Audit Report

OIG-22-013

CYBERSECURITY/INFORMATION TECHNOLOGY

Audit of the Department of the Treasury's Cybersecurity Information Sharing

November 23, 2021

Office of Inspector General

Department of the Treasury

This Page Intentionally Left Blank

Contents

Audit Report

Appendices

Abbreviations

AIS	Automated Indicator Sharing
CY	calendar year
CIGFO	Council of Inspectors General on Financial Oversight
CISA	Cybersecurity Information Sharing Act of 2015
CONOPS	*Threat Indicator Sharing Concept of Operations*
DHS	Department of Homeland Security
FS-ISAC	Financial Services – Information Sharing and Analysis Center
FSS	Financial Services Sector
GAO	Government Accountability Office
GSOC	Government Security Operations Center
HSIN	Homeland Security Information Network
IC IG	Inspector General of the Intelligence Community
IG	Inspector General
IP	Internet Protocol
OCCIP	Office of Cybersecurity and Critical Infrastructure Protection
OCIO	Office of the Chief Information Officer
ODNI	Office of the Director of National Intelligence
OIG	Office of Inspector General
PCLIA	Privacy and Civil Liberties Impact Assessment

PII	personally identifiable information
PTR	Office of Privacy, Transparency, and Records
SIEM	Security Information and Event Management
TEWI	Treasury Early Warning Indicator
TLP	Traffic Light Protocol
Treasury	Department of the Treasury
US-CERT	United States Computer Emergency Readiness Team

Audit Report

November 23, 2021

Tony Arcadi

Paul Neff
Director, Cyber Policy, Preparedness, and Response

This report presents the results of our audit of the Department of the Treasury's (Treasury) activities to carry out the cybersecurity information sharing provisions of Title I, the *Cybersecurity Information Sharing Act* (CISA) of the *Cybersecurity Act of 2015*.[1] Section 107 of CISA, "Oversight of Government Activities," requires Inspectors General of "appropriate Federal entities,"[2] in consultation with the Inspector General of the Intelligence Community (IC IG)[3] and the Council of Inspectors General on Financial Oversight (CIGFO)[4], to jointly report to Congress on the actions taken by the respective agencies over the recent 2-year period to carry out the provisions of CISA. This report represents our third biennial report to support the joint report.[5]

[1] P. L. 114-113, Division N (December 18, 2015).
[2] The "appropriate Federal entities" are comprised of the Office of the Director of National Intelligence and the departments of Commerce, Defense, Energy, Homeland Security, Justice, and the Treasury.
[3] Authorized by the *2010 Intelligence Authorization Act* (P.L. 111-259; October 7, 2010), the IC IG was established to conduct audits, investigations, inspections, and reviews of programs and activities within the responsibility and authority of the Director of National Intelligence.
[4] Authorized by the *Dodd-Frank Wall Street Reform and Consumer Protection Act* (P.L. 111-203; July 21, 2010), CIGFO was established to provide oversight of the Financial Stability Oversight Council (FSOC); provide a forum for the discussion of ongoing work of each IG who is a CIGFO member; and submit annual reports to Congress and FSOC highlighting the concerns and recommendations.
[5] *Survey Results–Department of the Treasury's Activities to Implement the Cybersecurity Act of 2015* (OIG-CA-17-020; June 15, 2017), and *Audit of the Department of the Treasury's Cybersecurity Information Sharing* (OIG-20-019; December 10, 2019).

Our audit objective was to assess Treasury's activities during calendar years (CY) 2019 and 2020 to carry out the provisions of CISA to share cyber threat indicators and defensive measures. A cyber threat indicator is information used to describe or identify security vulnerabilities, tools, and procedures that may be used by attackers to compromise information systems. A defensive measure is an action, device, procedure, technique, or other measure that detects, prevents, or mitigates a known or suspected cybersecurity threat or security vulnerability.[6] We assessed the following as required by Section 107 of CISA:

a) the sufficiency of policies, procedures, and guidelines related to the sharing of cyber threat indicators within the Federal Government, including those related to the removal of PII [personally identifiable information][7] that is not directly related to a cybersecurity threat;

b) whether cyber threat indicators and defensive measures have been properly classified, as well as an accounting of the security clearances authorized for the purpose of sharing cyber threat indicators or defensive measures with the private sector;

c) a review of the actions taken by the Federal Government based on cyber threat indicators and defensive measures shared with the Federal Government including (1) the appropriateness of subsequent uses and disseminations of cyber threat indicators and defensive measures, and (2) the timeliness and adequacy;

[6] P.L. 114-113, Division N (December 18, 2015), SEC. 102. Definitions, (6) Cyber Threat Indicator and (7) Defensive Measure.

[7] PII is information that can be used to trace or distinguish an individual's identity either alone or when combined with other personal or identifying information to include, among other things, an individual's name, biometric records, social security number, date and place of birth, and mother's maiden name.

d) the specific aspects of cyber threat indicators or defensive measures shared with the Federal Government;[8] and

e) barriers affecting the sharing of cyber threat indicators or defensive measures.[9]

The scope of our audit comprised Treasury's cyber information sharing policies and procedures as well as activities for sharing cyber threat indicators and defensive measures during CY 2019 and CY 2020. As part of our audit, we reviewed applicable provisions of CISA; Treasury's policies and procedures for sharing cyber threat indicators and defensive measures contained in the Government Security Operations Center's (GSOC)[10] *Threat Indicator Sharing Concept of Operations* (CONOPS) (March 20, 2017) document; and the Office of Cybersecurity and Critical Infrastructure Protection (OCCIP)[11] *Original Production Procedures* (October 1, 2020). We also applied the common question set provided by the IC IG to make the assessments required by Section 107, and reviewed and evaluated the responses provided by GSOC, OCCIP, and the Office of Privacy, Transparency, and Records (PTR). We reviewed all nine Treasury Early Warning Indicators (TEWIs)[12] containing cyber threat indicators and

[8] These specific aspects of cyber threat indicators or defensive measures include: (a) the number of cyber threat indicators or defensive measures shared using the capability implemented by the Department of Homeland Security Automated Indicator Sharing (AIS); (b) instances in which any federal or non-federal entity shared information that was not directly related to a cybersecurity threat and contained PII; (c) the effect of sharing cyber threat indicators or defensive measures with the Federal Government on privacy and civil liberties of specific individuals, including the number of notices that were issued with respect to a failure to remove information not directly related to a cybersecurity threat that contained PII; and (d) the adequacy of steps taken by the Federal Government to reduce any adverse effect from activities carried out under this title on the privacy and civil liberties of U.S. persons.

[9] CISA Section 107 requires the following assessment applicable to the Department of Justice only: "According to the Attorney General, the number of times information shared under CISA was used by a Federal entity to prosecute an offense."

[10] As of June 2021, GSOC was renamed the Treasury Shared Services Security Operations Center. The report refers to GSOC for consistency since the name change was made after the audit scope period of CY 2019 and CY 2020 and near the August 2021 end of fieldwork date.

[11] OCCIP underwent a reorganization in early CY 2020, in which the Cyber Information Group was disbanded and its functions absorbed by other units within OCCIP.

[12] A TEWI provides information regarding a specific cyber threat indicator that may include details such as the subject line of a malicious email, Internet Protocol (IP) addresses, domains (i.e. Treasury.gov), and a description of how the cyber-attack progresses.

defensive measures that were prepared by GSOC of which all 9 were shared externally in CY 2019 (5 TEWIs) and CY 2020 (4 TEWIs). We reviewed all 15 Circulars[13] containing cyber threat indicators and defensive measures that OCCIP shared externally in CY 2019 (10 Circulars) and CY 2020 (5 Circulars). We conducted this audit remotely between January 2021 and August 2021. Appendix 1 contains a more detailed description of our objective, scope, and methodology. Appendix 2 contains the common question set provided by the IC IG.

Results in Brief

We concluded that Treasury's activities to share cyber threat indicators and defensive measures during CY 2019 and CY 2020 were adequate and aligned with provisions of CISA. Specifically, GSOC and OCCIP (1) designed and implemented sufficient policy, procedures, and practices to ensure the sharing of cyber threat indicators and defensive measures, including the removal of PII not directly related to a cybersecurity threat; (2) did not share classified cyber threat indicators and defensive measures with the private sector that required authorization and accounting of the security clearances; (3) took appropriate, adequate, and timely[14] actions to disseminate cyber threat indicators shared with the Federal Government; (4) shared specific aspects of cyber threat indicators that have been shared with the Federal Government; and (5) had no barriers affecting the sharing of cyber threat indicators and defensive measures although there were reported challenges in receiving cyber information from the Financial Service Sector (FSS)[15] and other Federal agencies.

[13] Circulars are created by OCCIP to share timely, actionable cybersecurity information with partner agencies related to the Financial Services Sector (FSS) and other critical infrastructure partner organizations to assist in their network defense capabilities and planning. Contents of a Circular include the purpose, a summary of the information being provided, and the details.
[14] Timely is defined by DHS as "as quickly as operationally practicable."
[15] The FSS is a segment of the economy comprised of public sector and private sector partners such as banks, lenders, credit unions, and insurance companies. The FSS conducts essential transaction services and financial operations, including data and security operations centers. Members of this sector include Treasury and the Federal Reserve System. *Presidential Policy Directive 21 - Critical Infrastructure Security and Resilience* (February 12, 2013) authorized Treasury as the Sector Risk Management Agency for FSS, and as such, Treasury creates a sector-specific risk management plan through coordination with public and private sector partners.

As part of our reporting process, we provided Treasury management an opportunity to comment on a draft of this report. In a written response, Treasury officials stated that they were pleased that this report confirmed Treasury's sharing of cyber threat indicators and defensive measures was adequate and aligned with provisions of CISA, and they concurred with the conclusions of the report. Management's response, in its entirety, is included in appendix 3 of this report.

Background

CISA Section 107, "Oversight of Government Activities," requires the Inspectors General of "appropriate Federal entities," in consultation with the IC IG and the Council of Inspectors General on Financial Oversight, to jointly report to Congress on the actions taken by the respective agencies over the recent 2-year period to carry out the provisions of CISA.

CISA did not specifically direct Treasury, among other appropriate Federal entities, to carry out cybersecurity information sharing requirements. However, CISA did direct the Office of the Director of National Intelligence (ODNI), the Department of Homeland Security (DHS), the Department of Defense, and the Attorney General to consult with the appropriate Federal entities on the following:

- the development and issuance of procedures to facilitate and promote the timely sharing of cyber threat indicators and defensive measures by the Federal Government (CISA, Section 103);
- the development and issuance of procedures for periodic sharing of cybersecurity best practices, based on ongoing analysis of cyber threat indicators, defensive measures, and cybersecurity threats (CISA, Section 103);
- the development and issuance of procedures relating to the receipt of cyber threat indicators and defensive measures by the Federal Government (CISA, Section 105);

- the development and issuance of guidelines relating to privacy and civil liberties which govern the receipt, retention, use, and dissemination of cyber threat indicators by a Federal entity obtained in connection with cyber information sharing activities (CISA, Section 105);

- a periodic review of the privacy and civil liberties guidelines developed per CISA 105(b)(2)(B), not to be conducted less frequently than once every 2 years (CISA, Section 105); and

- the development and certification of a capability and process within DHS for non-Federal entities to provide cyber threat indicators and defensive measures to the Federal Government, and for the appropriate Federal entities to receive such cyber threat indicators and defensive measures (CISA, Section 105).

Treasury's Departmental Offices carries out CISA provisions via (1) GSOC under the Office of the Chief Information Officer (OCIO), (2) OCCIP, and (3) PTR. GSOC is a 24-hour, 365-day Treasury-wide incident response and security operations team focused on the detection and mitigation of advanced threats targeted against the Department, its users, and information technology systems. GSOC acts as the centralized coordination point for Treasury bureau cyber incidents and is the liaison with the DHS United States Computer Emergency Readiness Team (US-CERT)[16] and other Federal agency incident response teams.

OCCIP coordinates Treasury's efforts to enhance the security and resilience of FSS critical infrastructure and reduce operational risk. OCCIP works closely with financial sector companies, 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.

PTR provides Treasury library services and manages the Orders and Directives program, general administration for privacy,

[16] US-CERT is an organization within the DHS Cybersecurity and Infrastructure Security Agency and is responsible for analyzing and reducing cyber threats, vulnerabilities, disseminating cyber threat warning information, and coordinating incident response activities.

transparency, records, and related procurements. PTR serves both the Federal Government community and the public by determining and setting the standards for protecting, facilitating access, preserving, retaining, and disclosing Treasury information, including PII.

Audit Results

Treasury carried out the cyber information sharing provisions of CISA during CY 2019 and CY 2020. Specifically, GSOC and OCCIP (1) designed and implemented sufficient policy, procedures, and practices to ensure the sharing of cyber threat indicators and defensive measures, including the removal of PII not directly related to a cybersecurity threat; (2) did not share classified cyber threat indicators and defensive measures with the private sector that required authorization and accounting of the security clearances; (3) took appropriate, adequate, and timely actions to disseminate cyber threat indicators shared with the Federal Government; (4) shared specific aspects of cyber threat indicators that have been shared with the Federal Government; and (5) had no barriers affecting the sharing of cyber threat indicators and defensive measures although there were reported challenges in receiving cyber information from FSS and other Federal agencies.

The following describes the detail of our assessments required by Section 107 of CISA.

a) **An assessment of the sufficiency of policies, procedures, and guidelines related to the sharing of cyber threat indicators within the Federal Government, including those related to the removal of PII that is not directly related to a cybersecurity threat.**

CISA Section 103 required that ODNI, DHS, Department of Defense, and the Attorney General jointly develop and issue procedures for the sharing of cyber threat indicators and defensive measures by the Federal Government, in consultation with the appropriate Federal entities. However, CISA did not require that the entities follow these procedures, which were documented within the DHS joint procedures documents discussed below, for sharing cyber threat indicators and defensive measures both within and outside the Federal Government. That said, GSOC and OCCIP

developed and implemented their own standard policy and procedures in alignment with DHS's policies and procedures for sharing cyber threat indicators and defensive measures both within and outside the Federal Government in the CONOPS document and *OCCIP Original Production Procedures,* respectively.

We determined that the CONOPS document was sufficiently designed by GSOC to ensure the sharing of cyber information as the procedures contained therein aligned with DHS's four policies and procedures documents (hereinafter referred to as the DHS joint procedures): (1) *Sharing of Cyber Threat Indicators and Defensive Measures by the Federal Government under the Cybersecurity Information Sharing Act of 2015* (February 16, 2016); (2) *Final Procedures Related to the Receipt of Cyber Threat Indicators and Defensive Measures by the Federal Government* (June 15, 2016); (3) *Guidance to Assist Nonfederal Entities to Share Cyber Threat Indicators and Defensive Measures with Federal Entities under the Cybersecurity Information Sharing Act of 201*5 (October 2020); and (4) *Privacy and Civil Liberties Final Guidelines: Cybersecurity Information Sharing Act of 2015* (June 15, 2016).[17] We found no discrepancies between the CONOPS and the DHS joint procedures. GSOC also tailored the CONOPS to Treasury's operating environment and included guidance for removing PII. We noted that PTR personnel were not involved with a joint review of the DHS joint procedures during CY 2019 and CY 2020, as required by Section 105. This was because DHS and the Department of Justice have not initiated coordination with the appropriate Federal agencies since 2018. Furthermore, we reviewed all nine TEWIs that GSOC shared externally during CY 2019 and CY 2020 and confirmed that they did not contain any PII.

We concluded that GSOC followed its CONOPS document for sharing cyber threat indicators and defensive measures and removing any PII not directly related to a cybersecurity threat during CY 2019 and CY 2020.

We determined that OCCIP's policies and procedures document, *OCCIP Original Production Procedures,* was sufficiently designed for the sharing of cyber threat indicators and defensive measures

[17] Developed by DHS in conjunction with the departments of Justice, Defense, Commerce, Energy, and the Treasury, and the ODNI as a result of the enactment of CISA. While the joint procedures were updated in January 2021, this fell outside the scope of our audit work.

with non-Federal Government entities in the FSS and within the Federal Government, and that the procedures aligned with the DHS joint procedures. OCCIP doesn't address PII in its *OCCIP Original Production Procedures.* However, OCCIP officials stated that the office does not receive or handle PII. We confirmed that the 15 Circulars shared externally during CY 2019 and CY 2020 did not contain any PII. We concluded that OCCIP followed its *OCCIP Original Production Procedures* for sharing cyber threat indicators and defensive measures during CY 2019 and CY 2020.

Section (c) below provides a more detailed discussion of the procedures that GSOC and OCCIP followed.

b) An assessment of whether cyber threat indicators and defensive measures have been properly classified and an accounting of the security clearances authorized for the purpose of sharing cyber threat indicators and defensive measures with the private sector.

CISA Section 103 required the development and issuance of procedures for the timely sharing of unclassified, including controlled unclassified, cyber threat indicators and defensive measures by the Federal Government with relevant Federal agencies, non-federal entities, or the public, if appropriate, in consultation with the appropriate Federal entities. The procedures were to ensure that the Federal Government has and maintains the capability to share cyber threat indicators and defensive measures in real-time consistent with the protection of classified information.

CISA does not require that the appropriate Federal entities, including Treasury, follow the DHS joint procedures for sharing cyber threat indicators and defensive measures both within and outside the Federal Government. However, in practice, GSOC shares unclassified cyber-related information indirectly with the private sector via the Financial Services - Information Sharing and Analysis Center (FS-ISAC) portals.[18] OCCIP shares unclassified cyber-related information directly with the private sector through email distribution lists, and indirectly with the private sector via both the FSS portal within the Homeland Security Information Network (HSIN), and the FS-ISAC portal.

[18] FS-ISAC is a member-owned non-profit association of financial services firms that creates and develops processes for detecting and providing information on physical or cyber security risks.

When sharing cyber threat indicators and defensive measures external to Treasury, GSOC re-designates the information from "Unclassified//For Official Use Only" to "Traffic Light Protocol (TLP) Amber,"[19] which stipulates that "Recipients may only share TLP: AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to." We noted the nine TEWIs that were shared externally in CY 2019 and CY 2020 were designated as TLP: AMBER and did not contain information that required classification at a higher level.

As GSOC operates in an unclassified environment and does not share classified information with Federal and non-Federal entities, there was no need to authorize security clearances for this purpose. As such, a review of the proper classification of classified cyber threat indicators and defensive measures was not required.

When sharing cyber threat indicators and defensive measures with the FSS, OCCIP compiles cyber information from its sources into an unclassified format. The source that is sharing any classified cyber information is the originating classifier. To include this information in a Circular, OCCIP submits a request for declassification to the Office of Intelligence and Analysis. Once declassified, the cyber information is shared via Circulars and are typically designated as TLP: GREEN, which stipulates that "Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP: GREEN information may not be released outside of the community." Circulars may also be designated as TLP: AMBER or TLP: WHITE, which is "Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction." Out of the 15 Circulars produced in CY 2019 and CY 2020, we noted that 11 Circulars shared were TLP: GREEN, 2 were TLP: AMBER, and 2

[19] TLP is a classification method used by DHS US-CERT and its participants for classifying cyber threat information shared between parties. It employs four colors to indicate expected sharing boundaries to be applied by the recipient. See https://www.us-cert.gov/tlp.

were TLP: WHITE. We reviewed the content of all 15 Circulars that were shared externally to ensure that they did not contain information that required classification at a higher level and determined that the 15 Circulars did not contain any classified information.

While Circulars are not classified, OCCIP also partnered with the Office of Intelligence and Analysis to hold monthly classified meetings with FSS leaders, representatives, and regulators who either have active security clearances issued by another Federal agency or are issued clearances under the DHS Private Sector Clearance Program for Critical Infrastructure.[20] As such, Treasury does not administer the list of authorized security clearances for private sector members, and therefore, an accounting of the security clearances authorized for the purpose of sharing classified cyber threat indicators and defensive measures would be applicable to the issuing Federal agencies. Furthermore, OCCIP officials stated that information discussed at these meetings is not actionable. As such, the information is not re-disseminated.

c) A review of the actions taken by the Federal Government based on the cyber threat indicators or defensive measures shared with the Federal Government, to include a determination on:

i. the appropriateness of subsequent uses and disseminations of cyber threat indicators and defensive measures.

As noted above, CISA does not require that all appropriate Federal entities, including Treasury, follow the DHS joint procedures for sharing cyber threat indicators and defensive measures both within and outside the Federal Government.

GSOC has used but not disseminated cyber threat indicators and defensive measures received from the private sector and other Federal agencies. According to GSOC, notifications of cyber threat indicators and defensive measures were received via the Malware

[20] The DHS Private Sector Clearance Program for Critical Infrastructure, established in 2006, ensures the processing of national security clearance applications for critical infrastructure private sector owners, operators, and industry representatives to obtain clearances to access classified information for making more informed decisions.

Information Sharing Platform,[21] and emails to an inbox that is monitored by GSOC. GSOC does not generally re-share cyber threat indicators and defensive measures, but GSOC will share if a new cyber threat indicator is discovered. GSOC only issues TEWIs related to threats detected against Treasury's network. Therefore, GSOC's subsequent use and dissemination is applicable to Treasury's networks. We found that GSOC followed its CONOPS for sharing the nine TEWIs in CY 2019 and CY 2020, and as such, the subsequent use and dissemination were appropriate as described in section (ii).

OCCIP follows its *OCCIP Original Production Procedures* for sharing cyber threat indicators with non-Federal government entities in the FSS as well as other Federal agencies. In practice, OCCIP analyzes cyber information from its sources and repackages the cyber information at an unclassified level into Circulars, which are shared via the FS-ISAC portal. As noted in section (b), OCCIP also conducts monthly classified meetings with FSS leaders, representatives, and regulators as another means of communication as needed. We determined that OCCIP appropriately disseminated cyber threat indicators and defensive measures contained in its Circulars shared with FSS in CY 2019 and CY 2020 as described in section (ii).

ii. the timeliness and adequacy of sharing cyber threat indicators and defensive measures with appropriate entities, or, if appropriate, being made publicly available.

GSOC's process to share cyber threat indicators and defensive measures is to use the information received from the Malware Information Sharing Platform to identify cyber threat indicators that are tagged as Advanced Persistent Threats[22] or general malware. After these threats are evaluated to determine their validity and to remove false positives, an alert is created in the Security Information and Event Management (SIEM)[23] tool which scans the

[21] Malware Information Sharing Platform is an open-source software for information sharing of threat intelligence available to any users for managing their own list of cyber threats.
[22] An adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple attack vectors (e.g., cyber, physical, and deception).
[23] SIEM software collects and aggregates log data generated throughout the organization's technology infrastructure.

network for matching events. In addition, manual searches for historical matches are performed for the previous 365 days. If the indicator(s) are deemed serious based on evidence from the SIEM, a TEWI with a brief description of the event and other details such as source Internet Protocol (IP)[24] addresses, timestamps, and attachments are generated manually by a GSOC analyst and shared via the following approved portals:

• FS-ISAC portal: Access is available to the financial institutions that are members of the association.

• Internal Treasury GSOC Portal: Access is available to all Treasury bureaus' Security Operation Centers.

GSOC developed nine TEWIs during CY 2019 and CY 2020. We found that GSOC shared five TEWIs in CY 2019 and four TEWIs in CY 2020 using the FS-ISAC and Internal Treasury GSOC portals. Based on our review of the externally shared TEWIs, their associated tickets, and the delivery methods/portals used, we determined that GSOC shared cyber threat information and defensive measures in a timely (i.e. as quickly as operationally practical) and adequate manner with the appropriate entities. GSOC also complied with its CONOPS document for sharing sensitive TEWIs internally with bureaus' Security Operation Centers. During the review, there were no instances where PII was present in any shared TEWI.

OCCIP's process to share cyber threat indicators and defensive measures is to compile cyber information into Circulars and share them with the original source(s) to verify that the information is unclassified. Then the Circular is approved by officials within OCCIP and the Office of General Counsel before being shared with FSS through email distribution lists such as FS-ISAC. After Circulars are shared, they are uploaded to the DHS HSIN portal where members can view them in case they did not receive the original.

OCCIP developed 15 Circulars during CY 2019 and CY 2020 (10 in CY 2019 and 5 in CY 2020). Based on our review of all 15

[24] An IP address identifies a device on the Internet or a local network. It allows a system to be recognized by other systems connected via the IP.

Circulars, we determined that OCCIP shared cyber threat indicators and defensive measures in a timely (i.e. as quickly as operationally practical) and adequate manner with appropriate FSS entities during CY 2019 and CY 2020. Additionally, we determined that there were no instances where PII was present in any Circular that was shared.

d) An assessment of the cyber threat indicators and defensive measures shared with the appropriate Federal entities to include:

i. The number of cyber threat indicators and defensive measures shared using the capability and process developed in accordance with 105(c);

Section 105(c) of CISA directs DHS to develop and implement a capability and process that accepts cyber threat indicators and defensive measures from non-Federal entities, in real time, and shares them with other Federal entities. The Automated Indicator Sharing (AIS)[25] initiative is the capability and process that DHS certified for this purpose.

While CISA 105(c) requires DHS to provide the AIS capability and process, neither GSOC nor OCCIP are required to use AIS. GSOC and OCCIP did not use information provided via AIS during CY 2019 and CY 2020. GSOC described the feed as high volume, zero context, and filled with bad cyber threat indicators. Instead of using AIS, GSOC shared the nine TEWIs using FS-ISAC and OCCIP shared the 15 Circulars using both FS-ISAC and DHS HSIN.

ii. Instances of sharing PII not directly related to a cybersecurity threat.

CISA Section 103 required that the joint procedures include a requirement that a Federal entity, prior to sharing a cyber threat indicator, assess whether it contains any PII that is not directly related to a cybersecurity threat, and implement and utilize a technical capability to remove any such PII. DHS's joint procedures contain these provisions for sharing cyber threat

[25] The AIS capability enables the real-time exchange of machine-readable cyber threat indicators and defensive measures to protect the AIS community, consisting of public and private sector partners, by identifying and helping to mitigate cyber threats through information sharing.

indicators and defensive measures, including the removal of PII that does not relate to a cybersecurity threat. However, CISA does not require the appropriate Federal entities, including Treasury, to follow the DHS joint procedures. That said, GSOC requires the removal of PII not directly related to a cybersecurity threat in the CONOPS document. As discussed above in section (a), the *OCCIP Original Production Procedures* do not address PII, and OCCIP officials stated that the office does not receive or handle PII. We confirmed that the 15 Circulars shared externally during CY 2019 and CY 2020 did not contain any PII.

As noted in section (a), we confirmed that the 9 TEWIs and 15 Circulars shared externally by GSOC and OCCIP, respectively, did not contain any PII unrelated to a cybersecurity threat.

iv. A quantitative and qualitative assessment of the effect of sharing cyber threat indicators or defensive measures on privacy and civil liberties.

CISA Section 105 required the Attorney General and DHS to jointly develop and issue guidelines relating to privacy and civil liberties which govern the receipt, retention, use, and dissemination of cyber threat indicators by a Federal entity obtained in connection with cyber information sharing activities. Per the guidelines issued by DHS and the Attorney General, *Privacy and Civil Liberties Final Guidelines: Cybersecurity Information Sharing Act of 2015* (June 15 2018), Federal entities that participate in cybersecurity information sharing activities are: (1) required to limit the receipt, retention, use, and dissemination of cyber threat indicators containing PII; and (2) comply with all other applicable US laws, orders, directives, and policies.

Treasury Directive 25-07 requires a Privacy and Civil Liberties Impact Assessment (PCLIA)[26] to be conducted for all information systems and projects that collect, maintain, or disseminate PII. A PCLIA is an assessment that must be conducted per Treasury policy to fulfill the Federal privacy

[26] Treasury Directive 25-07, *Privacy Impact Assessment (PIA)* (August 6, 2008). Treasury is in the process of updating this document to change the name of the assessment from PIA to PCLIA. It is a change in name only and not in the assessment.

requirements[27] which require, among other things, a PCLIA to be conducted before:

- developing or procuring IT systems or projects that collect, maintain, or disseminate PII from or about members of the public, or

- initiating a new collection of information that: a) will be collected, maintained, or disseminated using IT; and b) includes any PII permitting the physical or online contacting of a specific individual, if identical questions have been posed to, or identical reporting requirements imposed on, 10 or more persons. Agencies, instrumentalities, or employees of the federal government are not included.

On November 28, 2017, PTR staff performed a PCLIA for the "GSOC Network" that included: (1) an overview of its purpose and functions; (2) a description of the information collected; (3) a description of how information is maintained, used, and shared; (4) an assessment of compliance with federal requirements that support information privacy; and (5) an overview of the redress/complaint procedures available to individuals who may be affected by the use or sharing of information by the system or project. PTR concluded that GSOC did not make adverse determinations about individuals.[28]

As noted above in section (d) (ii), we confirmed that there was no PII in the 9 TEWIs and the 15 Circulars that were shared externally by GSOC and OCCIP, respectively. As such, a qualitative and quantitative assessment of the effect on privacy and civil liberties from sharing TEWIs and Circulars was not required.

[27] Federal privacy requirements are set forth in: (1) Section 208 of the E-Government Act of 2002; and (2) the Office of the Management and Budget (OMB) Memorandum 03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*.
[28] Treasury, *Privacy and Civil Liberties Impact Assessment for the Treasury Government Security Operations Center Network* (November 28, 2017).

v. The adequacy of steps taken to reduce adverse effect on the privacy and civil liberties.

As noted above, GSOC, OCCIP, and PTR personnel determined that there were no adverse effects on the privacy and civil liberties of individuals when sharing cyber threats and defensive measures during CY 2019 and CY 2020. As such, no steps were necessary to reduce adverse effects.

e) An assessment of the sharing of cyber threat indicators and defensive measures within the Federal Government to identify barriers to sharing information.

CISA section 107 requires IGs of the appropriate Federal entities to make an assessment of the sharing of cyber threat indicators or defensive measures among Federal entities to identify inappropriate barriers[29] to sharing information. We found no barriers that impeded GSOC's and OCCIP's sharing of cyber threat indicators and defensive measures with appropriate Federal and non-Federal entities as described in section (c) of this report. However, GSOC and OCCIP reported several barriers in receiving cyber threat indicators and defensive measures from other Federal entities.

GSOC officials expressed barriers when cyber threat indicator and defensive measures are received in a format that requires manual extraction, verification, and human analysis rather than automated functions to determine prioritization. Some cyber threat indicators and defensive measures were received without context, such as the time frame of an activity which is necessary to determine when an alert occurred. GSOC also noted that different trust levels between different Federal entities also created a reluctance to share information over concerns of the potential misuse of sensitive information. Furthermore, GSOC officials noted that over-classification of cyber threat indicators and defensive measures may have significantly delayed or halted GSOC's ability to analyze shared indicators, due to the amount of effort necessary to declassify and transfer the indicators to the unclassified side. GSOC officials told us that they attempt to mitigate these barriers by evaluating cyber threat indicators and defensive measure feeds based on alert precision rather than on the volume received.

[29] CISA does not define "inappropriate barriers" related to the sharing of cyber threat indicators and defensive measures.

Additionally, automated actions based on received cyber threat indicators and defensive measures are limited to the alerts from feeds that are of high confidence and trusted.

Similarly, OCCIP officials reported that requests for additional information regarding received classified cyber threat indicators and defensive measures were sometimes denied, which meant OCCIP was not able to effectively assess these classified alerts, incidents, and risks to FSS. OCCIP officials also noted other difficulties due to a reluctance by the private sector to share information with Federal entities. This included a lack of understanding of how Federal entities would use and protect the information being shared. OCCIP officials also noted they had a lack of insight into the nature of cyber events taking place in the FSS, and reported that all of these difficulties affected the quality of their responses to, and response rates to, shared incidents. Also due to this reluctance by the private sector for sharing information with Federal entities, OCCIP reported that in some cases they were not able to conduct risk analyses on, or respond in a timely fashion to, information that was received. OCCIP officials told us that they have worked to mitigate these barriers by implementing Memorandum(s) of Understanding with other Federal entities that clarified how information may be shared and used.

Conclusion

Overall, we concluded that Treasury carried out the cyber information sharing provisions of CISA during CY 2019 and CY 2020. Specifically, we determined that GSOC and OCCIP complied with Treasury policies and procedures, which aligned with the DHS joint procedures, for sharing the 9 TEWIs and 15 Circulars.

* * * * * *

I would like to extend my appreciation to the officials and personnel within the offices of the OCIO, GSOC, OCCIP, and PTR for the cooperation and courtesies extended to my staff during the audit. If you have any questions, please contact me at (202) 927-0361 or Irma Wahlstrom, Information Technology Specialist/Audit Manager, at (202) 487-0942. Major contributors to this report are listed in appendix 4.

/s/

Larissa Klimpel
Director, Cyber/Information Technology Audit

Appendix 1: Objectives, Scope, and Methodology

Our audit objective was to assess the Department of the Treasury's (Treasury) activities during calendar years (CY) 2019 and 2020 to carry out the provisions of the *Cybersecurity Information Sharing Act of 2015* (CISA), under Title I of the *Cybersecurity Act of 2015*, to share cyber threat indicators and defensive measures. We assessed the following as required by Section 107 of CISA:

a) the sufficiency of policies and procedures related to sharing cyber threat indicators within the Federal Government;

b) whether cyber threat indicators and defensive measures have been properly classified, as well as an accounting of the security clearances authorized for the purpose of sharing cyber threat indicators or defensive measures with the private sector;

c) the appropriateness, adequacy, and timeliness of the actions taken to use and disseminate cyber threat indicators or defensive measures shared with the Federal Government;

d) the specific aspects of cyber threat indicators or defensive measures that have been shared with the Federal Government; and

e) barriers affecting the sharing of cyber threat indicators or defensive measures.

The scope of our audit comprised Treasury's cyber information sharing policies and procedures issued by the Government Security Operations Center (GSOC) and the Office of Cybersecurity and Critical Infrastructure Protection (OCCIP). The scope of our audit also included GSOC's and OCCIP's activities for sharing cyber threat indicators and defensive measures contained in 9 Treasury Early Warning Indicators (TEWIs) and 15 Circulars during CY 2019 and CY 2020. We conducted this audit remotely between January 2021 and August 2021.

To accomplish our audit objectives, we performed the following steps:

- reviewed the provisions of CISA applicable to Federal agencies to include Sections 103, 105, and 107;
- reviewed the Department of Homeland Security's (DHS) four policy and procedure documents: (1) *Sharing of Cyber Threat Indicators and Defensive Measures by the Federal Government under the Cybersecurity Information Sharing Act of 2015* (February 16, 2016); (2) *Final Procedures Related to the Receipt of Cyber Threat Indicators and Defensive Measures by the Federal Government* (June 15, 2016); (3) *Guidance to Assist Nonfederal Entities to Share Cyber Threat Indicators and Defensive Measures with Federal Entities under the Cybersecurity Information Sharing Act of 2015* (October 2020); and (4) *Privacy and Civil Liberties Final Guidelines: Cybersecurity Information Sharing Act of 2015* (June 15, 2018);
- reviewed GSOC's *Threat Indicator Sharing Concept of Operations* (March 20, 2017) policy, procedures, guidelines, and practices for sharing cyber threat indicators and defensive measures within the Federal Government and with Non-Federal Government entities;
- reviewed OCCIP's *OCCIP Original Production* (October 1, 2020) policy, procedures, guidelines, and practices for sharing cyber threat indicators and defensive measures with Non-Federal Government entities in the financial services sector and within the Federal Government;
- applied the common question set created by the Intelligence Community Inspectors General for the purpose of the Section 107 joint report (see appendix 2);
- evaluated the responses to the common question set applicable to GSOC, OCCIP, and the Office of Privacy and Transparency (PTR);
- conducted interviews with (1) GSOC officials and staff responsible for monitoring and sharing of cyber threat indicators and defensive measures with Federal and Non-Federal entities, and (2) OCCIP officials and staff responsible

for monitoring intelligence and sharing cyber threat indicators and defensive measures with the financial services sector;

- performed a walkthrough of GSOC's and OCCIP's process for sharing and receiving cyber threat indicators and defensive measures with Federal and Non-Federal Government entities;
- examined GSOC's internal tickets and associated TEWIs that were shared by GSOC during CY 2019 and CY 2020;
- reviewed the Circulars that were shared by OCCIP during CY 2019 and CY 2020;
- conducted a data call with PTR official responsible for conducting Privacy and Civil Liberties Impact Assessments;
- reviewed the Privacy and Civil Liberties Impact Assessment for all information systems and projects that collect, maintain, or disseminate personally identifiable information;
- reviewed the Government Accountability Office's (GAO) *Standards for Internal Control in the Federal Government* (September 2014) to identify the components and principles of internal control that are significant within the context of the audit objectives. We determined that the control environment, control activities, information and communication, and monitoring components were significant to our audit objectives. Specifically we assessed policies, procedures, and guidance against the following principles in which management should: (1) design control activities to achieve objectives and respond to risks; (2) implement control activities through policies; (3) use quality information to achieve the entity's objectives; (4) internally communicate the necessary quality information to achieve the entity's objectives; (5) externally communicate the necessary quality information to achieve the entity's objectives; (6) establish and operate monitoring activities to monitor the internal control system and evaluate the results; and (7) remediate identified internal control deficiencies on a timely basis.
- reviewed GAO's *Assessing Data Reliability* guidance which states that a data reliability determination does not involve attesting to the overall reliability of the data or database. For this audit, the audit team determined the reliability of the

specific data needed to support our assessment of Treasury's sharing of cyber threats and defensive measures and our conclusions in the context of the audit objectives. Specifically, we (1) compared GSOC's *Threat Indicator Sharing Concept of Operations* (March 20, 2017) and OCCIP's *OCCIP Original Production* (October 1, 2020) policy, procedures, guidelines, and practices to DHS' four policy and procedure documents to determine that they were sufficiently designed and implemented for the sharing of cyber threat indicators and defensive measures; (2) conducted walkthroughs of GSOC and OCCIP's processes for receiving and sharing cyber threat indicators and defensive measures to validate processes against policies and procedures; (3) validated data contained in TEWIs and Circulars by comparing data against information in the external portals (Financial Services - Information Sharing and Analysis Center and the Financial Services Sector portal within the Homeland Security Information Network); and (4) interviewed and obtained information from officials knowledgeable about processes and data for receiving and sharing cyber threat indicators and defensive measures. We determined that the data was sufficiently reliable for the purposes of answering our audit objectives.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix 2: Common Question Set

Below is the common question set developed by the Inspector General of the Intelligence Community (IC IG) for conducting assessments required under Section 107 of the Cybersecurity Information Sharing Act (CISA) of the Cybersecurity Act of 2015[30] related to executive branch agencies cyber information activities in calendar years (CY) 2019 and 2020. Responses to the common question set are provided to the IC IG separately from this report.

Section 107(b) Joint Project Steps

Background

CISA Section 107(b) requires the IGs of the appropriate Federal entities (departments of Commerce, Defense, Energy, Homeland Security (DHS), Justice, the Treasury, and Office of the Director of National Intelligence (ODNI), in consultation with the IC IG and Council of IGs on Financial Oversight, to jointly submit to Congress an interagency report on their actions over the most recent 2-year period to carry out this title.[31] According to CISA Section 107(b), the contents of the joint report shall include:

A. An assessment of the sufficiency of policies and procedures related to sharing cyber threat indicators within the Federal Government, including the removal of personally identifiable information (PII). (Steps 1-8)

B. An assessment of whether cyber threat indicators and defensive measures have been properly classified and an accounting of the security clearances authorized for the purpose of sharing cyber threat indicators and defensive measures with the private sector. (Steps 9-13)

C. A review of the actions taken by the Federal Government to share cyber threat indicators and defensive measures, to include a

[30] P.L. 114-113, Division N (December 18, 2015)
[31] Title I—*Cybersecurity Information Sharing Act of 2015*, Section 107, Oversight of Government Activities.

determination on the timeliness, adequacy, and appropriateness of the sharing. (Steps 14-17)

D. An assessment of the cyber threat indicators and defensive measures shared with the appropriate Federal entities to include:

i. The number of cyber threat indicators and defensive measures shared using the capability and process developed in accordance with 105(c). (Steps 18-21)

ii. Instances of sharing PII not directly related to a cybersecurity threat. (Step 22)

iii. According to the Attorney General, the number of times information shared under CISA was used by a Federal entity to prosecute an offense. (Department of Justice only)

iv. A quantitative and qualitative assessment of the effect of sharing cyber threat indicators or defensive measures on privacy and civil liberties. (Steps 23-24)

v. The adequacy of steps taken to reduce adverse effect on the privacy and civil liberties. (Step 25)

E. An assessment of the sharing of cyber threat indicators and defensive measures within the Federal Government to identify barriers to sharing information. (Step 26)

Definitions:

Question 14a – *Appropriately* – used and disseminated the information to individuals/entities with appropriate security clearances [Section 103(b)(1)(A)], only used and disseminated information related to a cybersecurity threat without disclosing personal information of a specific individual or identifying a specific individual, and protected the information from unauthorized use [See Section 105(a)(4)(B)].

Question 15a – *Timely* – agency shared in an automated manner, in real-time or as quickly as operationally practical with appropriate Federal entities. [Section 105(a)(3)(A)]

Question 15a – *Adequate Manner* – agency shared only relevant and useful information related to a cybersecurity threat and protected the information from unauthorized access. [See Section 103(b)(1)(D)]

Question 15a - *Appropriate entities* – agency used the appropriate sharing capability to ensure receipt by entities with the need for the cyber threat information and with the proper clearances based on the classification of the information.

** Additional guidance for responding to question 15a can be obtained from the procedure document, *Sharing of Cyber Threat Indicators and Defensive Measures by the Federal Government under CISA*.

Question 17a – *Timely* – other Federal entities shared in an automated manner, in real-time or shared quickly so that the data received was still relevant and useful. [Section 105(a)(3)(A)]

Question 17a – *Adequate* – other Federal entities shared relevant and useful information related to a cybersecurity threat and protected the information from unauthorized access. [See Section 103(b)(1)(D)]

Question 17a – *Appropriate Manner* – other Federal entities shared using the appropriate sharing capability to ensure receipt by entities with the need for the cyber threat information and with the proper clearances based on the classification of the information.

**Additional guidance for responding to question 17a can be obtained from the procedure document, *Final Procedures Related to the Receipt of Cyber Threat Indicators and Defensive Measures by the Federal Government.*

Question 25a - Adequate steps – the steps taken reduced/mitigated the adverse effects on the privacy and civil liberties of U.S. persons. Also see the procedure document, *Privacy and Civil Liberties Final Guidelines: CISA*.

Project Steps:

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

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

3. Do the policies, procedures, and guidelines include guidance for removing information not directly related to a cybersecurity threat that is personal information of a specific individual or information that identifies a specific individual?

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

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

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

7. If there are differences in the policies, procedures, and guidelines implemented among the agencies, does it impact the sharing of cyber threat information? (Offices of Inspector General can first determine whether not using the four procedure documents impacts the sharing – IC IG will coordinate additional follow-up, if necessary)

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

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

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

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

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

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

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

    a. If yes, how did the agency account for the number of security clearances and how many security clearances were active in CYs 2019 and 2020?

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

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

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

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

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

    a. If yes, review a sample to determine whether the agency shared the cyber threat information in a timely

and adequate manner with appropriate entities or, if appropriate, made publicly available. Provide results.

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

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

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

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

19. (For DHS only) How many of those cyber threat indicators and defensive measures reported for question 23 did Department of Homeland Security share with other Federal entities CYs 2019 & 2020? Provide results.

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

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

22. Did any Federal or non-Federal entity share information with the agency that was not directly related to a cybersecurity threat that contained personally identifiable information (PII)?

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

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

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

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

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

25. Was there any adverse effect on the privacy and civil liberties of U.S. persons due to the activities carried out under this title by the agency?

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

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

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

    b. Any difficulties due to classification of information?

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

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

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

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

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

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

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

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

Appendix 3: Management Response

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C.

MEMORANDUM FOR LARISSA KLIMPEL
DIRECTOR, INFORMATION TECHNOLOGY AUDIT

FROM: Tony Arcadi Antony P. Arcadi Digitally signed by Antony P. Arcadi Date: 2021.10.29 11:20:21 -04'00'
Acting Deputy Assistant Secretary for Information Systems and Chief Information Officer

Paul Neff Paul E. Neff Digitally signed by Paul E. Neff Date: 2021.10.28 16:24:47 -04'00'
Director, Cyber Policy, Preparedness, and Response

SUBJECT: Management Response to Draft Audit Report - *Audit of the Department of the Treasury's Cybersecurity Information Sharing*

Thank you for the opportunity to review the draft report, *Audit of the Department of the Treasury's Cybersecurity Information Sharing,* assessing Treasury's cybersecurity information sharing provisions of the Cybersecurity Information Sharing Act (CISA). We are pleased the report continues to confirm Treasury's activities sharing cyber threat indicators and defensive measures were adequate and aligned with provisions of CISA.

The Office of Cybersecurity and Critical Infrastructure Protection and the Office of Chief Information Officer concur with the conclusions of this report. We thank the Office of the Inspector General for their thorough analysis and professionalism throughout this audit.

Appendix 4: Major Contributors to This Report

Mitul "Mike" Patel, Audit Manager
Irma Wahlstrom, Audit Manager
Joshua Matadial, Auditor-In-Charge
David Studley, IT Specialist
Jung "Hyub" Lee, IT Specialist
Shedaun Smith, IT Specialist
Christine Vaing, IT Specialist
Patrick Arnold, Referencer

Appendix 5: Report Distribution

Department of the Treasury

Deputy Secretary
Assistant Secretary for Management
Office of the Chief Information Officer
Director, Government Security Operations Center
Director, Office of Privacy, Transparency, and Records
Director, Office of Cybersecurity and Critical Infrastructure Protection
Office of Strategic Planning and Performance Improvement
Office of the Deputy Chief Financial Officer, Risk and Control Group

Office of Management and Budget

Office of Inspector General Budget Examiner

Inspector General of the Intelligence Community

Office of the Inspector General of the Intelligence Community

This Page Intentionally Left Blank

REPORT WASTE, FRAUD, AND ABUSE

Submit a complaint regarding Treasury OIG Treasury Programs and Operations using our online form:
https://oig.treasury.gov/report-fraud-waste-and-abuse

TREASURY OIG WEBSITE

https://oig.treasury.gov/