



Office of the Inspector General of the Intelligence Community

Joint Report on the Implementation of the Cybersecurity Information Sharing Act of 2015

December 19, 2017



Important Notice

(U) This report contains information that the Office of the Inspector General of the Intelligence Community has determined is confidential, sensitive, or protected by Federal Law, including protection from public disclosure under the Freedom of Information Act (FOIA) 5 USC § 552. Recipients may not further disseminate this information without the express permission of the Office of the Inspector General of the Intelligence Community personnel. Accordingly, the use, dissemination, distribution, or reproduction of this information to or by unauthorized or unintended recipients may be unlawful. Persons disclosing this information publicly or to others not having an official need to know are subject to possible administrative, civil, and/or criminal penalties. This report should be safeguarded to prevent improper disclosure at all times. Authorized recipients who receive requests to release this report should refer the requestor to the Office of the Inspector General of the Intelligence Community.



OFFICE OF THE INSPECTOR GENERAL OF THE INTELLIGENCE COMMUNITY
AUDIT DIVISION
WASHINGTON, DC 20511

ES-2017-01002

MEMORANDUM FOR: See Distribution

SUBJECT: Report No. AUD-2017-005, Joint Report on the
Implementation of the Cybersecurity Information Sharing
Act of 2015, December 19, 2017

We are providing this final report for your information and use. Our objective was to provide a joint report on actions taken during calendar year 2016 to carry out the Cybersecurity Information Sharing Act of 2015 (CISA) requirements.

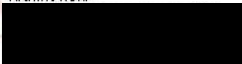
On December 18, 2015, Congress passed the Consolidated Appropriations Act of 2016, including Title I – CISA. CISA Section 107(b) requires the Inspectors General of the Office of the Director of National Intelligence and the Departments of Commerce, Defense, Energy, Homeland Security, Justice, and Treasury to jointly report to Congress on actions taken over the most recent two-year period to carry out the CISA requirements. Each of the Offices of Inspectors General obtained the required assessments on its agency’s implementation of the CISA requirements and provided the results to us. We compiled the results in this report.

We also provided a discussion draft of this report to the participating Offices of Inspectors General and the Council of Inspectors General on Financial Oversight, and we incorporated their comments when preparing the final report.

We appreciate the courtesies extended to our staff throughout this review. Please direct questions related to this report to the Inspector General of the Intelligence Community at (571) 204-8149.

Mark A.
Krulikowski

Digitally signed by Mark A.
Krulikowski



12/19/17

Mark A. Krulikowski
Assistant Inspector General for Audit (Acting)
Office of the Inspector General
of the Intelligence Community

Date

FREDERICK
MENY

Digitally signed by FREDERICK
MENY



12/18/17

Frederick J. Meny Jr.
Assistant Inspector General for Audit
and Evaluation (Acting)
U.S. Department of Commerce Office
of Inspector General

Date

GORMAN.CAROL.N
ATALIE.

Digitally signed by
GORMAN.CAROL.NATALIE



12/18/17

Carol N. Gorman
Assistant Inspector General for Readiness
and Cyber Operations
Department of Defense Office
of Inspector General

Date

Sarah B. Nelson

Digitally signed by Sarah B.
Nelson



12/18/17

Sarah B. Nelson
Assistant Inspector General for Audits
and Administration
Department of Energy Office
of Inspector General

Date

SONDRA F
MCCAULEY

Digitally signed by SONDRA F. MCCAULEY




12/18/17

Sondra F. McCauley
Assistant Inspector General for
Information Technology Audits
Department of Homeland Security Office
of Inspector General

Date

JASON
MALMSTROM

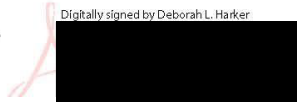
Digitally signed by JASON MALMSTROM


12/18/17

Jason R. Malmstrom
Assistant Inspector General for Audit
Department of Justice Office
of the Inspector General

Date

Deborah L.
Harker

Digitally signed by Deborah L. Harker


12/18/17

Deborah L. Harker
Assistant Inspector General for Audit
Department of the Treasury Office
of Inspector General

Date

Distribution:

Director, National Intelligence
Secretary of Commerce
Secretary of Defense
Secretary of Energy
Secretary of Homeland Security
Attorney General, Department of Justice
Secretary of the Treasury
The Honorable Richard Burr
The Honorable Mark Warner
The Honorable Devin Nunes
The Honorable Adam Schiff
The Honorable John Culberson
The Honorable Jose Serrano
The Honorable Kay Granger
The Honorable Peter J. Visclosky
The Honorable Mike Simpson
The Honorable Marcy Kaptur
The Honorable Tom Graves
The Honorable Mike Quigley
The Honorable John Carter
The Honorable Lucille Roybal-Allard
The Honorable Mac Thornberry
The Honorable Adam Smith
The Honorable Greg Walden
The Honorable Frank Pallone
The Honorable Bob Goodlatte
The Honorable Jerry Nadler
The Honorable Jeb Hensarling
The Honorable Maxine Waters
The Honorable Michael McCaul
The Honorable Bennie Thompson
The Honorable Trey Gowdy
The Honorable Elijah Cummings
The Honorable Lamar Smith
The Honorable Eddie Bernice Johnson
The Honorable Richard Shelby
The Honorable Jeanne Shaheen
The Honorable Thad Cochran
The Honorable Richard Durbin
The Honorable Lamar Alexander
The Honorable Dianne Feinstein

The Honorable Shelley Moore Capito
The Honorable Christopher Coons
The Honorable John Boozman
The Honorable Jon Tester
The Honorable John McCain
The Honorable Jack Reed
The Honorable John Thune
The Honorable Bill Nelson
The Honorable Lisa Murkowski
The Honorable Maria Cantwell
The Honorable Orrin Hatch
The Honorable Ron Wyden
The Honorable Ron Johnson
The Honorable Claire McCaskill
The Honorable Chuck Grassley

Executive Summary

Objective

Our objective was to provide a joint report on actions taken during calendar year 2016 to carry out the Cybersecurity Information Sharing Act of 2015 (CISA) requirements. Specifically, we are reporting on the appropriate Federal entities' assessments of:

- The sufficiency of policies and procedures related to sharing cyber threat indicators within the Federal Government;
- Whether cyber threat indicators or defensive measures have been properly classified and an accounting of the security clearances authorized by the Federal Government for the purpose of sharing with the private sector;
- The actions taken by the Federal Government based on cyber threat indicators or defensive measures shared with the Federal Government;
- The cyber threat indicators or defensive measures shared with the appropriate Federal Government entities; and
- The sharing of cyber threat indicators or defensive measures within the Federal Government to identify barriers to sharing information.

Background

On December 18, 2015, Congress passed the Consolidated Appropriations Act of 2016, including Title I – CISA. CISA Section 107(b) requires the Inspectors General of the Office of the Director of National Intelligence and the Departments of Commerce, Defense, Energy, Homeland Security, Justice, and Treasury, in consultation with the Inspector General of the Intelligence Community and the Council of Inspectors General on Financial Oversight, to jointly report to Congress on actions taken over the most recent two-year period to carry out the CISA requirements.

Results

Each Office of Inspector General independently obtained the required assessments on its agency's implementation of the CISA requirements and provided the results to us. We compiled the results in this report. We provided a discussion draft of this report to the participating Offices of Inspectors General and the Council of Inspectors General on Financial Oversight for their review and comment.

Table of Contents

Executive Summary7

Table of Contents8

Introduction.....9

 Objective..... 9

 Background..... 9

 Scope and Methodology 10

Consolidated OIG Responses.....12

 A. Sufficiency of Policies and Procedures..... 12

 B. Classification and Accounting 14

 C. Actions Taken 15

 D. Sharing Cyber Threat Indicators and Defensive Measures..... 20

 E. Inappropriate Barriers 25

Acronyms28

Introduction

Objective

Our objective was to provide a joint report to Congress on the actions taken during calendar year (CY) 2016 to carry out the Cybersecurity Information Sharing Act of 2015 (CISA) requirements. Specifically, we are reporting on the appropriate Federal entities' assessments of:

- The sufficiency of policies and procedures related to sharing cyber threat indicators within the Federal Government;
- Whether cyber threat indicators or defensive measures have been properly classified and an accounting of the security clearances authorized by the Federal Government for the purpose of sharing with the private sector;
- The actions taken by the Federal Government based on cyber threat indicators or defensive measures shared with the Federal Government;
- The cyber threat indicators or defensive measures shared with the appropriate Federal Government entities; and
- The sharing of cyber threat indicators or defensive measures within the Federal Government to identify barriers to sharing information.

Background

CISA, Section 103, requires the Director of National Intelligence, the Secretary of Homeland Security, the Secretary of Defense, and the Attorney General, in consultation with the heads of the appropriate Federal entities, to jointly develop and issue procedures to facilitate and promote the timely sharing of classified and unclassified cyber threat indicators and defensive measures with Federal and non-Federal entities.¹ Such procedures should ensure the real-time sharing of cyber threat indicators and defensive measures, while protecting classified information; protecting against unauthorized access to the cyber threat information;² and ensuring Federal entities identify and remove any personally identifiable information (PII) not directly related to a cybersecurity threat included in the cyber threat indicator prior to sharing. CISA also includes requirements regarding:

- Authorizations for preventing, detecting, analyzing, and mitigating cybersecurity threats (Section 104);
- Development and implementation of a capability and process within the Department of Homeland Security (DHS) for non-Federal entities to provide cyber threat indicators and defensive measures (Section 105);

¹ The Consolidated Appropriations Act, 2016, Pub. L. No. 114-113, Div. N., § 103 (b), 129 Stat. 2940 (2015); 6 U.S.C. §1502(b).

² In this joint report, we use the term, cyber threat information, to summarize cyber threat indicators and defensive measures.

- Protections from liability for sharing or receiving cyber threat indicators or defensive measures in accordance with CISA (Section 106);
- Oversight of Government activities pertaining to the implementation of CISA (Section 107);
- Lawful disclosures (Section 108); and
- Report on cybersecurity threats (Section 109).³

CISA defines a cyber threat indicator as information that describes or identifies a security vulnerability, method of defeating a security control or exploiting a security vulnerability, malicious cyber command, results of a cybersecurity threat, or any other attribute of a cybersecurity threat.⁴ CISA defines a defensive measure as an action, device, procedure, signature, technique, or other measure applied to an information system that detects, prevents, or mitigates a known or suspected cybersecurity threat.⁵

CISA, Section 107(b),⁶ requires the Inspectors General of the appropriate Federal entities,⁷ in consultation with the Inspector General of the Intelligence Community and the Council of Inspectors General on Financial Oversight,⁸ to jointly report to Congress on the actions taken over the most recent two-year period to carry out the CISA requirements.

Scope and Methodology

We prepared questions that addressed the CISA Section 107(b) requirements and requested that the Offices of Inspectors General (OIGs) for the appropriate Federal entities respond. The OIGs obtained the responses to the questions from their respective entities and submitted the results to us.

We requested that the OIGs provide their respective entities' assessments on the actions taken in CY 2016 to implement CISA. Congress passed CISA in December 2015, requiring the OIGs to submit the first joint report by December 2017. We did not include CY 2015 in our scope because CISA was passed at the end of CY 2015 and the joint report was required to reflect the implementation of CISA. However, some OIGs provided responses covering additional periods. ODNI, DoD, Energy, and Justice OIGs provided responses for CY 2016. Commerce OIG provided responses for December 2015 through July 2017. DHS OIG provided responses for October 2015 through June 2017. Treasury OIG provided responses for CYs 2015 and 2016.

³ See 6 U.S.C. §§ 1503 – 1508.

⁴ See 6 U.S.C. § 1501(a)(6).

⁵ See 6 U.S.C. § 1501(a)(7).

⁶ See 6 U.S.C. § 1506(b); “Biennial Report on Compliance.”

⁷ CISA defines “appropriate Federal entities” as the Office of the Director of National Intelligence (ODNI), Department of Commerce (Commerce), Department of Defense (DoD), Department of Energy (Energy), DHS, Department of Justice (Justice), and the Department of the Treasury (Treasury).

⁸ The Council of Inspectors General on Financial Oversight is comprised of nine financial regulatory agency Inspectors General and chaired by the Inspector General, U.S. Department of Treasury. Council members share information regarding their ongoing work and focus on concerns that may apply to the broader financial sector and ways to improve financial oversight.

This joint report establishes a baseline for the December 2019 joint report, which will cover the two-year period for CYs 2017 and 2018.

The OIG representatives for the appropriate entities discussed whether CISA applies only to using the DHS Automated Indicator Sharing (AIS) system. DHS developed the AIS system to comply with CISA Section 105(c) requirement for a capability to accept cyber threat information from non-Federal entities. The OIGs did not come to a consensus on whether we should include information in this joint report specific to the AIS system or whether we should include all cyber threat information shared and received using any mechanism. Consequently, the OIGs provided responses pertaining to all mechanisms used by the entities to share and receive cyber threat indicators and defensive measures, except for the NSA. NSA limited its responses based on its interpretation that activities under CISA are limited to sharing carried out through the AIS system or through the other aspects of the DHS portal, which accepts submissions by email and other means.

We compiled the responses from the OIGs provided by ten Federal entities⁹ regarding the implementation of CISA. We briefed the Council of Inspectors General on Financial Oversight on the results and status of the report and provided them a discussion draft of this report for their consultation. We also provided the participating OIGs a discussion draft of this report for their review and comment. We incorporated the comments we received into the final report.

⁹ The DoD Office of the Inspector General (DoD OIG) identified four DoD components that share or receive cyber threat indicators or defensive measures. The Office of the Chief Information Officer and DoD Cyber Crime Center (DoD CIO and DC3), the National Security Agency (NSA), and the U.S. Cyber Command (USCYBERCOM) are three Federal cybersecurity centers whose mission includes cybersecurity information sharing. The fourth component, the Defense Information Systems Agency (DISA), is a Combat Support Agency that provides, operates, and assures information-sharing capabilities in direct support to joint warfighters, national-level leaders, and other mission and coalition partners. According to DoD OIG officials, together the four components work to protect the DoD Information Network. As such, we reported DoD as four separate entities in this joint report in addition to the other six entities required to report by CISA: ODNI, Commerce, Energy, DHS, Justice, and Treasury, for a total of ten entities. Note that the DoD CIO provides policy and program oversight for DC3's implementation of the Defense Industrial Base Cyber Security Program. For the purpose of the joint report, DoD CIO and DC3 were considered one entity.

Consolidated OIG Responses

The OIGs provided responses to our questions on their entities' assessments of their implementation of CISA requirements. Specifically, the responses addressed the:

- A. Sufficiency of policies and procedures related to sharing cyber threat indicators within the Federal Government;
- B. Classification of cyber threat indicators and defensive measures, and an accounting of the security clearances for the purpose of sharing with the private sector;
- C. Actions taken based on shared cyber threat indicators or defensive measures;
- D. Cyber threat indicators and defensive measures shared with Federal entities; and
- E. Any barriers to sharing information among Federal entities.

A. Sufficiency of Policies and Procedures

CISA Section 107(b) requires that this joint report include the following information from each of the OIGs:

An assessment of the sufficiency of policies and procedures related to sharing cyber threat indicators within the Federal Government, including the policies, procedures, and guidelines relating to the removal of information not directly related to a cybersecurity threat that is personal information of a specific individual or information that identifies a specific individual.

We developed four questions to assist the entities in assessing the sufficiency of their policies and procedures:

1. Does your agency have policies, procedures, and guidelines for sharing cyber threat indicators within the Federal Government? Please list.
2. Do these 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? Please provide title of policy, procedure, or guidance.
3. Are the policies, procedures, and guidelines for sharing cyber threat indicators within the Federal Government sufficient?
4. How did your agency determine sufficiency?

The OIGs responded that eight of the ten entities – ODNI, Commerce, DoD CIO and DC3, NSA, Energy, DHS, Justice, and Treasury – provided the policies, procedures, or guidelines their entities used to share cyber threat indicators within the Federal Government and determined they were sufficient. DoD OIG responded that the remaining two entities – DISA and USCYBERCOM – did not identify policies, procedures, or guidelines for sharing cyber threat information.

For those eight entities, the OIGs responded that Commerce, DoD CIO and DC3, NSA, Energy, DHS, and Justice stated that their policies, procedures, or guidelines contain guidance on the removal of personally identifiable information (PII). ODNI indicated that its policies do not provide guidance on the removal of PII because it does not receive cyber threat information with PII. Treasury responded that its policy does not contain guidance specific to removing PII but stated a shared report generally should not contain names, roles, or offices of Treasury targets.

Table 1 summarizes the entities' responses.

Table 1. Entities' Responses on Sufficiency of Guidance for Sharing Cyber Threat Indicators

Entity	Entity Provided Guidance for Sharing Cyber Threat Indicators	Entity Indicated Guidance Addressed Removing PII	Entity Assessed Guidance as Sufficient
ODNI	yes	no	yes
Commerce	yes	yes	yes
DoD	DISA	no	
	DoD CIO and DC3	yes	yes
	NSA	yes	yes
	USCYBERCOM	no	
Energy	yes	yes	yes
DHS	yes	yes	yes
Justice	yes	yes	yes
Treasury	yes	no	yes

For the eight entities that provided policies, procedures, or guidelines, the OIGs provided the following responses on how the entities determined the sufficiency of their guidance:

- ODNI, DoD CIO and DC3, and NSA determined their guidance was sufficient because it did not inhibit the timely sharing of cyber threat indicators;
- Energy, DHS, and Justice determined sufficiency based on a review of their guidance;
- Commerce determined sufficiency based on its evaluation of the “consistency of the syntax and format” of the shared threat information and because Commerce “participate[s] in AIS, as required by Federal guidelines”; and

- Treasury determined its guidance was sufficient because it had used the guidance for more than five years and the basic principles have been consistent, well established, and understood. The guidance needed only minor adjustments to incorporate emerging new agreements and sharing mechanisms.

B. Classification and Accounting

CISA Section 107(b) requires the joint report to include the following information from each of the OIGs:

An assessment of whether cyber threat indicators and defensive measures have been properly classified and an accounting of the number of the security clearances authorized by the Federal Government for the purpose of sharing cyber threat indicators or defensive measures with the private sector.

We developed four questions to assist the entities in assessing whether they properly classified shared cyber threat indicators and defensive measures and had an accounting of security clearances:

1. Has your agency shared cyber threat indicators and defensive measures with the private sector?
2. Did your agency properly classify the cyber threat indicators and defensive measures shared with the private sector?
3. How did your agency determine whether the shared cyber threat indicators and defensive measures were properly classified?
4. How does your agency account for the number of security clearances authorized for sharing cyber threat indicators and defensive measures with the private sector?

Sharing and Classifying Cyber Threat Information. The OIGs responded that six of the ten entities – DoD CIO and DC3, USCYBERCOM, Energy, DHS, Justice, and Treasury – stated that they shared cyber threat information with the private sector and properly classified the information.

- DoD CIO and DC3, USCYBERCOM, Energy, and DHS indicated they classify threat information using classification manuals, guides, and personnel.
- Treasury indicated it uses unclassified methods, and all cyber threat indicators and defensive measures shared with the private sector via trusted communities are unclassified.
- Justice responded that it only shares unclassified cyber threat information with the private sector.

The OIGs responded that the remaining four entities – ODNI, Commerce, DISA, and NSA – reported that they did not share cyber threat indicators or defensive measures with the private sector.

Accounting for Security Clearances. The OIGs responded that two of the ten entities – Energy and DHS – indicated they accounted for security clearances authorized for the purpose of sharing cyber threat indicators and defensive measures with the private sector. According to the OIGs:

- Energy officials commented that they accounted for security clearances by reviewing monthly reports from DHS on energy sector clearance holders.
- DHS reported accounting for security clearances using a security clearance database.

The OIGs responded that seven of the ten entities – ODNI, Commerce, DISA, DoD CIO and DC3, NSA, Justice, and Treasury – stated they did not account for security clearances authorized for the purpose of sharing cyber threat indicators and defensive measures with the private sector.

- ODNI and DoD CIO and DC3 indicated they do not issue security clearances for sharing cyber threat information with the private sector.
- Commerce and DISA reported that they do not share cyber threat information with the private sector.
- NSA reported that it did not issue security clearances to the private sector because it does not share cyber threat indicators or defensive measures with the private sector.
- Justice responded that DHS is responsible for vetting security clearances for CISA participants.
- Treasury stated that security clearances are not required because it only shares unclassified cyber threat information. While Treasury may receive classified cyber threat information from outside sources, it does not redistribute them.

DoD OIG responded that the remaining entity, USCYBERCOM, stated it did not provide information on how it accounts for the number of security clearances authorized for sharing cyber threat indicators and defensive measures with the private sector.

C. Actions Taken

CISA Section 107(b) requires this joint report to include the following information from each of the OIGs:

A review of the actions taken by the Federal Government based on cyber threat indicators or defensive measures shared with the Federal Government under this title, to include a review of the following:

- i. **The appropriateness of subsequent uses and disseminations of cyber threat indicators or defensive measures.**
- ii. **Whether cyber threat indicators or defensive measures were shared in a timely and adequate manner with appropriate entities, or, if appropriate, made publicly available.**

We developed seven questions to assist the entities with their reviews. Three questions addressed the appropriateness of subsequent uses and dissemination, and four questions addressed whether the entities shared cyber threat indicators or defensive measures timely and adequately.

Subsequent Uses and Dissemination

1. Has your agency used and disseminated cyber threat indicators and defensive measures shared by other Federal agencies?
2. Did your agency use and disseminate the shared cyber threat indicators and defensive measures appropriately?
3. How did your agency determine if the use and dissemination of shared cyber threat indicators and defensive measures was appropriate?

The OIGs responded that nine of the ten entities – ODNI, Commerce, DISA, DoD CIO and DC3, USCYBERCOM, Energy, DHS, Justice, and Treasury – reported using and disseminating shared cyber threat indicators and defensive measures appropriately. The remaining entity, NSA reported it did not use or disseminate any cyber threat indicators or defensive measures shared by other Federal agencies.

The OIGs responded that the nine entities – ODNI, Commerce, DISA, DoD CIO and DC3, USCYBERCOM, Energy, DHS, Justice, and Treasury – that reported using and disseminating shared cyber threat indicators and defensive measures appropriately also provided explanations on how they determined appropriate use or dissemination.

Table 2 summarizes the responses on how they determined appropriate use or dissemination of shared cyber threat information.

Table 2. Entities’ Responses on Determining Whether Cyber Threat Information Use and Dissemination Was Appropriate

Entity	Responses on How Entities Determined Whether Use and Dissemination of Cyber Threat Information Was Appropriate
ODNI	ODNI determined that all cyber threat indicators received from other Federal agencies were specific to actual threat vectors and did not include PII. ODNI disseminated cyber threat information tied directly to specific technical defensive measures and that did not contain PII. In addition, ODNI provided information only on a “need to know” basis, and sharing information has not resulted in any information compromise.

Entity		Responses on How Entities Determined Whether Use and Dissemination of Cyber Threat Information Was Appropriate
	Commerce	Commerce indicated that any use of cyber threat information was appropriate if it enhanced situational awareness. In addition, it considers all cyber information from DHS as valuable for protecting its systems and information.
DoD	DISA	DISA determined the validity and impact of the cyber threat report contents and “implements appropriate mitigations.”
	DoD CIO and DC3	DoD CIO and DC3 shared cyber threat information in accordance with the caveats associated with handling the information, and disseminated only the information approved to be released to the Defense Industrial Base cyber security program participants.
	USCYBERCOM	USCYBERCOM leveraged liaison officers and 24/7 cyber operation center collaboration efforts to assess the use and dissemination of shared cyber threat information.
	Energy	Energy received cyber indicators from the AIS system, and nothing came to their attention to indicate they did not appropriately use and disseminate cyber threat indicators and defensive measures.
	DHS	DHS described using a protocol with a set of designations to ensure that sensitive information is shared with the appropriate audience and facilitates the sharing of information.
	Justice	Justice obtained cyber threat information through the AIS system and followed CISA Privacy and Civil Liberties Guidelines, which address the appropriate use and dissemination of cyber threat indicators.
	Treasury	Treasury followed guidance provided in the “Enhance Shared Situational Awareness Multilateral Information Sharing Agreement,” March 2015, established by multiple Federal agencies to enhance cybersecurity information sharing among Federal agencies. In addition, Treasury does not re-disseminate classified cyber threat information received from other organizations.

Sharing Cyber Threat Information

1. Has your agency shared cyber threat indicators and defensive measures with other Federal agencies?
2. Did your agency share the cyber threat indicators and defensive measures in a timely and adequate manner with appropriate entities or, if appropriate, made publicly available?
3. Have other Federal entities shared cyber threat indicators and defensive measures with your agency in a timely, adequate, and appropriate manner?
4. How did your agency determine timeliness, adequacy, and appropriateness of sharing the information?

The OIGs responded that all ten entities reported sharing cyber threat indicators or defensive measures in a timely and adequate manner with appropriate entities. In addition, all the entities except NSA reported that other Federal entities shared cyber threat information with their entity in a timely, adequate, and appropriate manner. NSA did not respond whether other Federal entities shared cyber threat information in a timely, adequate, and appropriate manner.

According to the OIGs, the entities' responses to determining the timeliness, adequacy, and appropriateness of sharing cyber threat information varied. Some entities expressed challenges with determining timeliness. Specifically:

- ODNI responded that timeliness is difficult to define and measure because it is dependent on the cyber attack. Complex attacks require more time to identify indicators.
- DoD CIO and DC3 stated that all actionable information is shared in a timely manner. However, information sharing is not timely when the information is no longer actionable or when release approval for sensitive indicators requires interagency de-confliction.
- Treasury stated that it believed other Federal entities shared cyber threat information in a timely, adequate, and appropriate manner. However, it noted that there was no easy way to categorize reporting received, short of an extensive time-consuming manual review. Some cyber threat reports received did not include discovery time; therefore, making it impossible to know whether the information was shared in a timely, adequate, and appropriate manner. Treasury noted that the trouble was not necessarily sharing bad indicators, but not being able to distinguish which received indicators were good or bad without intensive manual processes, which reduced the usefulness of automated sharing.

Table 3 summarizes the ten entities' responses on how they determined the timeliness, adequacy, and appropriateness of sharing cyber threat information.

Table 3. Entities' Responses on Determining Whether Information Sharing Was Timely, Adequate, and Appropriate

Entity		Responses on How Entities Determined Timely, Adequate, and Appropriate Information Sharing
	ODNI	ODNI was not aware of any mission impacts due to untimely, inadequate, or inappropriate sharing of cyber threat information.
	Commerce	Commerce used OMB guidance to determine timeliness and vetted cyber threat information for adequacy and appropriateness through analysts before sharing.
DoD	DISA	DISA stated that it does not have a prescribed methodology; individual analysts make judgment calls.
	DoD CIO and DC3	DoD CIO and DC3 reviewed the date of information within the source report and researched the threat information to determine whether the information is actionable and relevant to Defense Industrial Base cyber security program participants.
	NSA	NSA provided cyber threat indicators to DHS weekly and determined that it adequately shared cyber threat information because the AIS system allows NSA to share in "an automated way." In addition, NSA determined that it shared appropriately because the unclassified, shared information was tied to malicious cyber activity that could threaten other networks.
	USCYBERCOM	USCYBERCOM ensured constant communication and collaboration efforts with its liaison officer, 24/7 cyber operation centers, and cyber partners.
	Energy	Energy downloaded cyber threat information every 15 minutes. DHS contractors were working to resolve network performance problems related to latency. Energy officials believed the information shared was adequate and appropriate because nothing came to their attention to conflict with that assertion.
	DHS	DHS personnel reviewed cyber threat information and then shared the information in real-time.

Entity	Responses on How Entities Determined Timely, Adequate, and Appropriate Information Sharing
Justice	Justice responded that it followed the CISA Privacy and Civil Liberties Guidelines, which address the timeliness, adequacy, and appropriateness of sharing information in connection with activities authorized in CISA.
Treasury	Treasury determined usefulness by the following considerations (1) timeliness – measured by hours not days or months; (2) adequacy – how indicators related to each other, how they were used, and when activity was observed; and (3) appropriateness/reliability – whether adversaries used shared or legitimate infrastructure to launch attacks, which limit the usefulness of some indicators due to high false positive rates.

D. Sharing Cyber Threat Indicators and Defensive Measures

CISA Section 107(b) requires the joint report to include the following information from each of the OIGs:

An assessment of the cyber threat indicators or defensive measures shared with the appropriate Federal entities under this title, including the following:

- i. **The number of cyber threat indicators and defensive measures shared through the capability and process developed in accordance with 105(c).**
- ii. **An assessment of information not directly related to a cybersecurity threat that is personal information of a specific individual and was shared by a non-Federal entity with the Federal Government or shared within the Federal Government in contravention of CISA, including a description of the violation.**
- iii. **The number of times, according to the Attorney General, that information shared under CISA was used by a Federal entity to prosecute an offense listed in Section 105(d)(5)(A).**
- iv. **A quantitative and qualitative assessment of the effect of sharing cyber threat indicators or defensive measures with the Federal Government on privacy and civil liberties of specific individuals, to include the number of notices issued due to a failure to remove personal information not directly related to a cybersecurity threat, in accordance with procedures required by section 105(b)(3)(E).¹⁰**

¹⁰ CISA Section 105(b)(3)(E) states that guidelines shall include procedures for Federal entities receiving information to notify Federal and non-Federal entities when the information received does not constitute a cyber threat indicator.

v. The adequacy of steps taken by the Federal Government to reduce any adverse effect from activities carried out under CISA on the privacy and civil liberties of U.S. persons.

We developed 14 questions to assist the entities with their reviews. Three questions address the number of indicators and measures shared using the AIS system; two address assessing information not directly related to a cybersecurity threat; seven address the effect of sharing indicators and measures on privacy and civil liberties of specific individuals; and two address the adequacy of steps taken to reduce any adverse effects of CISA-related activities. In addition, Justice requested information on the number of times information shared under CISA was used to prosecute an offense.

Number of Cyber Threat Indicators and Defensive Measures Shared Using the AIS system

1. (To be answered by DHS OIG only) How many cyber threat indicators and defensive measures have non-Federal entities shared with the DHS through the capability and process developed under section 105(c)?
2. (To be answered by DHS OIG only) How many of those cyber threat indicators and defensive measures reported for the question above did the DHS share with other Federal entities?
3. (To be answered by all entities' OIGs except DHS) How many cyber threat indicators and defensive measures from non-Federal entities did the DHS relay to your agency?

CISA Section 105(c) required DHS to develop and implement a capability and process to accept cyber threat indicators and defensive measures from non-Federal entities in real-time and then share the information in an automated manner in real-time with the Federal Government. DHS developed the AIS initiative as the primary mechanism to exchange unclassified cyber threat indicators and defensive measures with Federal and non-Federal entities in an automated manner. The AIS system connects participating organizations to a DHS-managed system that allows two-way sharing of cyber threat indicators.

According to DHS OIG, DHS reported that between November 2016 and June 2017, non-Federal entities shared 181,307 unclassified cyber threat indicators and two defensive measures using the AIS system. DHS then shared the cyber threat indicators and defensive measures with other Federal entities.

The OIGs for the remaining nine entities responded as follows:

- Energy reported receiving 26,236 cyber threat indicators through the AIS Industry system in 2016; however, the name of the company sharing the information was redacted and all indicators appeared to come from DHS.
- Treasury reported receiving 19,855 cyber threat indicators and defensive measures from non-Federal entities via DHS as of March 2017. However, Treasury stated that private sector submissions to DHS may have details identifying the reporter removed; therefore, it was possible that multiple reported indicators were condensed into a single indicator and the actual number could be higher than the 19,855 reported via DHS.

- Justice reported DHS shared approximately 30,000 cyber threat indicators; however, the source of the indicators was not disclosed to the recipients.
- NSA stated that it had not ingested AIS system data into its databases because it continues to work to appropriately tag the data in a manner that would assist with appropriate access and dissemination by analysts. NSA reported “one instance” of receiving information from a private entity via a non-automated process.
- ODNI and Commerce stated they could not identify whether the cyber threat indicators and defensive measures from DHS were from non-Federal entities because the information did not identify the originating entity.
- USCYBERCOM reported it received cyber threat indicators and defensive measures from DHS; however, it could not provide the total number from non-Federal entities.
- DoD CIO and DC3 indicated they do not have a process for tracking the number of cyber threat indicators and defensive measures from other Federal entities.
- DISA reported it does not have a method to count indicators shared by DHS.

Information Not Directly Related to a Cybersecurity Threat

1. Did any Federal or non-Federal entity share information with your agency that was not directly related to a cybersecurity threat that was personal information of a specific individual or information identifying a specific individual in violation with this title?
2. Please include a description of the violation.

The OIGs responded that none of the ten entities reported receiving information from any Federal or non-Federal entity that was not directly related to a cybersecurity threat and that included personal information of a specific individual.

Prosecuting an Offense. Justice reported that crediting a case solely on information shared under CISA is not measureable because information gathered to prosecute an offense may come from multiple sources, including CISA.

Effects of Sharing Cyber Threat Indicators and Defensive Measures

1. Was there an effect of your agency sharing cyber threat indicators and defensive measures with the Federal Government on privacy and civil liberties of specific individuals?
2. What was the effect on privacy and civil liberties of specific individuals?
3. How did your agency quantitatively and qualitatively assess the effect?
4. Did your agency receive any notices regarding a failure to remove information that was not directly related to a cybersecurity threat, and were any of those notices related to personal information of a specific individual or information that identified a specific individual?
5. How many notices did your agency receive?

6. Did your agency issue any notices regarding a failure to remove information that was not directly related to a cybersecurity threat, and were any of those notices related to personal information of a specific individual or information that identified a specific individual?
7. How many notices did your agency issue?

For questions one through four, only Treasury identified potential effects on the privacy and civil liberties of specific individuals due to sharing cyber threat indicators and defensive measures with the Federal Government. Specifically, Treasury identified a limited potential impact in the event a Treasury report adversely affects a Treasury employee based on the report information. Treasury is in the final stages of its review of the Privacy and Civil Liberties Impact Assessment and will be able to more definitively answer this question upon the completion of the assessment. Although no effect has actually been found, Treasury applies a quantitative analysis using Fair Information Practice Principles and other considerations, such as whether security activities involve monitoring or interception of communications or compiling of information on lawful activities that may impact civil liberties.

For questions five through seven, none of the ten entities reported receiving or issuing notices for a failure to remove information containing PII when not directly related to a cybersecurity threat.

Steps Taken to Reduce Adverse Effects

1. Were the steps taken by your agency to reduce adverse effects from the activities carried out under this title on the privacy and civil liberties of U.S. persons adequate?
2. How did your agency determine adequacy of the steps taken?

The OIGs responded that two of the ten entities – DISA and Energy –reported they did not take any steps to reduce potentially adverse effects from activities under CISA on the privacy and civil liberties of U.S. persons because they were not aware of any adverse effects. NSA reported they did not take any steps beyond those required by the CISA Privacy Guidelines and applicable procedures because they were not aware of any adverse effects. The OIGs responded that the remaining seven entities – ODNI, Commerce, DoD CIO and DC3, USCYBERCOM, DHS, Justice, and Treasury – stated they took adequate steps to reduce any adverse effects and explained how they determined adequacy of those steps.

Table 4 provides responses on how the seven entities listed above determined adequacy.

Table 4. Entities' Responses on Determining Adequacy of Steps Taken

Entity	Responses on How Entities Determined Adequacy of Steps Taken to Reduce Adverse Effects	
ODNI	ODNI determined all cyber threat indicators provided to and shared by ODNI were tied directly to specific technical system/network vulnerabilities and protections. They did not include PII or require steps to reduce any impact on persons.	
Commerce	Commerce reported that the Commerce Threat Intelligence Portal system removed certain types of information to develop indicators, and PII would not meet the format of an indicator. Shared indicators cannot be viewed until they are reviewed by administrators who determine whether to publish the indicators. In addition, no protected personal information has been accidentally shared with unauthorized entities.	
DoD	DoD CIO and DC3	DoD CIO and DC3 responded they only shared cyber incidents with PII after the submitting contractor had determined that the information was relevant and necessary to cyber incidents, follow-on forensics, or cyber intrusion damage assessment analysis.
	USCYBERCOM	USCYBERCOM continuously evaluated the adequacy of steps taken through constant communication and collaboration efforts with its liaison officers, 24/7 cyber operation centers, and cyber partners, along with annual training requirements.
DHS	DHS developed privacy and civil liberties guidelines and U.S. Computer Emergency Readiness Team Information Handling guidelines and implemented privacy controls to prevent PII violations. In addition, DHS performed a manual review to remove personal information to ensure there is no unauthorized release of PII and a privacy impact assessment on the AIS system.	
Justice	Justice determined the cyber threat indicators provided to and shared via the Justice platform were specific to technical system and network vulnerabilities and did not include PII or require steps to reduce the impact on persons. Additionally, Justice and DHS co-authored the CISA Privacy and Civil Liberties Guidelines that address proper safeguard and handling of PII and violations.	
Treasury	Treasury has not found any reports shared or received that contained inappropriate personal or other data.	

E. Inappropriate Barriers

CISA Section 107(b) requires the joint report to include the following information from each of the OIGs:

An assessment of the sharing of cyber threat indicators and defensive measures among Federal entities to identify inappropriate barriers to sharing information.

We developed two questions to assist the entities with their reviews.

1. Has your agency identified any barriers that adversely affected the sharing of cyber threat indicators and defensive measures among Federal entities?
2. Please describe the barriers and the effect the barriers have on the sharing of cyber threat indicators and defensive measures.

Barriers to Sharing Cyber Threat Information. The OIGs responded that seven of the ten entities reported different barriers to sharing cyber threat information. Several of the barriers included issues with sharing cyber threat information. Table 5 presents the responses for the seven entities that reported barriers to sharing cyber threat information.

Table 5. Entities' Responses on Barriers to Sharing Cyber Threat Information

Entity	Entities' Responses on Barriers to Sharing Cyber Threat Information
Commerce	Commerce responded that cyber threat indicators might contain information pertaining to an internal agency that would present a threat if published externally. In addition, the Commerce Threat Intelligence Portal, used for sharing between the Department and its bureaus, does not allow for integration with the bureaus' automated tools necessary for processing the indicators, thereby hindering the sharing of cyber threat indicators and defensive measures.
DoD	DISA DISA reported that agencies that have not requested access to Cyber Situational Awareness Analytic Capabilities/Fight by Indicator and/or do not have access to SIPRNet are prevented from sharing cyber threat indicators and defensive measures.
	USCYBERCOM USCYBERCOM responded that some indicators derived from intelligence reporting might not be authorized for wider dissemination due to the classification level. These indicators will not be shared with Federal entities or trusted agents without appropriate clearance.

Entity	Entities' Responses on Barriers to Sharing Cyber Threat Information
Energy	<p>Energy indicated that cultural barriers had an impact on sharing cyber threat indicators and defensive measures. The reluctance to release information deemed organizationally specific, liability concerns, or the general resistance to change are ongoing challenges. In addition, a general lack of openness by both government and private entities concerning cyber threat details hindered the positive impact such information could provide. Participants receive cyber threat indicators from others, but most agencies were reluctant to share their information. Energy did not identify any significant technical barriers.</p>
DHS	<p>DHS reported the following barriers and challenges to sharing cyber threat indicators:</p> <ul style="list-style-type: none"> • The system DHS currently uses does not provide the quality, contextual information needed to ensure appropriate responses to evolving threats. • A cross-domain solution and automated tools are lacking to analyze and share cyber threat information timely. • Enhanced outreach is needed to increase participation and better coordinate information sharing across Federal agencies and the private sector.
Justice	<p>Justice reported the following barriers:</p> <ul style="list-style-type: none"> • Information sharing between Justice and the Intelligence Community is often challenging due to the classification of information. • Participants in the AIS system are not extensively vetted, which is a concern when sharing sensitive cyber threat information through the AIS system. • Some private entities are hesitant to share cyber threat information because they believe sharing such information may raise legal and competitive issues, including potential anti-trust issues. • Justice continues to face challenges in communicating with some private sector companies and industries based on the perception that cooperation with law enforcement may lead to negative business and regulatory consequences. • Justice continues to operate in an environment in which public perception of Federal Government actions in cyberspace, especially those of law enforcement agencies, is mixed.

Entity	Entities' Responses on Barriers to Sharing Cyber Threat Information
Treasury	Treasury responded that sharing cyber threat indicators and defensive measures with the AIS system requires using a specialized report format. Treasury needs to build another report generation algorithm, which has delayed its ability to share information with Federal partners via the AIS system.

For the remaining three entities:

- ODNI responded that it recently deployed a capability to share indicators across the Intelligence Community, and it expects to learn more about potential barriers as sources of indicators are added and users from across the Intelligence Community access the data for cyber defense activities.
- DoD CIO and DC3 did not report any barriers. However, they stated that in order to share classified information under the Defense Industrial Base Cyber Security program, DoD CIO and DC3 required Defense Industrial Base participants to have safeguards to receive and store classified information at the Secret level and use Defense Industrial Base Net-Secret.
- NSA responded that it has not uncovered any barriers that would adversely affect sharing cyber threat information among Federal entities. However, NSA stated that it implements complex data tagging processes to ensure ingested data is properly marked in NSA repositories. As a result, determining the proper tagging for cyber threat indicators ingested via the AIS system requires deliberation, and NSA has been challenged by the ingestion and storage of cyber threat indicators obtained from the AIS system.

Acronyms

AIS	Automated Indicator Sharing
CIO	Chief Information Office
CISA	Cybersecurity Information Sharing Act of 2015
CY	Calendar Year
DC3	DoD Cyber Crime Center
DHS	Department of Homeland Security
DISA	Defense Information Systems Agency
DoD	Department of Defense
NSA	National Security Agency
ODNI	Office of the Director of National Intelligence
OIG	Office of Inspector General
PII	Personally Identifiable Information
USCYBERCOM	U.S. Cyber Command

IC IG HOTLINE

BE PART OF THE

SOLUTION

YOU JOINED TO MAKE A DIFFERENCE, REPORT FOR THE SAME REASON



Office of the Inspector General of the Intelligence Community | 571 204 8149 | Hotline: 855 731 3260 | dni.gov/icig