OFFICE OF INSPECTOR GENERAL

# DHS Made Limited Progress to Improve Information Sharing under the Cybersecurity Act in Calendar Years 2017 and 2018

Homeland Security

September 25, 2020
OIG-20-74

**OFFICE OF INSPECTOR GENERAL**
Department of Homeland Security

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

September 25, 2020

MEMORANDUM FOR: The Honorable Christopher Krebs
Director
Cybersecurity and Infrastructure Security Agency

Joseph V. Cuffari

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

SUBJECT: *DHS Made Limited Progress to Improve Information Sharing under the Cybersecurity Act in Calendar Years 2017 and 2018*

Attached for your information is our final report, *DHS Made Limited Progress to Improve Information Sharing under the Cybersecurity Act in Calendar Years 2017 and 2018.* We incorporated the formal comments provided by your office.

The report contains four recommendations aimed at improving information sharing under the Cybersecurity Act. Your office concurred with all four recommendations. Based on the information provided in your response to the draft report, we consider recommendation 2 open and unresolved. As prescribed by the Department of Homeland Security Directive 077-01, *Follow-Up and Resolutions for the Office of Inspection 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. We consider recommendations 1, 3, and 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. 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 call me with any questions, or your staff may contact Sondra McCauley, Assistant Inspector General for Audits, at (202) 981-6000.

Attachment

# DHS OIG HIGHLIGHTS

## *DHS Made Limited Progress to Improve Information Sharing under the Cybersecurity Act in Calendar Years 2017 and 2018*

**September 25, 2020**

## Why We Did This Review

Section 107 of the *Cybersecurity Act of 2015* requires Inspectors General from the Intelligence Community and appropriate agencies to submit a joint report to Congress on Federal Government actions to share cybersecurity information. We conducted this review to evaluate CISA's progress in meeting Cybersecurity Act requirements for calendar years 2017 and 2018.

## What We Recommend

We recommend CISA improve quality by increasing participants' sharing of cyber information, completing system upgrades, and hiring the staff needed to enhance program training and outreach.

**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 Department of Homeland Security has addressed the basic information sharing requirements of the *Cybersecurity Act of 2015.* To carry out its mandate, the Cybersecurity and Infrastructure Security Agency (CISA) within DHS, developed policies, procedures, and an automated capability, known as the Automated Indicator Sharing (AIS) program, to share cyber threat information between the Federal Government and the private sector. CISA increased the number of AIS participants as well as the volume of cyber threat indicators it has shared since the program's inception in 2016. However, CISA made limited progress improving the overall quality of information it shares with AIS participants to effectively reduce cyber threats and protect against attacks.

CISA's lack of progress in improving the quality of information it shares can be attributed to a number of factors, such as limited numbers of AIS participants sharing cyber indicators with CISA, delays receiving cyber threat intelligence standards, and insufficient CISA office staff. To be more effective, CISA should hire the staff it needs to provide outreach, guidance, and training.

Risks to the Nation's systems and networks continue to increase as security threats evolve and become more sophisticated. As such, the cyber threat information DHS provides to Federal agencies and private sector entities must be actionable to help better manage this growing threat. Until CISA improves the quality of its information sharing, AIS participants remain restricted in their ability to safeguard their systems and the data they process from attack, loss, or compromise.

## CISA Response

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

## Table of Contents

## Appendixes

## 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 |
| IT | information technology |
| MOE | Mission Operating Environment |
| OIG | Office of Inspector General |
| OMB | Office of Management and Budget |
| PII | personally identifiable information |
| STIX | Structured Threat Information eXpression |
| TAXII | Trusted Automated eXchange of Indicator Information |
| TS MOE | Top Secret Mission Operating Environment |

## Background

Federal agencies depend on information technology (IT) systems and networks to carry out operations and process, maintain, and report on essential information. As cyber threats evolve, increase, and become more sophisticated, securing our systems and networks from unauthorized access and potential exploits is one of the most difficult challenges we face as a Nation. These threats include the use of phishing, malicious software, identity theft, device access, and bank fraud.[1] Advances in IT and the proliferation of mobile devices have introduced even more cybersecurity risks across all industries, and researchers predict that more than 20 billion devices will be connected to the Internet by 2020. National security and our economy depend on a stable, safe, and resilient cyber space.

The Department of Homeland Security is responsible for coordinating nation-wide responses to cyber incidents. One of DHS' key missions is to safeguard and secure the Nation by assessing the cyber risk landscape, reducing vulnerabilities, and building resilience. The Cybersecurity and Infrastructure Security Agency (CISA) leads the national effort to defend critical infrastructure against cyber threats by working with partners across all levels of government and in the private sector. CISA serves as a central point of command for partners to analyze cybersecurity information, communicate and share timely and actionable information, and coordinate response, mitigation, and recovery efforts.[2] To carry out its mission, analysts at CISA use a number of tools, such as National Cybersecurity Protection System capabilities,[3] to secure and defend the Federal Government's information technology infrastructure against cyber threats.

Information sharing is a key component of addressing ever expanding cybersecurity threats. On December 18, 2015, the President enacted the *Cybersecurity Act of 2015* (the Act) to establish a voluntary process for sharing cyber threat information between Federal agencies and private sector entities.[4] The Act requires the Director of National Intelligence, the Secretaries of Defense and Homeland Security, and the Attorney General to develop and issue procedures jointly to facilitate and promote sharing of classified and

[1] Phishing attacks refer to cybercriminal attempts to lure users to click on links to malicious websites or open file attachments to infect users' computers with viruses or malware to steal personal and financial information.
[2] CISA's partners include other government agencies, the private sector, and international entities.
[3] National Cybersecurity Protection System capabilities are operationally known as EINSTEIN.
[4] Federal agencies include Federal departments, agencies, and components of agencies.

unclassified cyber threat information. The Act encourages Federal and private organizations to share this information while protecting classified information, intelligence sources and methods, privacy, and civil liberties. Specifically, the Act promotes the sharing of three key elements: cyber threat indicators (e.g., malicious Internet Protocol addresses or phishing email addresses), defensive measures, and best practices.

According to the Act, cyber threat indicators are defined 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;
- methods of defeating a security control or exploitation of a security vulnerability;
- security vulnerabilities, including anomalous activity, that appear to indicate the existence of a security vulnerability;
- methods of exploiting a security vulnerability to gain unauthorized access to information or an information system;
- malicious cyber command and control;
- actual or potential harm caused as a result of a particular cybersecurity threat; and
- disclosure of any other attribute of a cybersecurity threat that is not prohibited by law.

Defensive measures are defined as actions, devices, procedures, signatures, techniques, or other measures applied to an information system to detect, prevent, or mitigate known or suspected cybersecurity threats or security vulnerabilities.[5]

### DHS Program to Share Cyber Threat Indicators

CISA is the central hub for overseeing the real-time exchange of cyber threat information between the Federal Government and the private sector to protect against attacks. Federal entities exchange classified and unclassified cyber information in real-time under the *Enhance Shared Situational Awareness Multilateral Information Sharing Agreement.*[6] To fulfill the Act's requirements

[5] These measures do not include actions to cause destruction or inflict harm on an information system or information that is not owned by the private entity.

[6] This Federal multi-agency agreement was developed to enhance cybersecurity information sharing among Federal agencies to better protect U.S. computer systems from malicious cyber threats fully consistent with the Federal laws and oversight requirements.

for sharing cyber threat indicators and defensive measures, CISA implemented the Automated Indicator Sharing (AIS) program in March 2016. All Federal and non-Federal entities, as well as foreign governmental and foreign private sector entities, are eligible to participate in the AIS program.

The fundamental concept of the AIS program is the interaction between participants (i.e., information producers and information consumers) to exchange cyber threat indicators across the Federal Government, state, local, tribal, and territorial governments, and the private sector. The AIS capability was designed to allow CISA to exchange unclassified cyber threat information, such as commercially-available threat information and partner-submitted data from various sources, or information producers. To receive unclassified cybersecurity threat information through the AIS program, participating entities must first sign an information sharing agreement. CISA offers three separate information sharing categories, or data feeds, to AIS participants:

- FedGov – is for Federal entities that have signed the *Enhance Shared Situational Awareness Multilateral Information Sharing Agreement*.

- AIS – is for non-Federal entities (e.g., private sector, state, local, tribal, and territorial partners, and foreign participants) that are signatories to the AIS Terms of Use, or customers of AIS participants that are allowed to re-distribute the information.

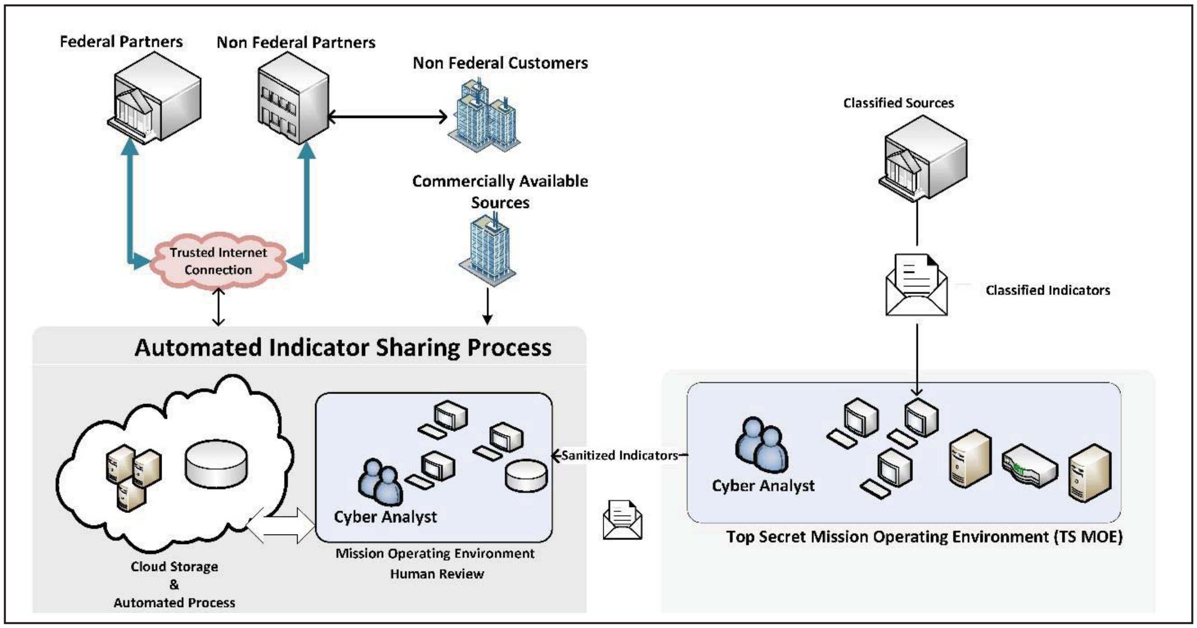
- Cyber Information Sharing and Collaboration Program (CISCP) – is a program for public-private information sharing that complements ongoing CISA information sharing efforts. CISA and participating companies share information about cyber threats, incidents, and vulnerabilities. Participants are able to join the AIS initiative by agreeing to the *CISCP Cooperative Research and Development Agreement*.

To facilitate the information sharing process, CISA cyber analysts receive cyber threat indicators and defensive measures submitted through AIS. CISA cyber analysts use unclassified Mission Operating Environment (MOE) workstations to review the information received.[7] Then, cyber analysts remove personally identifiable information (PII) and other sensitive information not directly related to the cybersecurity threat. Analysts disseminate the edited information through AIS to share with Federal and private sector partners. Additionally, CISA compiles information from classified sources, then removes sensitive or private information before disseminating it. Analysts enter declassified

[7] The Top Secret Mission Operating Environment (TS MOE), a component of EINSTEIN 3 Accelerated, processes classified information for the National Cybersecurity Protection System.

indicators into MOE. Nonetheless, the background information supporting the now unclassified indicators may remain classified. The unclassified and classified data flows are illustrated in Figure 1.

**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 & Automated Process
Mission Operating Environment Human Review
Top Secret Mission Operating Environment (TS MOE)

*Source*: DHS Office of Inspector General (OIG)-generated based on information received from CISA

The left side of Figure 1 shows that AIS participants have the capability to share unclassified cyber threat information over a trusted (i.e., encrypted) bi-directional Internet connection. The information is stored in the cloud or on machines and transferred to cyber analysts for review. Subsequently, the analysts send the machine-readable files out to the AIS participants. AIS participants may analyze and manage the files within their own networks for their own purposes.

The right side of Figure 1 shows how classified cyber threat indicators are sent to cyber analysts by email, as there is no automatic transfer from TS MOE to MOE. Cyber analysts review and enter the classified indicators manually into TS MOE. The horizontal illustration shows that, after cyber analysts remove classified information from the indicators, the declassified indicators are entered into MOE by emails for sharing with Federal and non-Federal partners.

### Cybersecurity Act Reporting Requirements

Title I, Section 107 of 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. Specifically, the joint report requires an overall assessment of:

- policies, procedures, and guidelines for sharing cyber threat indicators within the Federal Government, including the removal of personal information not directly related to cyber threat indicators;
- proper classification of cyber threat indicators or defensive measures and an accounting of security clearances granted to private sector users to receive classified information under this Act;
- actions taken by Federal agencies based on cyber threat indicators or defensive measures shared within the Federal Government; and
- barriers to sharing cyber threat indicators or defensive measures among Federal agencies.

In addition, the joint report submitted under this section of the Act may include Inspector General recommendations to improve or modify the authorities and processes under this title.[8] We developed this separate, agency-level report based on our evaluation of DHS' progress in meeting its cybersecurity information sharing requirements for calendar years 2017 and 2018. The objective, scope, and methodology for our report are included in Appendix A.

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 39 questions on the actions the agency has taken to implement the Act. Our responses to these questions can be found in Appendix C.

### Prior Reported Findings

In November 2017, we reported on DHS' implementation of the cybersecurity information sharing requirements in 2015 and 2016.[9] We reported that the

[8] The Office of the Inspector General of the Intelligence Community issued the *Unclassified Joint Report on the Implementation of the Cybersecurity Information Sharing Act of 2015,* AUD-2019-005-U, December 19, 2019.

[9] *Biennial Report on DHS' Implementation of the Cybersecurity Act of 2015,* OIG-18-10, November 1, 2017.

Department had adequately addressed the following requirements of Title I of the Act:

- DHS developed adequate policies and procedures and a supporting capability to share cyber threat indicators and defensive measures;
- DHS properly classified cyber threat indicators and defensive measures and accounted for the security clearances of private sector users authorized to receive this information; and
- DHS used the cyber threat indicator and defensive measure information received to mitigate potential security risks.

Although such actions are fundamental to DHS establishing a viable cyber threat information sharing capability with its Federal and private sector partners, we also identified the following deficiencies:

- DHS emphasized timeliness, velocity, and volume in cybersecurity information sharing, but the system DHS used did not provide the quality or contextual data needed to effectively defend against ever-evolving threats; and
- DHS could not increase participation and improve coordination of information sharing across Federal and private organizations without conducting more enhanced outreach.

## Results of Review

DHS has addressed the basic information sharing requirements of the *Cybersecurity Act of 2015*. To carry out its mandate, CISA developed policies, procedures, and AIS program, to share cyber threat information between the Federal Government and the private sector. CISA has increased the number of AIS participants as well as the volume of cyber threat indicators it had shared since the program's inception in 2016. However, CISA has made limited progress improving the overall quality of information it shares with AIS participants to effectively reduce cyber threats and protect against attacks.

CISA's lack of progress in improving the quality of information it shares can be attributed to a number of factors, such as limited numbers of AIS participants sharing cyber indicators with CISA, delays receiving cyber threat intelligence standards, and insufficient CISA office staff. To be more effective, CISA should hire the staff it needs to provide outreach, guidance, and training.

Risks to the Nation's systems and networks continue to increase as security threats evolve and become more sophisticated. As such, the cyber threat information DHS provides to Federal agencies and private sector entities must be actionable to help better manage this growing threat. Until CISA improves the quality of its information sharing, AIS participants remain restricted in their ability to safeguard their systems and the data they process from attack, loss, or compromise.

## DHS Met Basic Cybersecurity Act Requirements, but Made Limited Improvements to the Overall Quality of Information It Shares

DHS has addressed the key requirements of Title I of the Act. Namely, CISA has developed policies, procedures, and an automated capability for information sharing, as well as for classifying information to account for the security clearances of information recipients. CISA has increased the number of AIS participants, as well as the number of cyber threat indicators shared since the program's inception in 2016. However, CISA has made limited progress improving the overall quality of information it shares with AIS participants to effectively reduce cyber threats.

### DHS Addressed Key Cybersecurity Act Requirements

In accordance with information sharing requirements of Title I of the Act, CISA has (1) developed policies and procedures needed for sharing cyber threat indicators and defensive measures with Federal and private entities, (2) classified cyber threat indicators and defensive measures, and (3) accounted for the security clearances of private sector users authorized to receive this information.

#### Policies and Procedures for Information Sharing

CISA developed adequate policies and procedures for sharing cyber threat indicators and defensive measures with Federal and private entities to mitigate potential threats, as required by Title I of the Act. As stated previously, CISA implemented the AIS program in 2016 to enable the exchange of unclassified cyber threat information across various sources. In support of the AIS program, CISA also established standard operating procedures for indicator management and cyber threat management, among others.

CISA also met Section 103 requirements to periodically review, at least once every 2 years, the guidelines related to privacy and civil liberties. In June 2018, CISA assisted with the update of the *Privacy and Civil Liberties*

*Guidelines: Cybersecurity Information Sharing Act of 2015* for sharing cyber threat indicators and protecting PII within the timeframe.

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 use derivative classification for the cyber threat indicator and defensive measures. CISA classifies the majority of the cyber threat indicators based on the original classification authority. For example, CISA shared 673 classified threat indicators with non-Federal entities in 2017, and nearly 2,000 in 2018. This was done through its Enhanced Cybersecurity Services program which, unlike the AIS program, can share sensitive and classified cyber threat information to detect and block malicious cyber activity.[10]

Security Clearances for Private Sector to Receive Classified Information

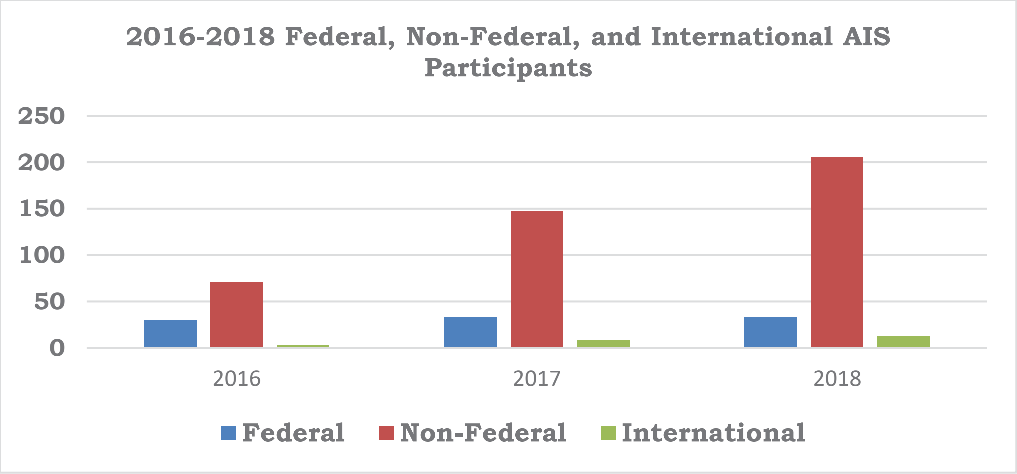
CISA accurately accounted for the security clearances of private sector users authorized to receive classified information. Under various information sharing programs, the Department granted 129 security clearances to private sector partners in 2017, and 155 in 2018. In total, CISA maintained 1,536 active security clearances in 2017, and 1,691 in 2018. However, it should be noted that 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

CISA has increased the overall number of AIS program participants by 142 percent since the program's inception in 2016. Specifically, CISA increased the number of non-Federal participants by more than 195 percent — from 74 in 2016 to 219 in 2018, including 13 International Computer Emergency Response Teams. On the other hand, the number of Federal participants remained fairly steady, with only a 10 percent increase— from 30 entities in 2016 to 33 in 2018. Figure 2 shows the increase of AIS participants from 2016 to 2018.

[10] 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.

**Figure 2. Increase in Federal, Non-Federal, and International AIS Participants**



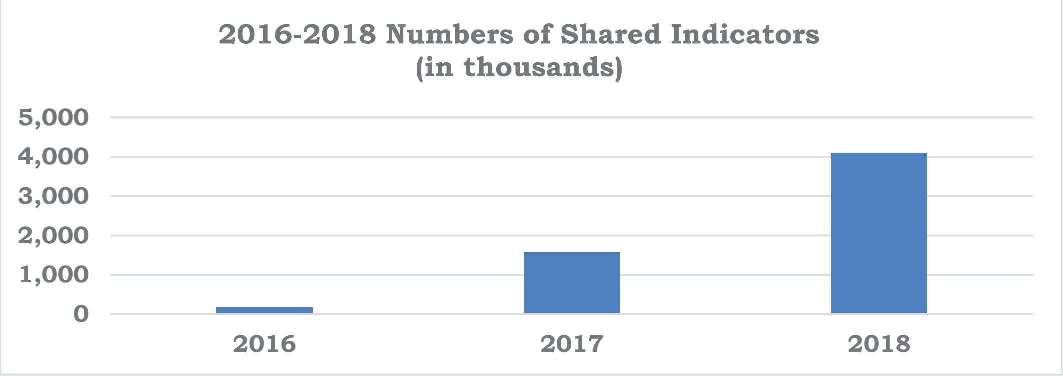
*Source:* DHS OIG analysis

CISA has also increased the number of cyber threat indicators it shared with AIS participants since 2016. For example, CISA increased the overall number of indicators it shared from nearly 180,000 in 2016 to more than 4 million in 2018 (more than 2,000 percent). In total, CISA shared more than 5.4 million indicators via its AIS data feeds in 2017 and 2018. As shown in Figure 3, the 5.4 million total indicators included:

- 332,389 and 407,831 unclassified indicators with private entities in 2017 and 2018, respectively, and

- 1.4 million and 4 million unclassified indicators to other Federal entities program data feeds in 2017 and 2018, respectively. Note that this also included the same indicators shared with the private entities.

**Figure 3. Increase in Shared Indicators for 2016 through 2018**[11]



*Source:* DHS OIG analysis

## CISA Has Not Improved the Quality of Information It Shares

While CISA has increased the number of cyber threat indicators and defensive measures shared with program participants, the AIS information did not contain enough detail to fully mitigate potential threats. Specifically, the AIS indicators shared with participants did not contain actionable information, including sufficient context or background details to effectively protect Federal and private networks. Examples of contextual information may include Internet Protocol addresses, domain names, or hash files, which may be helpful for determining the appropriate course of action to mitigate threats against networks.

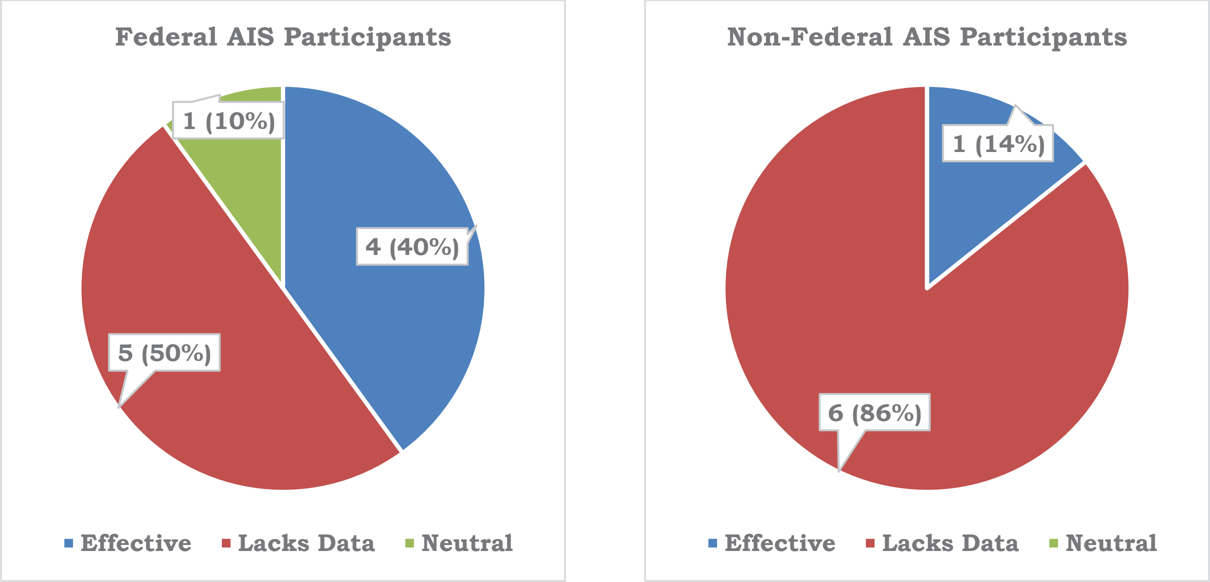
To determine whether CISA had improved the quality of information it shared under the AIS program, we obtained feedback from 17 AIS participants (10 Federal agencies and 7 private sector entities). Although some participants conceded the accuracy and quality of the indicators were not high, they still found the information beneficial. The feedback we obtained is outlined as follows, and shown in Figure 4:

- 11 of 17 participants (5 Federal and 6 private sector) said the indicators lacked contextual/background data for determining the appropriate course of action to mitigate threats against their networks. Additionally, some participants stated that some indicators received were false positives or unusable information.

[11] During 2017 and 2018, CISA continued to share cyber threat indicators via three data feeds: AIS, CISCP, and FedGov.

- 6 of 17 participants (3 Federal and 3 private sector) said they had to augment the AIS indicators with additional information from other third-party sources.[12]
- 5 of 17 participants (4 Federal and 1 private sector) stated the AIS program was effective or helpful.
- 1 Federal agency did not express an opinion on the usefulness of the program.

**Figure 4. Sample of Federal and Non-Federal Participants' Feedback on Quality of Indicators**



*Source:* DHS OIG analysis

## Multiple Factors Contributed to Lack of Progress in Improving the Quality of Information CISA Shares

CISA's lack of progress to improve the quality of the information shared under the AIS program can be attributed to multiple external and internal factors. External factors include the limited number of AIS participants sharing cyber indicators with CISA and the delays in receiving the cyber threat intelligence standards needed to upgrade the AIS capability. Internal factors include insufficient staffing in the CISA office to adequately support the AIS program. Collectively, these shortcomings have hindered CISA's ability to improve the quality of AIS indicators and have thwarted outreach efforts to increase participation and the usefulness of the AIS program.

[12] Private sector entities included the information technology and legal services critical infrastructures.

### More Information Producers May Improve the Quality of AIS Indicators

The limited number of participants that share cyber threat information in AIS is the primary impediment to achieving better quality and more actionable information sharing. Although CISA increased the number of AIS program participants (information consumers) by 142 percent between 2016 and 2018, this did not equate to an increase in the number of information producers. According to program officials we spoke with, the number of program participants using the AIS capability to share cyber threat indicators is minimal. For example, CISA has experienced only a slight increase in data producers sharing their cyber threat indicators and defensive measures using AIS during the past 2 years. Specifically, only 2 of 188 AIS participants (1 percent) shared cyber indicators with CISA in 2017, and only 9 of 252 participants (3 percent) shared indicators in 2018. Without more information producers, CISA cannot improve the quality of information it shares under the program and AIS participants remain restricted in their ability to effectively mitigate evolving security threats and vulnerabilities.

The Office of Management and Budget (OMB) recognized information sharing as important to understanding the Federal Government's cybersecurity risks. In its October 2015 memorandum, OMB required Federal agencies to work with DHS to implement an automated indicator sharing capability within 12 months.[13] According to the OMB memorandum, the Department analyzes cybersecurity information from sensors deployed across the Federal Government and from incidents reported by Federal agencies and the private sector. To promote the sharing of this information, in a January 2016 memorandum,[14] the Assistant to the President for Homeland Security and Counterterrorism emphasized the importance of agencies using the AIS capability to share indicators with DHS about incidents involving their networks.

To increase participation, CISA developed the *AIS Engagement Action Plan* in November 2017.[15] This plan calls for identifying and recruiting targeted partners and helping them overcome challenges through an educational webinar series focused on AIS attributes and functions. Until more Federal agencies and private sector entities share their cyber threat information, CISA

[13] OMB, *Cybersecurity Strategy and Implementation Plan for the Federal Civilian Government,* M-16-04, October 30, 2015.
[14] Lisa O. Monaco, *Participation in Automated Cyber Indicator Sharing with the Department of Homeland Security*, January 15, 2016.
[15] Stakeholder Engagement and Cyber Infrastructure Resilience, *FY 2018 AIS Stakeholder Engagement Plan: Increasing AIS Coverage and Participation*, November 2017.

is restricted in its ability to provide more contextual cyber threat indicators and defensive measures to assist AIS participants with their cyber defense.

### Delayed Updates to Cybersecurity Standards Have Impeded AIS Upgrades

Delays receiving the latest approved industry cyber threat intelligence standards have caused CISA to postpone its plan to upgrade AIS. Initially, CISA expected the AIS upgrade would be completed by December 2018. However, the Organization for the Advancement of Structured Information Standards is experiencing delays finalizing the new Structured Threat Information eXpression (STIX)/Trusted Automated eXchange of Indicator Information (TAXII) standards.[16] According to CISA, STIX/TAXII are community-driven technical specifications designed to enable automated information sharing for cybersecurity situational awareness, network defense, and threat analysis.

CISA officials stated that, in 2017, they started adding more contextual information from more than 90 different data feeds and 2 data enrichment sources to AIS data. CISA expects to have more quality cyber threat information when it completes this upgrade. However, AIS program officials said that CISA could not provide a revised upgrade timeline or complete new AIS technical specifications until the STIX/TAXII standards are finalized.

### Insufficient Staffing Hinders Overall Effectiveness of AIS Program

Insufficient staffing has hindered CISA’s outreach and support efforts (i.e., training and guidance) for the AIS program. During 2017 and 2018, CISA actually had no dedicated staff to manage the AIS capability, perform outreach, or support the program. For example, when we met with the AIS Program Manager, the position was not designated as a permanent one. Rather, the incumbent was performing this function along with many other collateral duties. While managing the AIS program has always been a collateral duty for CISA staff, the time dedicated to it has been decreasing since 2017. To illustrate, the AIS Program Manager dedicated 50 percent of her time to the AIS program in 2017. However, this decreased to 20 percent in 2018.

[16] The Organization for the Advancement of Structured Information Standards, a not-for-profit international consortium, promotes industry consensus and produces worldwide standards for security, cloud computing, the Smart Grid, content technologies, emergency management, E-Government, and many other areas. DHS initiated the development of these standards in 2012 and licensed them to the Organization for the Advancement of Structured Information Standards in 2015 for future continued updates. STIX is a computing language that enables organizations to share structured cyber threat information. TAXII is the main transport mechanism for sharing cyber threat information in a secure and automated manner.

AIS participants have expressed the need for better training and guidance for the AIS program. For example, CISA provides guidance on sharing cyber threat information with Federal and Non-Federal entities, and if necessary, removing PII before sharing cyber threat indicators with CISA. However, AIS participants expressed a need for additional support, as well as a better means of providing feedback to CISA. We spoke with representatives from 14 Federal and private sector AIS participants to determine whether the outreach and support that CISA provided was adequate. Representatives expressed the following concerns:

- One non-Federal participant stated that CISA provides data submission guidance, but stressed that more AIS training (e.g., an onboarding process) was needed.

- Three participants (two Federal and one non-Federal) had experienced technical problems, such as file format incompatibility. The problems were still ongoing because they related to the AIS upgrade and the absence of technical capabilities to share indicators via the AIS. One participant stated that a company needed to upgrade its system to receive the indicators fully.

- Three participants (two Federal and one non-Federal) wanted training (e.g., hands-on sessions and webinars) on how to digest and use the cyber threat indicators received via AIS capability, as well as how to send information back to CISA using the system.

We reported similar issues in our November 2017 report.[17] Particularly, Federal and private sector representatives stated that CISA had not provided sufficient training on how to use the cyber threat indicators and defense measures received through the AIS program. Some representatives indicated assistance would be helpful, as they often could not determine whether certain indicators were intended for action or for information purposes only. Further, in 2017, CISA officials acknowledged the need to increase AIS participation and assist Federal and private sector entities that needed help to overcome technical, resource, or cultural obstacles. Upon issuing our report, we recommended that DHS enhance outreach to promote DHS' information sharing program.

[17] *Biennial Report on DHS' Implementation of the Cybersecurity Act of 2015,* OIG-18-10, November 1, 2017.

In its response to our report, DHS stated it planned to promote the AIS program by helping organizations experiencing technical, resource, or cultural hurdles impeding their participation. DHS established a goal of ensuring participation from all 16 critical infrastructure sectors, including engagement with the respective sector-specific agencies. The estimated completion date for these efforts was June 30, 2018. To this end, DHS developed a prioritized engagement strategy, continued to hold quarterly AIS webinars, and established an AIS Steering Committee to identify barriers to sharing and to provide recommended solutions. Accordingly, we closed our report recommendation in October 2018.

## More Contextual Information Is Needed to Better Enable Participants to Defend against Evolving Cyber Threats

The risks to IT systems supporting the Federal Government are increasing as security threats continue to evolve and become more sophisticated. In FY 2017 alone, Federal Government agencies faced approximately 35,000 information security incidents involving threats such as web-based attacks, phishing attacks, and the loss or theft of computer equipment.[18] Cyber threat information provided by DHS must be actionable to help Federal agencies and private sector entities manage these risks.

Until CISA improves the overall quality and contextual details of the information it shares with its Federal and private sector partners, AIS participants remain restricted in their ability to effectively mitigate evolving security threats and vulnerabilities. Without more data producers, CISA cannot achieve the National Cybersecurity Protection System's primary objective to prevent cybersecurity incidents from occurring through improved sharing of threat information. Likewise, CISA cannot reduce incident response times or improve efficiencies through more automated information sharing.

By enhancing its AIS outreach program, CISA may increase participation and better educate Federal and private sector partners on the AIS program's services. Additional AIS outreach by CISA may also encourage bi-directional cyber threat indicator sharing across Federal and non-Federal entities, and promote better use of the cyber threat indicators shared. To accomplish this, outreach should include training, technical assistance, and information sharing forums to educate participants on how to better receive as well as share cyber threat information. To the extent that Federal and private sector entities can share and exchange cyber threat indicators generated in their

[18] OMB's *Federal Information Security Modernization Act of 2014 FY 2018 Annual Report to Congress, Fiscal Year 2018,* August 23, 2019.

respective environments, the Nation's networks can be better protected from a widening range of potential cyber threats.

## Recommendations

We recommend the Director of CISA:

**Recommendation 1:** Develop an approach to encourage Federal and private sector participants to share information with the Department and become data producers under the AIS program.

**Recommendation 2:** Collaborate with the Organization for the Advancement of Structured Information Standards to expedite the approval of new standards so that the CISA can complete AIS upgrades.

**Recommendation 3:** Actively promote the AIS program through increased outreach, training, technical assistance, and information sharing forums for Federal and private sector entities.

**Recommendation 4**: Place priority on hiring administrative and operational staff needed to conduct outreach, training, and performance measurement to improve the AIS program's operational effectiveness.

## Management Comments and OIG Analysis

CISA concurred with all four of our recommendations. A copy of CISA's response in its entirety is included in Appendix B. CISA also provided technical comments and suggested revisions to our report in a separate document. We reviewed the technical comments and made changes to the report where appropriate. A summary of CISA's response and our analysis follows.

**CISA Comments to Recommendation 1:** Concur. CISA is undertaking multiple efforts that are responsive to this recommendation, such as coordinating discussions to assess the cyber threat needs of Federal and private sector AIS participants. CISA is also evaluating ways to improve Federal/private sector ability to contribute to AIS and is updating AIS documentation and working with private sector providers to enable the ability to share data under AIS. Moreover, CISA is working with other agencies through the Integrated Cyber Defense Working Group to establish clear cyber threat information sharing goals, objectives, and standards to enhance federal automated machine-to-machine sharing, and to reduce and eliminate any associated challenges and barriers.

Furthermore, CISA is leading numerous efforts to systematically: 1) tackle real and perceived challenges within AIS; 2) build trust and confidence from the cybersecurity community; and 3) encourage more active participation. Initiatives include testing AIS data-enriched feeds with various vendors to offer better quality data, as well as exploring other forms of cyber threat data made shareable via AIS, such as threat actor Tactics, Techniques, and Procedures and automated machine-shareable workflows. Finally, CISA will update the "AIS Submission Guidance" document, which will provide step-by-step instructions for all participants to successfully format and share data through AIS. The estimated completion date is December 31, 2020.

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

**CISA Comments to Recommendation 2:** Concur. CISA remains an active member of the Organization for the Advancement of Structured Information Standards and continues to work collaboratively through the standards development process to advocate for the Federal, State, local, tribal, territorial, and private sector cybersecurity enterprise. Furthermore, the STIX 2.1, dated July 26, 2019, and the TAXII 2.1, dated January 27, 2020, specifications were updated, approved, and publicly released. Separately, CISA still requires approval and release of the STIX/TAXII 2.1 Interoperability Test Document Part 1 prior to completing the development and release of AIS 2.0. Based on the actions taken to date, CISA requests the OIG consider this recommendation resolved and closed, as implemented.

**OIG Analysis of CISA Comments:** CISA's actions are largely responsive to this recommendation. However, CISA does not meet the intent of the recommendation to complete AIS 2.0 upgrades and also has provided no target completion date by which to do so. This recommendation will remain open and unresolved until CISA completes AIS upgrades and provides supporting documentation.

**CISA Comments to Recommendation 3:** Concur. Throughout FY 2020, CISA took steps to promote AIS through interagency briefs and forums, such as the previously mentioned Integrated Cyber Defense Working Group and CISA's newly designated Cybersecurity Quality Services Management Office, in which AIS will be highlighted and promoted via the Cybersecurity Quality Services

Management marketplace. Furthermore, in July 2020, CISA published the first edition of the “CISA Services Catalog” on CISA’s public-facing website. Among other things, this catalog highlights AIS as an important CISA service offering and a resource that provides users with access to information on all CISA services available to Federal, State, local, tribal, and territorial government entities; private industry; academia; non-governmental organizations; non-profit entities; and general public stakeholders. Lastly, CISA is planning and developing a communication and outreach strategy for the upcoming AIS 2.0 release. This AIS 2.0 strategic document will be completed by the second quarter of FY 2021 and will aid CISA’s efforts to effectively engage the cybersecurity community through various forums. The estimated completion date is March 31, 2021.

**OIG Analysis of CISA Comments:** We agree that the steps CISA has taken satisfy the intent of this recommendation. We consider this recommendation open and resolved until CISA provides documentation to support that all planned corrective actions are completed.

**CISA Comments to Recommendation 4:** Concur. CISA supports the need to prioritize hiring the administrative and operational staff necessary to support AIS and broader information sharing efforts. CISA plans to build out and formalize AIS with structure and resources to better manage its indicator sharing and threat information sharing activities. Moreover, CISA expects to complete the Cyber Threat Information Sharing Roadmap in the first quarter of FY 2021, which will outline the approach needed to improve the operational effectiveness of AIS. Lastly, CISA will build its national cyber threat information sharing strategy in collaboration and coordination with its partners and stakeholders. This national strategy is projected to be completed during the fourth quarter of FY 2021. The estimated completion date is September 30, 2021.

**OIG Analysis of CISA Comments:** We agree that the steps CISA has taken satisfy the intent of this recommendation. We consider this recommendation open and resolved until CISA provides documentation to support that all planned corrective actions are completed.

## Appendix A
## Objective, Scope, and Methodology

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*.

We assessed CISA's progress implementing the cybersecurity information sharing requirements according to Section 107 of the *Cybersecurity Act of 2015*. Our evaluation focused on the progress CISA has made since our last review in fiscal year 2017. Specifically, we determined whether DHS and its components have:

- revised existing policies and procedures or issued additional guidance to improve the sharing of cyber threat indicators within the Federal Government;

- enhanced the information sharing mechanisms and methodology used to receive and share cyber threat indicators and defensive measures and remove unrelated personal information;

- increased the participants that share and receive cyber threat indicators;

- improved the timeliness and quality of the cyber threat indicators that CISA shares and receives with its partners; and

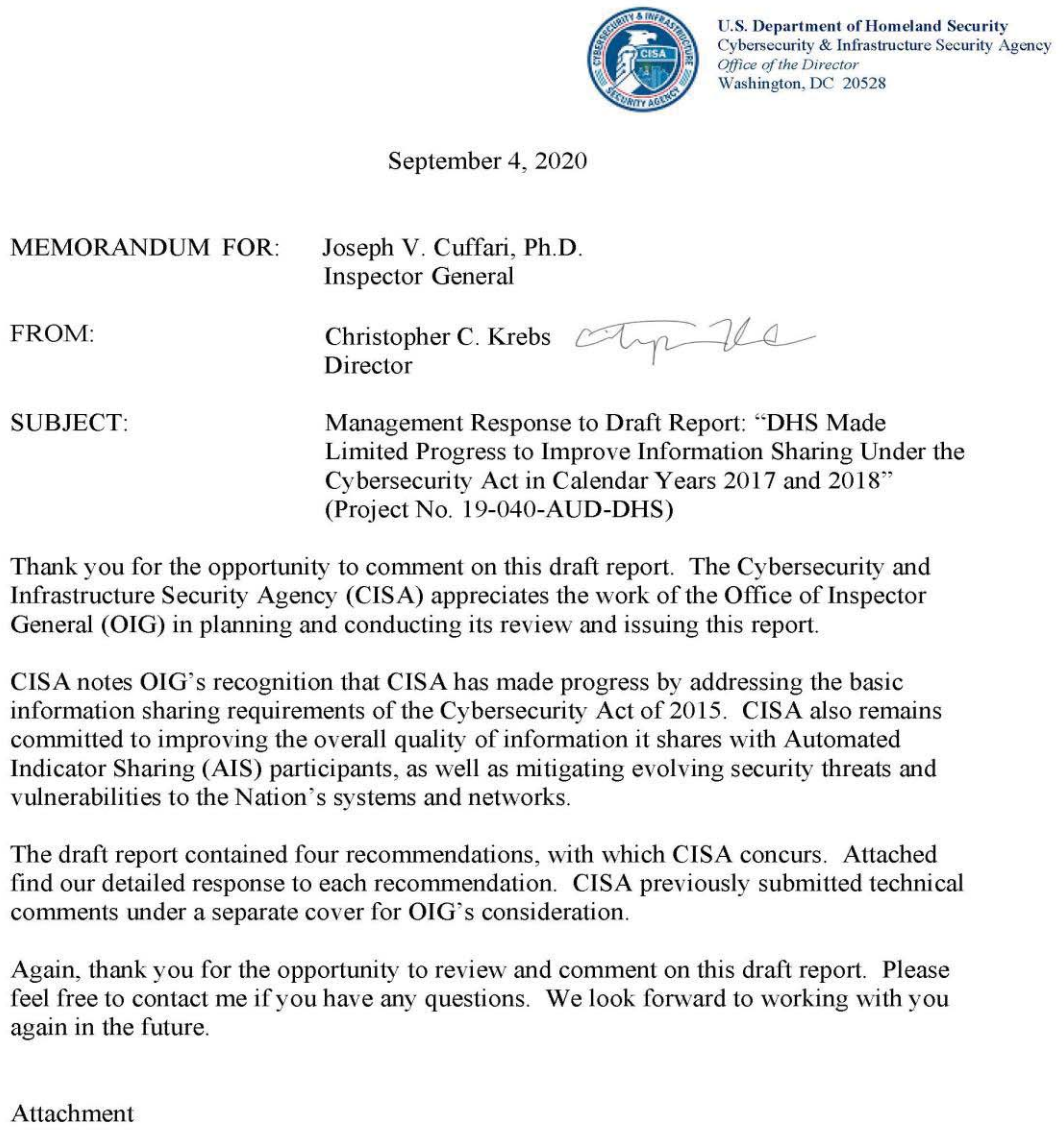
- established new guidance or revised existing procedures to ensure cyber threat indicators and defensive measures are properly classified.

Our fieldwork consisted of interviewing selected personnel from DHS components and offices including CISA, Office of Policy, U.S. Immigration and Customs Enforcement, and United States Secret Service. 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 judgmentally selected and solicited feedback from a total of 44 AIS participants (14 Federal agencies and 30 non-Federal entities), to obtain their perspectives on the effectiveness of the AIS program. Only 17 of 44 participants provided their feedback, including 7 non-Federal entities. We met with representatives of the Departments of Health and Human Services, State, and Veterans Affairs; the General Services Administration, Nuclear Regulatory Commission, Office of

Personnel Management, and Social Security Administration. To limit the scope of our review, we did not interview representatives of state, local, territorial governments, or foreign partners.

We conducted this review between March and November 2019 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 standards. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based upon our review objectives. Major OIG contributors to the review are identified in Appendix D.

## Appendix B
## Agency Comments to the Draft Report



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

September 4, 2020

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

FROM: Christopher C. Krebs
Director

SUBJECT: Management Response to Draft Report: "DHS Made Limited Progress to Improve Information Sharing Under the Cybersecurity Act in Calendar Years 2017 and 2018" (Project No. 19-040-AUD-DHS)

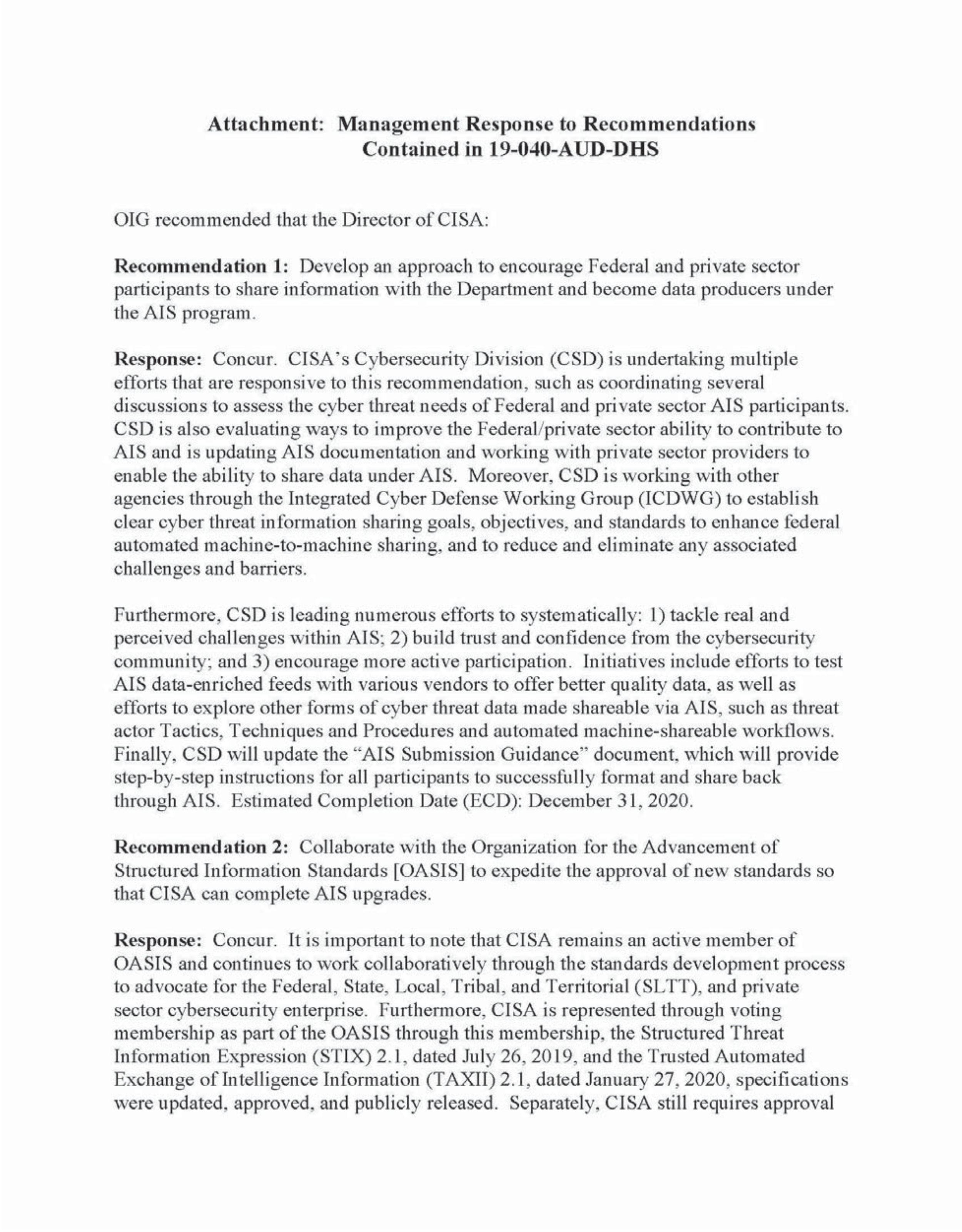
Thank you for the opportunity to comment on this draft report. The Cybersecurity and Infrastructure Security Agency (CISA) appreciates the work of the Office of Inspector General (OIG) in planning and conducting its review and issuing this report.

CISA notes OIG's recognition that CISA has made progress by addressing the basic information sharing requirements of the Cybersecurity Act of 2015. CISA also remains committed to improving the overall quality of information it shares with Automated Indicator Sharing (AIS) participants, as well as mitigating evolving security threats and vulnerabilities to the Nation's systems and networks.

The draft report contained four recommendations, with which CISA concurs. Attached find our detailed response to each recommendation. CISA previously submitted technical comments 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.

Attachment



**Attachment: Management Response to Recommendations Contained in 19-040-AUD-DHS**

OIG recommended that the Director of CISA:

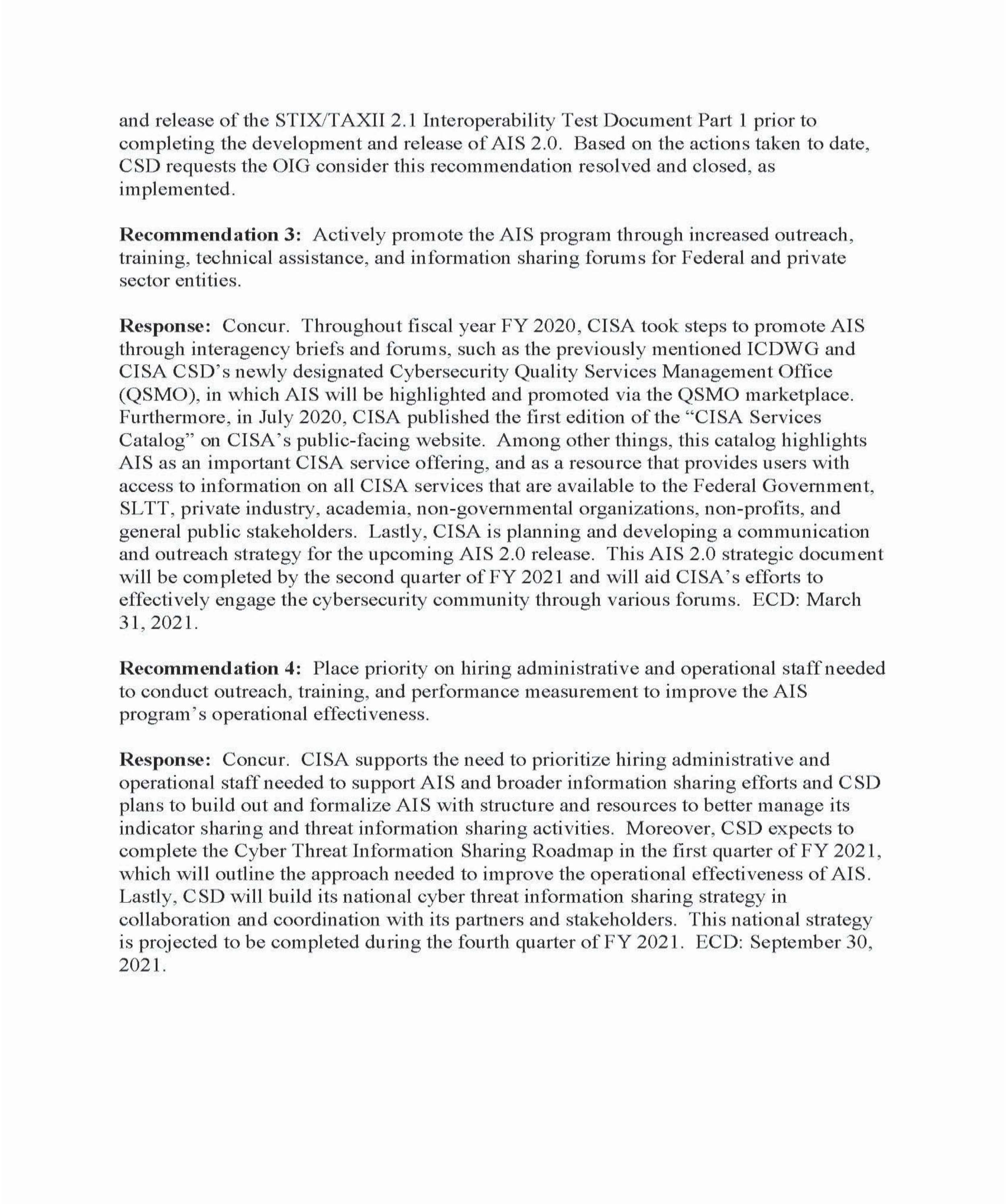
**Recommendation 1:** Develop an approach to encourage Federal and private sector participants to share information with the Department and become data producers under the AIS program.

**Response:** Concur. CISA's Cybersecurity Division (CSD) is undertaking multiple efforts that are responsive to this recommendation, such as coordinating several discussions to assess the cyber threat needs of Federal and private sector AIS participants. CSD is also evaluating ways to improve the Federal/private sector ability to contribute to AIS and is updating AIS documentation and working with private sector providers to enable the ability to share data under AIS. Moreover, CSD is working with other agencies through the Integrated Cyber Defense Working Group (ICDWG) to establish clear cyber threat information sharing goals, objectives, and standards to enhance federal automated machine-to-machine sharing, and to reduce and eliminate any associated challenges and barriers.

Furthermore, CSD is leading numerous efforts to systematically: 1) tackle real and perceived challenges within AIS; 2) build trust and confidence from the cybersecurity community; and 3) encourage more active participation. Initiatives include efforts to test AIS data-enriched feeds with various vendors to offer better quality data, as well as efforts to explore other forms of cyber threat data made shareable via AIS, such as threat actor Tactics, Techniques and Procedures and automated machine-shareable workflows. Finally, CSD will update the "AIS Submission Guidance" document, which will provide step-by-step instructions for all participants to successfully format and share back through AIS. Estimated Completion Date (ECD): December 31, 2020.

**Recommendation 2:** Collaborate with the Organization for the Advancement of Structured Information Standards [OASIS] to expedite the approval of new standards so that CISA can complete AIS upgrades.

**Response:** Concur. It is important to note that CISA remains an active member of OASIS and continues to work collaboratively through the standards development process to advocate for the Federal, State, Local, Tribal, and Territorial (SLTT), and private sector cybersecurity enterprise. Furthermore, CISA is represented through voting membership as part of the OASIS through this membership, the Structured Threat Information Expression (STIX) 2.1, dated July 26, 2019, and the Trusted Automated Exchange of Intelligence Information (TAXII) 2.1, dated January 27, 2020, specifications were updated, approved, and publicly released. Separately, CISA still requires approval



and release of the STIX/TAXII 2.1 Interoperability Test Document Part 1 prior to completing the development and release of AIS 2.0. Based on the actions taken to date, CSD requests the OIG consider this recommendation resolved and closed, as implemented.

**Recommendation 3:** Actively promote the AIS program through increased outreach, training, technical assistance, and information sharing forums for Federal and private sector entities.

**Response:** Concur. Throughout fiscal year FY 2020, CISA took steps to promote AIS through interagency briefs and forums, such as the previously mentioned ICDWG and CISA CSD's newly designated Cybersecurity Quality Services Management Office (QSMO), in which AIS will be highlighted and promoted via the QSMO marketplace. Furthermore, in July 2020, CISA published the first edition of the "CISA Services Catalog" on CISA's public-facing website. Among other things, this catalog highlights AIS as an important CISA service offering, and as a resource that provides users with access to information on all CISA services that are available to the Federal Government, SLTT, private industry, academia, non-governmental organizations, non-profits, and general public stakeholders. Lastly, CISA is planning and developing a communication and outreach strategy for the upcoming AIS 2.0 release. This AIS 2.0 strategic document will be completed by the second quarter of FY 2021 and will aid CISA's efforts to effectively engage the cybersecurity community through various forums. ECD: March 31, 2021.

**Recommendation 4:** Place priority on hiring administrative and operational staff needed to conduct outreach, training, and performance measurement to improve the AIS program's operational effectiveness.

**Response:** Concur. CISA supports the need to prioritize hiring administrative and operational staff needed to support AIS and broader information sharing efforts and CSD plans to build out and formalize AIS with structure and resources to better manage its indicator sharing and threat information sharing activities. Moreover, CSD expects to complete the Cyber Threat Information Sharing Roadmap in the first quarter of FY 2021, which will outline the approach needed to improve the operational effectiveness of AIS. Lastly, CSD will build its national cyber threat information sharing strategy in collaboration and coordination with its partners and stakeholders. This national strategy is projected to be completed during the fourth quarter of FY 2021. ECD: September 30, 2021.

## Appendix C
## 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?

**Comment: To meet requirements of the Cybersecurity Act of 2015 (Public Law 114-113), DHS has implemented the Automated Indicator Sharing (AIS) program. AIS participants are Federal departments and agencies; state, local, tribal, and territorial governments; private sector entities; information sharing and analysis centers and organizations; and foreign entities. The Department shares unclassified cyber threat indicators and defensive measures through three data feeds:**

- **The AIS capability is for non-Federal entities that have signed the AIS Terms of Use, or are customers of AIS participants that are allowed to re-distribute the information.**
- **The CISCP distributes the cyber threat information to non-Federal entities that have signed the CISCP Cooperative Research and Development Agreement.**
- **FedGov shares cyber threat information with Federal departments and agencies that have signed the Multilateral Information Sharing Agreement.**

**DHS shares unclassified cyber threat indicators and defensive measure with Federal agencies through AIS, CISCP, and FedGov data feeds, and classified cyber threat indicators through the Enhanced Cybersecurity Services program. Through AIS, CISCP, and FedGov data feeds, the Department shared 1,445,960 unclassified indicators and defensive measures in 2017, and 4,032,918 in 2018.**

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

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

- **Federal Government Sharing Guidance – February 2016**
- **Non-Federal Entity Sharing Guidance (sec 105 (a)) – June 2016**
- **Operational Procedures (105) (a) – June 2016**

- **Privacy and Civil Liberties Guidelines - June 2018**
- **Automated Indicator Sharing (AIS) Brokering - July 2016**
- **Indicator Management Standard Operating Procedures - February 2017**
- **Cyber Threat Management – February 2017**
- **Intelligence Triage Process – February 2017**
- **Indicator Vetting Process – February 2017**
- **Cybersecurity Information Handling Guidelines – October 2018**

3. If the four procedure documents created as a result of CISA (CISA procedure documents) were not provided for question 2, is the agency aware of the documents? If they are aware of the CISA documents, why are they not used by the agency?

**Comment: Not applicable.**

4. If the agency uses policies, procedures, and guidelines different from the CISA procedure documents, do they 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?

**Comment: Yes.**

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?

**Comment: Yes.**

6. Are the agency's policies, procedures, and guidelines (only 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)? (Government Accountability Office report documents the sufficiency of the CISA procedure documents already)

**Comment: Yes.**

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

**Comment: Yes, Department officials believe the policies, procedures, and guidelines are sufficient. DHS has fulfilled the requirements mandated by Section 103 of the Cybersecurity Act of 2015.**

8. If there are differences in the policies, procedures, and guidelines implemented among the agencies (different from the CISA procedure documents), 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)

**Comment: None.**

## 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?

**Comment: Yes. DHS shares unclassified cyber threat indicators and defensive measures with the private sector through AIS and CISCP data feeds, and classified indicators and defensive measures via Enhanced Cybersecurity Services program. In total, DHS shared a total of 333,062 indicators in 2017, and 409,830 indicators in 2018.**

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

**Comment: Yes. 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. Via the Enhanced Cybersecurity Services program, the Department shared 673 classified indicators in 2017, and an additional 1,999 in 2018.**

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

**Comment: DHS has classified cyber threat indicators using derivative classification. Original classification of the cyber threat indicators remained with the Original Classification Authority. 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.

**Comment: After judgmentally selecting and reviewing 30 unclassified and 30 classified indicators, we determined the indicators were properly classified.**

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

**Comment: Yes.**

## Accounting of Security Clearances

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

**Comment: Yes. DHS granted 129 security clearances in 2017 and 155 in 2018 to private sector partners under various DHS information sharing programs. However, DHS does not track the number of security clearances issued under the Act. Since DHS shares unclassified cyber threat indicators via the AIS program, a security clearance is not required to receive this information.**

13. If yes, how did the agency account for the number of security clearances and how many security clearances were active in CYs 2017 and 2018?

**Comment: The Department maintains active security clearance information in its MS SharePoint application. DHS maintained 1,536 active security clearances in 2017 and 1,691 in 2018.**

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

**Comment: According to representatives we interviewed from selected private sector entities, most of their employees do not possess security clearances. These representatives did not identify security clearances as a barrier because DHS does not share classified information via the AIS program.**

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

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

**Comment: Yes, DHS has used cyber threat indicators shared by other Federal agencies such as the Department of Energy and National Security Agency.**

16. If yes to question 15, review a sample and determine whether the agency used and disseminated the shared cyber threat information appropriately? Provide results.

**Comment: Yes, 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.**

17. If yes to question 15, did the agency use the shared cyber threat information to mitigate potential threats? Please explain.

**Comment: Yes, DHS shares unclassified indicators via the AIS program to help Federal agencies protect their networks and improve their cybersecurity postures.**

## Sharing Cyber Threat Indicators and Defensive Measures with Other Federal Agencies

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

**Comment: Yes, DHS shares unclassified cyber threat indicators and defensive measures with 33 Federal departments and agencies participating in the AIS Program via AIS, CISCP, and FedGov data feeds.**

| |
|---|
| 19. 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. |
| **Comment: After obtaining a sample of indicators from the Department of State and General Services Administration, we traced the indicators back to the AIS capability. Yes, based on our interviews with the Nuclear Regulatory Commission, National Science Foundation, and Office of Personnel Management officials, DHS shared cyber threat indicators and defensive measures in a timely and adequate manner. 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.** |
| 20. With which Federal agencies and what capabilities or tools were used to share the cyber threat information? |
| **Comment: DHS shares cyber threat information with 33 Federal departments and agencies such as the Departments of Agriculture, Commerce, Defense, Education, Energy, Health and Human Services, Housing and Urban Development, Transportation, Treasury, and Veteran Affairs; National Aeronautics and Space Administration; National Science Foundation; and Nuclear Regulatory Commission. DHS uses Direct Connection (i.e., Splunk, DHS TAXII Client), Shared Service Connections (e.g., IID Threat Intelligence, Anomali), or both Direct Connection and Shared Service Connections to share cyber threat information.** |
| 21. Have other Federal entities shared cyber threat indicators and defensive measures with the agency? |
| **Comment: Yes, the Department of Energy and the National Security Agency shared into the AIS capability.** |
| 22. 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. |
| **Comment: We reviewed a sample of indicators and determined that they were received and shared in a timely, adequate, and appropriate manner. Yes, based on our interviews with selected Office of Personnel Management, National Regulatory Commission, and National Science Foundation personnel, cyber threat indicators and defensive measures were shared in a timely and adequate 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)** |
| 23. 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 2017 & 2018? Provide results. |

**Comment: DHS received 3,438,478 indicators in CY 2017, and 12,171,713 indicators in CY 2018.**

**Note: This number includes duplicative Indicators of Compromise, and Indicators of Compromise that were dropped. This number, by default, is higher than the unique number; but does not include DHS internal Indicators of Compromise as the Department also publishes to both AIS_INGEST and FedGov.**

24. How many of those cyber threat indicators and defensive measures reported for question 23 did Department of Homeland Security share with other Federal entities in 2017 & 2018? Provide results.

**Comment: The Department subsequently shared all 846,555 indicators received in CY 2017, and the 1,933,609 indicators received in CY 2018 to Federal entities.**

**Note: This number includes duplicative Indicators of Compromise, and Indicators of Compromise that were dropped. This number, by default, is higher than the unique number; but does not include DHS internal Indicators of Compromise as the Department also publishes to both AIS_INGEST and FedGov.**

## Cyber Threat Indicators and Defensive Measures Received from Other Federal Agencies

25. (Agencies other than DHS) How many cyber threat indicators and defensive measures did Department of Homeland Security relay to the agency via the AIS capability in 2017 & 2018? Provide results.

**Comment: Not applicable.**

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

**Comment: Not applicable.**

## Personal Information Violations

27. 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)?

**Comment: No. According to DHS officials, there has been no PII violation since the inception of the AIS Program in March 2016. To ensure no personal information is released, DHS implemented controls in the AIS capability to remove for additional review any free text that may contain potential PII. DHS uses human review to redact any PII and subsequently send the approved information through the AIS capability.**

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

**Comment: Not applicable.**

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

**Comment: None.**

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

**Comment: Not applicable.**

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

**Comment: None.**

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

**Comment: Not applicable.**

33. 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?

**Comment: None.**

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

**Comment: Not applicable.**

## Potential Barriers

35. 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.

**Comment: A lack of information sharing and input from program participants is the main barrier to DHS improving the quality of indicators it shares via the AIS capability. Representatives we interviewed from agencies included in our review provided various reasons for not sharing indicators with the Department, such as small staff and limited resources to adequately perform their cyber functions. These representatives believed dedicated time and resources were needed to share their indicators with the Department via AIS. Because of limited sharing and input from its partners, DHS does not receive the quality and quantitative data needed to enrich the indicators with more actionable information to mitigate potential cyber threats.**

35a. Any difficulties with using a specific capability or tool to share and/or receive cyber threat information?

**Comment: Based on our interviews, some agency and private sector personnel informed us that they do not understand how to share their**

**indicators with DHS through the AIS capability. Architectural changes to the AIS capability have also caused some issues for some Federal agencies. Organization for the Advancement of Structured Information Standards and DHS are upgrading to AIS 2.0 to address these technical issues. DHS also uses its Homeland Security Information Network portal to share enriched cyber threat indicators with various critical infrastructure and key resource communities of interest. However, representatives from selected private sector companies we spoke with stated that the Homeland Security Information Network was difficult to navigate because of the different sector communities it serves. As a result, it is a challenge to correlate information to obtain a comprehensive understanding of a specific indicator.**

35b. Any difficulties due to classification of information?

**Comment: No, DHS AIS capability does not share classified information.**

35c. Any difficulties due to a reluctance to sharing information?

**Comment: No Federal entities stated they were reluctant to share information.**

35d Any difficulties due to the number of cyber threat indicators and defensive measures received? Too many to ingest and review?

**Comment: Smaller agencies did not have the manpower to sift through the large number of indicators they received via the AIS capability.**

35e. Any issues with the quality of the information received?

**Comment: Based on our interviews, AIS participant opinions were mixed. Some Federal agency officials and private sector representatives told us that AIS indicators lacked contextual information to make them actionable. They said DHS must enrich the indicators to make them effective before distribution. To further illustrate, according to DHS Chief Information Security Officer personnel, their office ingests AIS indicators after a third party enriches them. Several Federal agency officials told us the Department has improved its data and this information is very helpful.**

35f. Has the agency performed any steps to mitigate the barriers identified?

**Comment: DHS plans to upgrade the AIS capability to share more enriched information. Organization for the Advancement of Structured Information Standards will release new Structured Threat Information eXchange (STIX) and Trusted Automated eXchange of Indicator Information (TAXII) standards to improve data enrichment and trend correlation. Once the new standards are released, it will take the DHS 90 days to migrate to AIS 2.0.**

36. 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)] Also, see procedure document, Sharing of Cyber Threat Indicators and Defensive Measures by the Federal

Government under CISA, on Periodic Sharing of Cybersecurity Best Practices, which includes some best practices from Department of Commerce, DHS, Defense Industrial Base Critical Sector, Federal Bureau of Investigation, and National Security Agency.

**Comment: DHS has developed the *AIS Engagement Action Plan* to identify and recruit targeted partners, and help entities that are not sharing information with DHS overcome their hurdles through a series of AIS webinars.**

37. 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? Also, see procedure document, Sharing of Cyber Threat Indicators and Defensive Measures by the Federal Government under CISA, which lists some sharing programs from DHS, Defense Industrial Base Critical Sector, Federal Bureau of Investigation, Department of Energy, and Treasury.

**Comment: DHS uses the AIS capability, the Homeland Security Information Network portal, and email to share and receive cyber threat indicators. The tools/capabilities provide the necessary information; however, as CISA management acknowledges the upgraded AIS version will enrich/enhance the information shared and possibly address the concerns of the participants.**

38. Does the agency share or receive unclassified cyber threat information from Intelligence Community Analysis and Signature Tool? If not, what issues is the agency having with adoption of the Intelligence Community Analysis and Signature Tool and sharing threat indicator data via the capability either manually or through a feed? (funding issues, system incompatibility, lack of information)

**Intelligence Community Analysis and Signature Tool is an open source tool managed by the Intelligence Community Security Coordination Center that receives and shares cyber threat indicators and defensive measures. Intelligence Community Analysis and Signature Tool has the ability to share both classified and unclassified cyber threat information with the agencies. The agencies can receive information by directly logging into the system or through a hub and spoke setup with its own Intelligence Community Analysis and Signature Tool or other indicators of compromise/cyber threat indicator platform.

**Comment: No, according to National Cybersecurity and Communication Integration Center officials, they are working with the AIS capability and the Intelligence Community Analysis and Signature Tool to establish bi-directional connection. This connection will provide an unclassified pipeline of indicators to the Intelligence Community Analysis and Signature Tool, enabling the tool to pass identified unclassified indicators and context to the classified network. In addition, CISA officials emphasized that the**

**Intelligence Community Analysis and Signature Tool and the AIS capability have two distinctly different purposes. The Intelligence Community Analysis and Signature Tool focuses on comparing unclassified indicators with classified information. The AIS capability program serves as a brokerage of information on unclassified networks and shares cyber threat information broadly with Federal entities and the private sector.**

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

**Comment: Yes, in June 2018, DHS and the heads of the appropriate Federal entities jointly updated the Privacy and Civil Liberties Final Guidelines: The Cybersecurity Information Sharing Act of 2015.**

## Appendix D
## Major Contributors to This Report

Tarsha Cary, Director
Yusuf Lane, IT Auditor
Stefanie Holloway, IT Auditor
Michael Gigas, Program Analyst
Zachary Israel, IT Auditor
Jane DeMarines, Communications Analyst
Kathy Hughes, Referencer

# 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
Assistant Director, Cybersecurity Division, Cybersecurity and Infrastructure Agency (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