Council of Inspectors General on Financial Oversight

January 15, 2020

MEMORANDUM FOR Steven T. Mnuchin
Chairman, Financial Stability Oversight Council

FROM: Richard K. Delmar
Acting Chair, Council of Inspectors General on Financial Oversight

SUBJECT: Survey Results— CIGFO Working Group's Survey of FSOC and its Federal Member Agencies' Efforts to Implement the Cybersecurity Act of 2015

With this memorandum, we hereby transmit the results of a Council of Inspectors General on Financial Oversight (CIGFO) Working Group survey of the Financial Stability Oversight Council's (FSOC) and its Federal voting member agencies' efforts to implement the information sharing provisions under Title I, the Cybersecurity Information Sharing Act (CISA) of the Cybersecurity Act of 2015. Section 107 of CISA, "Oversight of Government Activities," requires Inspectors General of "appropriate Federal entities,"[1] in consultation with the Intelligence Community Inspector General (IC IG) and CIGFO, to jointly report to Congress on the actions taken by the respective agencies over the most recent 2-year period to carry out the requirements of CISA. The first joint Inspectors General report was submitted to Congress in December 2017 (2017 joint IG report)[2] and the second joint report was issued in December 2019.

We undertook this survey to inform our reporting consultation role under Section 107, as well as provide FSOC and its Federal voting member agencies[3] with comparative information on how these agencies have implemented CISA.

We conducted the survey using a questionnaire based on the common question set created for the purpose of the 2017 joint IG report. In this regard, CISA Section

---

[1] The appropriate Federal entities are the Departments of Commerce, Defense, Energy, Homeland Security, Justice, the Treasury, and the Office of the Director of National Intelligence.

[2] *Joint Report on the Implementation of the Cybersecurity Information Sharing Act of 2015* (Office of the Inspector General of the Intelligence Community AUD 2017 005) (Dec. 19, 2017)

[3] The Federal voting members are the Secretary of the Treasury, Chairman of the Board of Governors of the Federal Reserve System, Comptroller of the Currency, Director of the Bureau of Consumer Financial Protection, Chairman of the U.S. Securities and Exchange Commission, Chairperson of the Federal Deposit Insurance Corporation, Chairperson of the Commodity Futures Trading Commission, Director of the Federal Housing Finance Agency, and the Chairman of the National Credit Union Administration.

107(b) requires that the joint report include certain information; the IC IG developed questions to gather that information. The CIGFO Working Group, led by the Department of the Treasury's (Treasury) Office of Inspector General (OIG), modified the common question set for the Federal financial sector survey audience. Our survey was not designed to assess Federal voting member agencies' compliance with CISA, and we make no such assessment in this memorandum.

We note that, while the Secretary of the Treasury is a Federal voting member of FSOC, Treasury was not included in this CIGFO Working Group survey. As one of the "appropriate federal entities" per CISA, Treasury's actions to carry out the requirements of CISA are reviewed separately by Treasury OIG. The results of Treasury OIG's reviews were included in the 2017 and 2019 joint IG reports to Congress. One of Treasury's bureaus, the Office of the Comptroller of the Currency (OCC), is a Federal voting member of FSOC and is included in this survey.

As part of this survey, in addition to the Federal voting members of FSOC, we interviewed officials from the FSOC Secretariat and Treasury's Office of Cybersecurity and Critical Infrastructure Protection (OCCIP) to gain an understanding of their role, if any, in implementing CISA. Treasury is a member of FSOC and OCCIP coordinates Treasury's efforts to enhance the security and resilience of financial sector critical infrastructure and reduce operational risk.

The following OIGs also participated in this Working Group: Board of Governors of the Federal Reserve System (Board) and the Bureau of Consumer Financial Protection (Bureau); Commodity Futures Trading Commission (CFTC); Federal Deposit Insurance Corporation (FDIC); Federal Housing Finance Agency (FHFA); National Credit Union Administration (NCUA); and U.S. Securities and Exchange Commission (SEC).

We conducted this survey from April 2019 through September 2019. The scope of our work covered the period of January 1, 2017 through March 31, 2019. As part of our survey, we reviewed applicable provisions of CISA and the agencies' responses to the common question set.

Background

In December 2015, CISA was signed into law to encourage the sharing of cyber threat information between the public and private sectors in a timely manner.[4] The act designated seven federal agencies to coordinate and develop government-wide,

[4] Consolidated Appropriations Act, 2016, Pub. L. No. 114-113, div. N (Cybersecurity Act of 2015), Title I (Cybersecurity Information Sharing Act of 2015), 129 Stat. 2242, 2936-56 (2015) (codified at 6 U.S.C. §§ 1501-10).

publicly available policies, procedures, and guidance to assist federal and non-federal entities in their efforts to receive and share cyber threat indicators and defensive measures.[5] Among the policies issued was *Sharing of Cyber Threat Indicators and Defensive Measures by the Federal Government under the Cybersecurity Information Sharing Act of 2015* (February 16, 2016) which states:

> "Federal entities are encouraged to share [cyber threat indicators (CTIs)] and [defensive measures (DMs)] as broadly and as quickly as possible. Whether CTIs and DMs are classified, declassified or unclassified, federal entities should continuously identify and implement programs to share such CTIs and DMs with each other and with non-federal entities."[6]

I. Survey Results

The agencies provided responses to our questions on their implementation of CISA. Specifically, the responses addressed the:

A. Sufficiency of policies and procedures related to sharing CTIs[7] within the Federal Government;
B. Classification of CTIs and DMs,[8] and an accounting of the security clearances for the purpose of sharing with the private sector;
C. Actions taken based on CTIs or DMs shared with the Federal Government;
D. CTIs and DMs shared with federal entities containing information not directly related to a threat that is personal information; and
E. Any barriers to sharing information among federal entities.

A. Sufficiency of Policies and Procedures

The following questions were designed to gain an understanding of an agency's policies, procedures, and guidelines relating to the sharing of CTIs within the Federal Government and relevant entities, including those policies, procedures, and guidelines relating to the removal of information not directly related to a

[5] See footnote 1 for the list of these agencies.

[6] The policy document cautions that federal entities engaging in activities authorized by CISA "shall do so in full compliance with the Constitution and all other applicable laws of the United States, Executive Orders, and other Executive Branch directives, regulations, policies and procedures, court orders and all other legal, policy and oversight requirements." For example, the sharing of classified CTIs and DMs is with representatives of federal and non-federal entities that have appropriate security clearances.

[7] CTI – per CISA, CTI is information used to describe or identify security vulnerabilities, tools and procedures that may be used by attackers to compromise information systems.

[8] DM – per CISA, DM is an action, device, procedure, technique, or other measure that detects, prevents, or mitigates a known or suspected cybersecurity threat or security vulnerability.

cybersecurity threat that is personal information of a specific individual or identifies a specific individual.

1. Does your agency have policies, procedures, and guidelines for:

   a) Sharing of CTIs within the Federal Government?
   b) Sharing CTIs with representatives of relevant entities (e.g., private entities, non-federal government agency, state/tribal/local government) as it pertains to the protection of classified information?
   c) Removal of information not directly related to a cybersecurity threat that is personal information of a specific individual or identifies a specific individual?
   d) Implementing security controls to protect against unauthorized access to CTIs or DMs?
   e) Notifying entities that received a CTI known to be in error?
   f) Notifying any U.S. person whose personal information is known to have been shared in violation of CISA?

2. To what extent have the policies, procedures, and guidelines for sharing CTIs been implemented?

3. Have there been any concerns or setbacks with regard to the implementation of the policies, procedures, and/or guidelines for sharing CTIs?

Table A.1 summarizes the agencies' responses to Questions 1a, 1b, 1c, 1e, 2 and 3.

Entity	Guidance for Sharing CTIs	Guidance for Sharing Classified Information w/ Relevant Entities	Guidance Addressing Removing PII[9] not related to CTIs	Guidance for Notifying Entities of CTIs Sent in Error	Guidance for Sharing CTIs Implemented	Concerns or Setbacks in Implementing Guidance for CTIs
Board	Yes	Yes	Yes	Yes	N/A	N/A
Bureau	Yes	N/A	Yes	Yes	Yes	No
CFTC	Yes	No[a]	Yes	Yes	Yes	No
FDIC	No	No	Yes	N/A	No	No
FHFA[b]	No	N/A	No	No	Yes	No
NCUA	No	No	Yes	No	No	Yes[c]
OCC	Yes	N/A	Yes	Yes	Yes	No
SEC	Yes	No	Yes	Yes	Yes	No

[a] CFTC has not developed specific policies, procedures, or guidelines for the sharing of CTIs with regulated entities. CFTC does not receive a significant amount of information regarding CTIs and the information received do not contain classified information.

[b] FHFA does not maintain policy/procedure documentation specific to sharing CTIs. However, FHFA answered that it implemented (1) information sharing agreements with certain Federal agencies and its regulated entities (Fannie Mae, Freddie Mac, and the Federal Home Loan Banks), and (2) procedures for controlling the release of PII outside the agency.

[c] NCUA reported that it does not have the resources or mature capabilities to develop or sustain the development of procedures and policies, implement a repeatable process to efficiently analyze threat indicators, or to categorize and share the information with other entities.

Table A.2 summarizes the agencies' responses to Question 1d.

Entity	Guidance for implementing security controls to protect against unauthorized access to CTIs or DMs.
Board	The Board has implemented controls to protect CTIs and DM and these controls are reviewed on a regular basis and continuously improved.

[9] PII – personally identifiable information – information that, when used alone or with other relevant data, can identify an individual.

Entity	Guidance for implementing security controls to protect against unauthorized access to CTIs or DMs.
Bureau	The Bureau's approach for applying protections for CTIs is consistent with appropriate controls for Federal Information Security Management Act (FISMA)[10] moderate systems as defined by applicable NIST[11] guidelines if external to a Bureau-owned system.
CFTC	The CFTC protects its sensitive information, including CTIs and DMs, by leveraging the NIST Cybersecurity Framework and Risk Management Framework in compliance with the FISMA.
FDIC	The FDIC uses the Anomali threat intelligence platform to store CTIs and leverages built-in, role-based access controls.
FHFA	FHFA does not have policies, procedures, or guidelines for implementing security controls to specifically protect against unauthorized access to CTIs. However, in practice, access to all cyber defense solutions, including vulnerability information, is restricted to members of FHFA's cybersecurity team and information technology engineers, as needed.
NCUA	OCIO[12] uses access controls for the protection of threat indicators. Most controls are two-factor authentication and are applied on the file shares, ticketing system and security tools.
OCC	Access controls for the security tools used by the OCC's internal cybersecurity operations to centralize and collocate open source intelligence and vendor-supplied threat and vulnerability information are set by internal agency logical access management policy and meet NIST SP 800-53 baseline security control requirements.
SEC	The SEC has documented its overarching policies pertaining to the implementation of access controls.

[10] FISMA – Federal Information Security Management Act of 2002 - U.S. legislation that defines a comprehensive framework for protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide integrity, confidentiality and availability. FISMA was amended by the Federal Information Security Modernization Act of 2014.

[11] NIST – National Institute of Standards and Technology – Part of the U.S. Department of Commerce, its mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.

[12] OCIO – Office of the Chief Information Officer

Table A.3 summarizes the agencies' responses to Question 1f.

Entity	Guidance for notifying any U.S. person whose personal information is known to have been shared in violation of CISA
Board	The Board has guidance pertaining to this topic.
Bureau	The Bureau noted that it is not aware of any instance where a U.S. person's personal information has been shared in violation of CISA, and should this occur, the Bureau's Privacy Office would coordinate the notification.
CFTC	CFTC has in place an Incident Response Plan that addresses the notification process of affected individuals in case of a PII compromise.
FDIC	FDIC does not have policies, procedures or guidelines specific to notifying U.S. persons of information shared in violation of CISA.
FHFA	PII maintained by FHFA that is lost, compromised or disclosed to an unauthorized individual is addressed by the FHFA in accordance with its policy for addressing and reporting PII breaches.
NCUA	NCUA has an overarching breach policy which (a) establishes internal and external notification procedures and required actions when a breach of PII occurs; and (b) includes policy specific to breaches affecting NCUA employees, contractors and the public.
OCC	The OCC internal cybersecurity operations limit such sharing to technical details. As no information about individuals is included in such reporting, no additional policy or procedures are required to address such notifications.
SEC	SEC has a plan that defines the roles and responsibilities of agency employees, managers, and contractors, including subcontractors, regarding the suspected or confirmed breach of PII. The plan also provides processes, procedures and associated tasks required by the Office of Management and Budget, applicable laws, and regulations.

B. Classification and Accounting

The following questions were designed to gain an understanding on whether CTIs or DMs identified by or shared with agencies have been properly classified and whether there is accountability over the number of security clearances authorized by the Federal Government for the purpose of sharing CTIs or DMs with the private sector:

1. Has your agency shared CTIs and DMs with the private sector?
2. Did your agency classify (i.e., a national security classification of confidential, secret, or top secret) the CTIs and DMs shared with the private sector?
3. How did your agency determine whether the shared CTIs and DMs were properly classified?
4. How does your agency account for the number of security clearances authorized for sharing CTIs and DMs with the private sector?

Sharing and Classifying Cyber Threat Information.

Table B.1 summarizes the agencies' responses to Questions 1, 2 and 4.

Entity	Sharing CTIs and DMs with Private Sector	Classifying of Shared DMs and CTIs	Accountability of Authorized Security Clearances for sharing DMs and CTIs
Board	Yes	No	Yes
Bureau	No	N/A	N/A
CFTC	Yes	No	N/A
FDIC	No	N/A	N/A
FHFA	No	N/A	N/A
NCUA	No	N/A	N/A
OCC	No	N/A	N/A
SEC	Yes	No	Yes

For the three agencies that indicated they share CTIs and/or DMs with the private sector but did not indicate classifying this information, they provided the following explanations:

- The Board reported that classified CTIs and DMs are shared with the Federal Reserve Banks and unclassified open source CTIs could be shared with the private sector through the Emergency Communication System. The Board also reported that it does not have classification authority.

- CFTC reported that the information it receives from the Cyber Information Group (CIG)[13] Circular is not classified.
- SEC reported that it does not have original classification authority and has not shared CTIs or DMs with a national security classification.

Additionally, FDIC reported that it has not shared classified CTIs or DMs and does not have classifying authority. FHFA reported that it only shares CTIs and DMs with its regulated entities. FHFA does not consider the regulated entities to be the private sector; they are government-sponsored enterprises. NCUA reported it does not have classification authority.

Accounting for Security Clearances. The agency responses varied as to how they accounted for the number of security clearances authorized for sharing CTIs and DMs with the private sector. Specifically, they responded as follows:

- The Board stated that all requests for security clearances at the Federal Reserve Banks sponsored by the Board are reviewed and approved by appropriate Board staff.
- The Bureau and OCC reported that they have not shared CTIs or DMs with the private sector.
- CFTC reported it does not provide clearances for CTIs because the information received is not classified.
- FDIC reported that it has not sponsored security clearances for the private sector.
- FHFA reported the question is not applicable.
- NCUA reported that its OCIO has not shared indicators or DMs with the private sector on a classified or unclassified level.
- SEC reported that its Office of Support Operations manages the issuance and tracking of clearances issued to agency personnel. Clearances are issued pursuant to agency and federal guidance. SEC does not share classified information with the private sector.

C. Actions Taken

The following questions were designed to gain an understanding of the actions taken by the agencies in response to CTIs or DMs shared between the agencies and other federal agencies:

[13] CIG – Treasury's Financial Sector CIG was established within Treasury's Office of Cybersecurity and Critical Infrastructure Protection in 2013. CIG monitors and analyzes all source information on cyber threats and vulnerabilities to the financial sector; provides timely, actionable cyber threat information to the sector; and solicits feedback and information requirements from the sector.

Subsequent Uses and Dissemination

1. Has your agency used and disseminated CTIs and DMs shared by other federal agencies?
2. Did your agency use or disseminate the shared CTIs and DMs appropriately?
3. How did your agency determine if the use and dissemination of shared CTIs and DMs was appropriate?
4. Has your agency shared CTIs and DMs with other federal agencies?
5. Did your agency share the CTIs and DMs in a timely and adequate manner with appropriate entities or, if appropriate, make them publicly available?
6. Have other federal entities shared CTIs and DMs with your agency in a timely, adequate, and appropriate manner?
7. How did your agency determine timeliness, adequacy and appropriateness of sharing the information?
8. How many CTIs and DMs from non-federal entities did the Department of Homeland Security (DHS) relay to your agency?

Six of the eight Federal voting member agencies – the Board, Bureau, CFTC, FDIC, OCC and SEC – reported using and disseminating CTIs and DMs shared by other federal agencies. FHFA and NCUA responses varied as to the use or dissemination of CTIs or DMs shared by other federal agencies. All eight Federal voting member agencies reported that they have used and disseminated the shared CTIs and DMs appropriately.

Table C.1 summarizes the agencies' responses to Question 1.

Entity	Responses to "Has your agency used and disseminated CTIs and DMs shared by other federal agencies?"
Board	CTIs and DMs received from other federal agencies are shared with the Federal Reserve Banks when appropriate.
Bureau	The Bureau receives threat indicators from DHS, the Federal Bureau of Investigation (FBI), and other federal agencies. When needed to apply protective controls, the Bureau shares a small subset of indicator information with its Managed Internet Service Provider for the purpose of applying DMs as defined in CISA. When Traffic Light Protocol[14] markings are affixed to indicator information, the Bureau adheres to the control markings.

[14] Traffic Light Protocol - TLP is a set of designations used to ensure that sensitive information is shared with the appropriate audience. It employs four colors to indicate expected sharing boundaries to be applied by the recipient(s).

Entity	Responses to "Has your agency used and disseminated CTIs and DMs shared by other federal agencies?"
CFTC	Yes, about five or six times a year, CFTC receives a CIG Circular from OIA.[15] The CIG Circulars do not contain any classified information. Two Divisions within the CFTC, the Division of Market Oversight and the Division of Clearing and Risk, determine whether they would be relevant for entities regulated by the CFTC. If the CIG Circular is relevant, the CFTC will email the Circular to appropriate contacts at the regulated entities.
FDIC	Yes, FDIC has used CTIs and DMs shared by other agencies.
FHFA	Yes, but only those provided by US-CERT[16] and the FBIIC[17]. FHFA has not received CTIs and DMs directly from other federal agencies.
NCUA	OCIO has used indicators from other federal agencies but does not disseminate indicators outside of NCUA.
OCC	Yes
SEC	Yes, the SEC has used cyber threat indicators and defensive measures shared by other Federal agencies such as CISA/DHS and the Federal Bureau of Investigation (FBI).

Table C.2 summarizes the agencies' responses to Question 3.

Entity	Responses to "How did your agency determine if the use and dissemination of shared CTIs and DMs was appropriate?"
Board	Board staff work with the Federal Reserve Banks to evaluate and assess their specific needs for CTIs and DMs, and limit access to responsive material.
Bureau	The Bureau follows its standard procedures for indicator handling.
CFTC	CIG Circulars include a traffic light protocol establishing the extent to which information can be shared and the CFTC follows that protocol in disseminating information in the Circulars.

[15] OIA – Office of Intelligence and Analysis is part of Treasury's Office of Terrorism and Financial Intelligence. It advances national security and protects financial integrity by informing Treasury decisions with timely, relevant, and accurate intelligence and analysis.

[16] US-CERT – United States Computer Emergency Readiness Team – a partnership between DHS and the public and private sectors, established to protect the nation's internet infrastructure.

[17] FBIIC – Financial and Banking Information Infrastructure Committee – coordinates the efforts of Federal and State financial regulators to address critical infrastructure issues, including preparation for and response to cyber or physical attacks against the financial system or indirect attacks or events that may affect the sector. The FBIIC consists of 18 member organizations from across the financial regulatory community, both federal and state and is chaired by a designee of the Secretary of the Treasury.

Entity	Responses to "How did your agency determine if the use and dissemination of shared CTIs and DMs was appropriate?"
FDIC	The use of shared CTI was based on the automated confidence scoring and the nature of specific indicators. They were deployed to appropriate defensive and protective controls.
FHFA	FHFA shares CTIs with its regulated entities and other Federal agencies as needed and follows dissemination instructions received with the CTI.
NCUA	OCIO adheres to the traffic light protocol established by DHS.
OCC	OCC internal cybersecurity operations has established procedures that are consistent with US-CERT requirements and guidance appearing in NIST Special Publication 800-150, *Guide to Cyber Threat Information Sharing*.
SEC	SEC was able to determine that the use of shared CTIs and DMs were appropriate by utilizing SOC[18] policies and procedures as well as guidance issued by DHS.

Table C.3 summarizes the agencies' responses to Question 4.

Entity	Responses to "Has your agency shared CTIs and DMs with other federal agencies?"
Board	Yes, the Board noted that it shares CTIs and DMs with US-CERT and the Federal Reserve Banks.
Bureau	Yes, the Bureau shares indicators directly with the DHS National Cybersecurity and Communications Integration Center using the STIX[19] 2.0 taxonomy.
CFTC	Yes, the CFTC shares the CTIs with DHS CISA, which in turn will share the relevant information with Federal agencies.
FDIC	FDIC has not shared CTIs or DMs with other Federal agencies.
FHFA	Yes, but only to US-CERT.
NCUA	OCIO does not disseminate indicators outside of NCUA.

[18] SOC – Security Operations Center – a command center facility for a team of information technology professionals with expertise in information security that is responsible for monitoring, analyzing, and protecting an organization from cyber-attacks.

[19] STIX - Structured Threat Information Expression – a standardized XML programming language for conveying data about cybersecurity threats in a common language that can be easily understood by humans and security technologies.

Entity	Responses to "Has your agency shared CTIs and DMs with other federal agencies?"
OCC	OCC internal cybersecurity operations has shared indicators with Treasury's Government Security Operations Center.
SEC	Yes, the SEC has previously shared cyber threat indicators and defensive measures with other Federal agencies.

Table C.4 summarizes the agencies' responses to Question 5.

Entity	Responses to "Did your agency share the CTIs and DMs in a timely and adequate manner with appropriate entities or, if appropriate, make them publicly available?"
Board	Yes
Bureau	Yes, the Bureau shared all indicators associated with incidents within the timeframes defined in the Federal Incident Reporting Guidelines.
CFTC	The CFTC SOC reports incidents and shares CTIs and DMs with DHS US-CERT in accordance with established DHS time reporting guidelines. CFTC does not share information it receives from DHS outside of the agency. Also, CFTC does not make information from CIG Circulars publicly available. Rather, CFTC makes relevant information from CIG Circulars available to regulated entities in a prompt manner.
FDIC	FDIC has not shared CTIs or DMs with other Federal agencies.
FHFA	Yes, with US-CERT; FHFA does not make CTIs and DMs publicly available.
NCUA	Not applicable, as OCIO does not disseminate indicators outside of NCUA.
OCC	OCC internal cybersecurity operations followed its established procedures for this information sharing. This information was not shared publicly.
SEC	The SEC has previously shared cyber threat indicators in a timely manner with appropriate entities.

Table C.5 summarizes agencies' responses to Question 6.

Entity	Responses to "Have other federal entities shared CTIs and DMs with your agency in a timely, adequate, and appropriate manner?"
Board	In general, yes.

Entity	Responses to "Have other federal entities shared CTIs and DMs with your agency in a timely, adequate, and appropriate manner?"
Bureau	Yes, the Bureau is a participant in the DHS Automated Indicator Sharing[20] (AIS) program.
CFTC	Yes
FDIC	By our estimation, data is shared in a timely manner. However, appropriateness is undermined by a large volume of indicators that alert on actors performing reconnaissance activity against the FDIC's outer bastion of network devices. The volume of indicators seems to adequately address various threat vectors, specifically those vectors for which the FDIC has a means to detect.
FHFA	FHFA has no way to make such a determination.
NCUA	Yes. OCIO receives indicators and DMs through the HSIN[21] portal, weekly Federal SOC calls, and bulletins from other federal entities as they are released.
OCC	Yes
SEC	Yes

Table C.6 summarizes agencies' responses to Question 7.

Entity	Responses to "How did your agency determine timeliness, adequacy and appropriateness of sharing the information?"
Board	There are no explicit metrics or measurement techniques for timeliness of information sharing.
Bureau	The AIS program provides the fastest available mechanism for unclassified indicator dissemination.
CFTC	The agency does not determine timeliness. Rather, the agency evaluates information received from either DHS or Treasury's OIA and assesses relevance to either the agency or to regulated entities.

[20] Automated Indicator Sharing – DHS' free capability that enables the exchange of CTIs between the Federal Government and the private sector at machine speed.

[21] HSIN - Homeland Security Information Network – is DHS' official system for trusted sharing of Sensitive but Unclassified information between federal, state, local, territorial, tribal, international and private sector partners.

Entity	Responses to "How did your agency determine timeliness, adequacy and appropriateness of sharing the information?"
FDIC	By our estimation, data is shared in a timely manner. However, appropriateness is undermined by a large volume of indicators that alert on actors performing reconnaissance activity against the FDIC's outer bastion of network devices. The volume of indicators seems to adequately address various threat vectors, specifically those vectors for which the FDIC has a means to detect.
FHFA	Not Applicable.
NCUA	OCIO has used indicators from other federal agencies, but does not disseminate indicators outside of NCUA. OCIO has not measured timeliness, adequacy and appropriateness of indicators from other federal agencies.
OCC	OCC's internal cybersecurity operations follow directions established in US-CERT federal incident notifications guidelines with regard to timely, adequate, and appropriate information sharing.
SEC	SEC evaluates the timeliness, adequacy, and appropriateness of the information shared on a case-by-case basis.

Table C.7 summarizes agencies' responses to Question 8.

Entity	Responses to "How many CTIs and DMs from non-federal entities did the DHS relay to your agency?"
Board	DHS did not relay any CTIs or DMs.
Bureau	As of June 2019, the Bureau had CTIs provided by DHS in its Threat Intelligence Platform. The Bureau did not receive the origin report for many of these indicators, so it is unclear how many were provided by non-Federal entities.
CFTC	Based on the information received from DHS and Treasury's OIA, CFTC is not able to determine whether CTIs conveyed by DHS are from non-federal entities.
FDIC	Undetermined. FDIC does not receive breakdowns of the original source of CTIs or DMs.
FHFA	This is a question for DHS.
NCUA	OCIO has received approximately 500 bulletins and advisories since January 1, 2019. It is difficult to determine non-federal vs federal agencies due to DHS not attributing CTIs or DMs to a specific agency or private entity.

Entity	Responses to "How many CTIs and DMs from non-federal entities did the DHS relay to your agency?"
OCC	DHS routinely relays such indicators and measures from non-federal entities through their semi-weekly conference calls and its situational awareness submissions to FS-ISAC,[22] which are sent out to both federal and local government agencies.
SEC	SEC regularly receives CTIs and DMs issued by DHS as part of DHS information sharing initiatives and regular report issuances.

D. Information Not Directly Related to a Cybersecurity Threat

The following questions were designed to gain an understanding of whether any information that is personal information of a specific individual was shared by a federal or non-federal entity with the agencies in contravention of law or guidelines required by CISA:

1. Did any federal or non-federal entity share information with your agency that was not directly related to a cybersecurity threat that is personal information of a specific individual or information identifying a specific individual in violation of CISA?
2. Please include a description of the violation.
3. To your knowledge, has your agency's sharing of CTIs and DMs within the Federal Government or with non-federal entities had an effect on the privacy and civil liberties of specific individuals?
4. What was the effect on privacy and civil liberties of specific individuals?
5. How did your agency quantitatively and qualitatively assess the effect?
6. 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?
7. How many notices did your agency receive?
8. 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?
9. How many notices did your agency issue?

[22] FS-ISAC – Financial Services Information Sharing and Analysis Center – is an industry consortium dedicated to reducing cyber-risk in the global financial system. It was created in response to the US Presidential Decision Directive 63, which was issued in 1998 and updated in 2003 by the Homeland Security Presidential Decision Directive 7.

10. Do you believe 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 were adequate?
11. How did your agency determine adequacy of the steps taken?

All Federal voting member agencies reported that they had not shared information not directly related to a cybersecurity threat that was personal in nature or had an effect on the privacy and civil liberties of individuals. Further, they had not issued or received any notices regarding failure to remove information not directly related to a cybersecurity threat or personally identifiable information. As a result, the agencies' responses to all other related questions were either no or not applicable.

E. Barriers

The following questions were designed to obtain each agency's perspective on any barriers to the sharing of CTIs or DMs among federal entities and non-federal entities:

1. Has your agency identified any barriers that adversely affected the sharing of CTIs and DMs among federal entities and non-federal entities?
2. Please describe the barriers and the effect the barriers have on the sharing of CTIs and DMs.

Barriers to Sharing Cyber Threat Information. Three of the eight Federal voting member agencies – the Board, the Bureau, and NCUA – reported barriers to sharing cyber threat information. The Board shared that intelligence providers should continue to weigh the need to highly classify actionable information as this limits the ability to widely share such information. The Board also noted that the need to have Secure Compartmentalized Information clearances for all recipients limits the ability to implement actionable intelligence quickly and efficiently. The Bureau stated that, in general, the AIS program worked as intended. However, it was difficult to get responses from the DHS Cyber Liaison team regarding technical specifics on options available to leverage deeper analysis on shared indicators (for example, how to take advantage of shared DHS LookingGlass[23] services). NCUA reported that OCIO does not have the resources, fiscal funds, or technical capabilities to implement a sharing of CTIs and DM program.

For the remaining five Federal voting member agencies:

- CFTC, FHFA, OCC and SEC did not report any barriers.
- FDIC reported that it has not shared CTIs or DMs with other federal or non-federal entities.

[23] LookingGlass is a contractor used by DHS to provide a variety of platforms and services to meet a range of cyber intelligence needs.

II. Office of Cybersecurity and Critical Infrastructure Protection

Located within Treasury's Office of Domestic Finance, OCCIP works closely with financial sector firms, industry groups, and government partners to share information about cybersecurity and physical threats and vulnerabilities, encourage the use of baseline protections and best practices, and respond to and recover from significant incidents affecting the sector. OCCIP executes the responsibilities assigned to Treasury as the Sector Specific Agency for the Financial Services Sector by Presidential Policy Directive 21, *Critical Infrastructure Security and Resilience*, and Executive Order 13636, *Improving Critical Infrastructure Cybersecurity* (February 12, 2013).

An OCCIP official told us that they actively work to bring awareness of CISA to the financial sector and work with government agencies to better understand CISA and its utility to firms. To facilitate this information sharing, OCCIP collaborates across organizations and with financial services sector groups such as the Financial and Banking Information Infrastructure Committee (regulators), the Financial Services Sector Coordinating Council, Financial Services Sector Government Coordinating Council, and the Financial Services Information Sharing and Analysis Center. OCCIP encourages firms to share actionable information (e.g., Indicators of Compromise) under the protections afforded under CISA, in accordance with other laws and applicable regulations consistent with their overall risk management strategy. However, as Treasury is not a regulator, OCCIP does not enforce compliance with CISA. (Given the existing degree of regulation and number of regulators of the sector, this is not an authority sought by Treasury.) Rather, OCCIP works to raise awareness of the benefits of voluntary cybersecurity information sharing under CISA by and with individual firms and the sector, as a whole; to date, it has not received any information sharing that has been explicitly linked to CISA.

III. Financial Stability Oversight Council Secretariat

FSOC Secretariat is a dedicated policy office within Treasury that assists in coordinating the work of the FSOC among its members and member agencies. An FSOC Secretariat official told us the Secretariat's role is to support FSOC activities by performing research, ensuring compliance with FSOC policies (bylaws), and providing administrative support (budget).

The FSOC Secretariat official also told us that FSOC's role in CISA is limited. The topic of cybersecurity had been discussed at meetings and in FSOC's annual reports, but CISA, the statute itself, had been rarely discussed. CISA was last

mentioned in FSOC's 2016 Annual Report.[24] FSOC Secretariat focuses on bringing regulatory attention of cybersecurity to private and government entities and providing recommendations. To date, the FSOC has not received any information explicitly related to CISA.

[24] In that report, FSOC noted that the Cybersecurity Act of 2015, which includes CISA, provides a foundation for further advances in cybersecurity-related information sharing. FSOC recommended that Treasury, the Departments of Homeland Security, Justice, and Defense, and financial regulators strongly support efforts to implement this legislation, including coordinating their associated processes with the financial services sector, consistent with processes established by the law.

Abbreviations

AIS	Automated Indicator Sharing
Board	Board of Governors of the Federal Reserve System
Bureau	Bureau of Consumer Financial Protection
CFTC	Commodity Futures Trading Commission
CIG	Cyber Intelligence Group
CIGFO	Council of Inspectors General on Financial Oversight
CISA	Cybersecurity Information Sharing Act of 2015
CTI	Cyber threat indicator
DHS	Department of Homeland Security
DM	Defensive measures
FBI	Federal Bureau of Investigation
FBIIC	Financial and Banking Information Infrastructure Committee
FDIC	Federal Deposit Insurance Corporation
FISMA	Federal Information Security Management Act of 2002
FHFA	Federal Housing Finance Agency
FS-ISAC	Financial Services Information Sharing Analysis Center
FSOC	Financial Stability Oversight Council
HSIN	Homeland Security Information Network
IC IG	Intelligence Community Inspector General
NCUA	National Credit Union Administration

Abbreviations (continued)

NIST	National Institute of Standards and Technology
OCC	Office of the Comptroller of the Currency
OCCIP	Office of Cybersecurity and Critical Infrastructure Protection
OCIO	Office of the Chief Information Officer
OIA	Office of Intelligence and Analysis
OIG	Office of Inspector General
PII	Personally identifiable information
SEC	U.S. Securities and Exchange Commission
SOC	Security Operations Center
STIX	Structured Threat Information Expression
Treasury	Department of the Treasury
US-CERT	United States Computer Emergency Readiness Team