulties due to classification of information?

No, AIS does not share classified information.

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

Yes, Federal entities stated they were reluctant to share information. Some Federal entity representatives expressed concerns regarding distribution of information outside of certain "communities." For example, some Federal entities were open to sharing with private sector but were concerned about sharing with the international community. Both the AIS Public Feed and the CISCP Feed have some level of participation by the international community.

26d. Any difficulties due to the number of cyber threat indicators and defensive measures received? Too many to ingest and review?

Based on our interview with a private sector entity, some agencies and private sector entities do not have the resources to sift through the large number of indicators that are available via AIS.

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

Private sector feedback identified concerns with AIS customers experiencing false positives from the AIS Public Feed that were later identified as known good indicators. CISA responded to this by improving the AIS "allow list" to ensure that these types of known good indicators are not distributed via AIS to stakeholders. Federal agency officials also noted that some Federal AIS participants have shared unconfirmed malware cyber threat indicator information or low confidence threat information that resulted in false positive alerting within security tools. Some Federal stakeholders can filter out some of these lower confidence indicators while others may not have the expertise or intermediate tools to further refine relevant cyber threat indicators before deploying them into security tools for automated alerting or mitigation.

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

As of our last reporting period, DHS was still in the process of upgrading the AIS infrastructure and implementing the latest Organization for the Advancement of Structured Information Standards. These open standards will improve TAXII 2.1 and Structured Threat Information eXpression (STIX) 2.1, which will enable sharing of improved data in an enriched environment and allow trend correlation. CISA has taken a leadership role in the Organization for the Advancement of Structured Information Standards Technical Committee to help the development and release of STIX/TAXII interoperability documentation and further version updates of AIS, TAXII, and STIX. CISA is also proactively developing and implementing updates to stakeholder engagement and awareness documentation to support the many improvements and new capabilities implemented in support of the latest cyber information sharing open standards.

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

DHS is developing documentation, including several guides in support of best practices, to align with the launch of AIS 2.0 in April 2022. A sampling of documents includes: *AIS Profile for Dummies*, *STIX for Dummies*, *Submission of Content to AIS TAXII for Dummies*, *Guide to Using AIS Data for Operational Defensive Measures,* and *Guide to Creating and Validating STIX Content.* In addition, DHS continues to implement an AIS Engagement Plan to identify and recruit targeted partners, which may help entities that are not sharing information with DHS to overcome their hurdles through multiple Federal and non-Federal parallel CISA-led formal engagements.

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

DHS uses AIS machine-to-machine capability, web form, email, and the Homeland Security Information Network portal to share and/or receive cyber threat indicators and defensive measures.

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

No, because the Intelligence Community and Analysis Tool does not follow the Federal interagency-approved MISA policy guidance.

30. Have 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)]

To meet the Act's requirement for Privacy and Civil Liberties Guidelines, CISA's Privacy Office engaged with the National Security Agency's Privacy and Civil Liberties Office and the Defense Privacy and Civil Liberties Office, among others, for the interagency portion of the 2020 review. The interagency portion of the review was delayed due to the new Administration. The review was completed in January 2021.

Appendix D
Major Contributors to This Report

Tarsha Cary, Director
Danny Urquijo, Audit Manager
James Diaz, Auditor-in-Charge
Zachary Israel, Auditor
Rob Williams, Program Analyst
Brandon Hoel, Program Analyst
Gaven Ehrlich, Program Analyst
Mai Huynh, Program Analyst
Nandini Parvathareddygari, IT Specialist
Swati Nijhawan, Independent Referencer
Ben Wing, Independent Referencer
Joshua Wilshere, Supervisory Data Architect
Thomas Hamlin, Communications Analyst

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
Executive Assistant Director, Cybersecurity Division, CISA
Assistant Director, National Risk Management Center, CISA
Audit Liaison, CISA

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees

Additional Information and Copies

To view this and any of our other reports, please visit our website at: www.oig.dhs.gov.

For further information or questions, please contact Office of Inspector General Public Affairs at: DHS-OIG.OfficePublicAffairs@oig.dhs.gov.
Follow us on Twitter at: @dhsoig.

OIG Hotline

To report fraud, waste, or abuse, visit our website at www.oig.dhs.gov and click on the red "Hotline" tab. If you cannot access our website, call our hotline at (800) 323-8603, fax our hotline at (202) 254-4297, or write to us at:

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