Audit Report

OIG-26-027

CYBERSECURITY/INFORMATION TECHNOLOGY

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

March 27, 2026

Office of Inspector General
Department of the Treasury

This Page Intentionally Left Blank

Contents

Audit Report

Results in Brief 4

Background 5

Audit Results 6

Appendices

Appendix 1: Objectives, Scope, and Methodology 17
Appendix 2: Common Question Set 21
Appendix 3: Management Response 30
Appendix 4: Major Contributors to This Report 31
Appendix 5: Report Distribution 32

Abbreviations

AIS	Automated Indicator Sharing
CI	Office of Counterintelligence
CY	Calendar year
CIGFO	Council of Inspectors General on Financial Oversight
CISA	Cybersecurity Information Sharing Act of 2015
CTIIN-FIN	Cyber Threat Intelligence & Indicators Notice
CONOPS	Threat Indicator Sharing Concept of Operations
DHS	Department of Homeland Security
FBIIC	Finance and Banking Infrastructure Committee
FSS	Financial Services Sector
IC IG	Inspector General of the Intelligence Community
IG	Inspector General
MISP	Malware Information Sharing Platform
OCCIP	Office of Cybersecurity and Critical Infrastructure Protection
ODNI	Office of the Director of National Intelligence
OIG	Office of Inspector General
PII	Personally identifiable information
PTR	Office of Privacy, Transparency, and Records
TEWI	Treasury Early Warning Indicators
TLP	Traffic Light Protocol
Treasury	Department of the Treasury
TSSSOC	Treasury Shared Services Security Operations Center

This Page Intentionally Left Blank

Audit Report

March 27, 2026

Samuel Corcos
Deputy Assistant Secretary, Information Systems and Chief Information Officer

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 fifth biennial report to support the joint report.[5]

Our audit objective was to assess Treasury's activities related to sharing cyber threat indicators and defensive measures per the

[1] Pub. L. 114-113, Division N Cybersecurity Information Sharing Act, pages 696-716 (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), *Audit of the Department of the Treasury's Cybersecurity. Information Sharing (*OIG-20-019; December 10, 2019*), Audit of the Department of the Treasury's Cybersecurity Information Sharing (*OIG-22-013; November 23, 2021) *and Audit of the Department of the Treasury's Cybersecurity Information Sharing (OIG-25-007; November 14, 2024)*.

provisions of CISA during calendar years (CYs) 2023 and 2024; and respond to the common question set created for the joint report. 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 and procedures related to sharing cyber threat indicators within the Federal Government, including the removal of personally identifiable information (PII);[7]

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 and 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] Pub. 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 cybersecurity information sharing policies and procedures as well as activities for sharing cyber threat indicators and defensive measures during CYs 2023 and 2024. 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 Treasury Shared Services Security Operations Center's (TSSSOC) *Threat Indicator Sharing Concept of Operations* (CONOPS) (February 15, 2023, and February 6, 2025); the Office of Cybersecurity and Critical Infrastructure Protection (OCCIP) *OCCIP Original Production and Information Dissemination Procedures* (January 7, 2022) and its *Unclassified Threats Exchange SOP* (March 28, 2025). We also applied the common question set provided by the IC IG to make the assessments required by Section 107 of CISA, and reviewed and evaluated the responses provided by TSSSOC, OCCIP, and the Office of Privacy, Transparency, and Records (PTR). We reviewed four Treasury Early Warning Indicators (TEWIs) containing cyber threat indicators and defensive measures that TSSSOC shared with appropriate entities during CYs 2023 and 2024. We also reviewed 118 products, which include 61 Circulars, 19 Cyber Threat Intelligence & Indicators Notices (CTIIN-FINs),[10]

[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] CTIIN-FINs are shared "as -is" by OCCIP in coordination with Treasury's Financial Crimes Enforcement Network and consist of relevant information on cybercriminal activity and indicators potentially associated with cyber-enabled financial origins derived from various sources, including U.S. government research and private financial sector reporting.

27 Indicator Notices,[11] and 11 Spotlight Reports containing cyber threat indicators and defensive measures that OCCIP shared with appropriate entities during CYs 2023 and 2024. We conducted this audit remotely between December 2024 and August 2025. Appendix 1 contains a more detailed description of our objectives, 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 CYs 2023 and 2024 were adequate and aligned with CISA's provisions. Specifically, TSSSOC 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[12] 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 that adversely affected the sharing of cyber threat indicators and defensive measures although there were reported difficulties in receiving cyber threat information.

As part of our reporting process, we provided Treasury management with an opportunity to comment on a draft of this report. In a memorandum, management shared that they were pleased the report states that Treasury cyber threat sharing and defensive measures in calendar year 2023 and 2024 were deemed adequate and aligned with the CISA. Additionally, management concurred with the lack of barriers to sharing cyber threat information and defensive measures; and noted that despite the reported difficulties in receiving cyber threat information, there

[11] Indicator Notices are shared "as-is" by OCCIP and are intended to assist network defense efforts by informing cybersecurity practitioners of indicators associated with malicious cyber activity.

[12] Timely is defined by CISA as "shared in an automated manner, in real-time or as quickly as operationally practical."

have not been any adverse impacts. Furthermore, officials from the OCCIP and the Office of the Chief Information Officer concurred with the conclusions of the report. Appendix 3 contains the management response in its entirety.

Background

Section 107 of CISA, "Oversight of Government Activities," requires the Inspectors General of "appropriate Federal entities," in consultation with the IC IG and CIGFO, 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 carry out CISA provisions via (1) TSSSOC under the Office of the Chief Information Officer, (2) OCCIP, and (3) PTR. TSSSOC is a Treasury-wide security operations center providing security monitoring, incident coordination, incident response, and reports of threats targeted against the Department, its users, and information technology systems. TSSSOC acts as the centralized coordination point for Treasury bureau cyber incidents and is the liaison with the Cybersecurity and Infrastructure Security Agency.

OCCIP coordinates Treasury's efforts to enhance the security and resilience of the Financial Services Sector (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, Paperwork Reduction Act, and general administration for privacy, transparency, records, and related procurements. PTR serves both the Federal Government community and the public by determining and setting the standards for collecting, protecting, facilitating access, preserving, retaining, and disclosing Treasury information, including PII.

Audit Results

Treasury carried out the cyber information sharing provisions of CISA during CYs 2023 and 2024. Specifically, TSSSOC 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 that adversely affected the sharing of cyber threat indicators and defensive measures although there were reported difficulties in receiving cyber threat information.

The following summarizes our assessment as required by Section 107 of CISA:

a) An assessment of the sufficiency of policies and procedures related to sharing cyber threat indicators within the Federal Government, including the removal of PII.

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. Both TSSSOC and OCCIP opted to develop and implement their own standard policies and procedures for sharing cyber threat indicators and defensive measures to align with DHS's four procedures documents (hereinafter referred to as the DHS joint procedures):[13] (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, updated October 2021); (3)

[13] Developed by DHS in conjunction with the Department of Justice, Defense, Commerce, Energy, and the Treasury, and the ODNI as a result of the enactment of CISA.

Guidance to Assist Nonfederal Entities to Share Cyber Threat Indicators and Defensive Measures with Federal Entities under the Cybersecurity Information Sharing Act of 2015 (June 2016, updated April 2024); and (4) *Privacy and Civil Liberties Final Guidelines: Cybersecurity Information Sharing Act of 2015* (June 15, 2018, updated November 2022).
We determined that TSSSOC designed the CONOPS document sufficiently to ensure the sharing of cyber threat information as the procedures contained therein aligned with DHS joint procedures. We found no discrepancies between the procedures in the CONOPS document and the DHS joint procedures. The CONOPS also included guidance for redacting information not directly related to a cybersecurity threat that is personal information of a specific individual unless they obtain specific direction from Treasury leadership. We reviewed all four products that were shared by TSSSOC and confirmed that no PII was involved.

We concluded that TSSSOC followed its CONOPS document for sharing cyber threat indicators and defensive measures; and removed information not directly related to a cybersecurity threat that is personal information during CYs 2023 and 2024.

We determined that OCCIP designed the *OCCIP Original Production and Information Dissemination Procedures* and the *Unclassified Threats Exchange SOP* sufficiently to ensure the sharing of cyber threat information as the procedures contained therein aligned with DHS joint procedures. The *OCCIP Original Production and Information Dissemination Procedures* describes how OCCIP shares cyber threat indicators within the FSS and partner organizations. The *Unclassified Threats Exchange SOP* describes OCCIP's process for conducting unclassified threats exchange briefings, which are held monthly to share topical cyber threat indicators and defensive measures. While neither of their policies state how instances of PII are handled since OCCIP does not use the collection of PII in performing its functions, OCCIP follows Treasury's requirements for safeguarding against and responding to breach of PII.[14] We reviewed all 118 products that were shared by OCCIP and confirmed that no PII was involved.

[14] Treasury Directive 25-08 *Safeguarding Against and Responding to the Breach of Personally Identifiable Information* (July 16, 2024).

We concluded that OCCIP followed both the *OCCIP Original Production and Information Dissemination Procedures* and the U*nclassified Threats Exchange SOP* for sharing cyber threat indicators and defensive measures; and removed information not directly related to a cybersecurity threat that is personal information during CYs 2023 and 2024.

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.

TSSSOC does not share classified information with federal and non-federal agencies. Therefore, they do not authorize security clearances for the purpose of sharing cyber threat indicators. However, TSSSOC reported that they maintain an adequate number of cleared staff for reviewing classified information. Additionally, TSSSOC considered onboarding delays to be a barrier when dealing with attrition of cleared staff.

We reviewed the four TEWI's shared by TSSSOC during CY 2023 and 2024 and confirmed that no classified information was present, and that they were at the appropriate classification level.

OCCIP does not share classified information with federal and non-federal agencies. Also, OCCIP only nominates individuals for security clearances, it does not authorize clearances. During CYs 2023 and 2024, OCCIP nominated 308 security clearances. Additionally, OCCIP reported that they maintain sufficient active security clearances for their information sharing and mitigation efforts.

We reviewed the 118 products shared by OCCIP during CY 2023 and 2024 and confirmed that no classified information was present, and that they were at the appropriate classification level.

c) A review of the actions taken by the Federal Government based on cyber threat indicators and defensive measures shared with the Federal Government, to include a determination on the timeliness, adequacy, and appropriateness of the actions.

TSSSOC used and disseminated cyber threat indicators and defensive measures shared by other Federal agencies. As reported in the fiscal year 2023 Audit Report,[15] TSSSOC does not share indicators already disseminated by outside agencies unless a new actionable indicator was discovered.

TSSSOC reported that they receive cyber threat information from numerous sources, which is then fed directly into the Malware Information Sharing Platform (MISP).[16] MISP then aggregates all cyber threat information and tags it so the data could be categorized by sources. It is then converted to a format readable by a Security Information and Event Management tool,[17] which is used to search historical and current data on Treasury networks to look for any indicators of compromise.

TSSSOC shared cyber threat information with the Cybersecurity and Infrastructure Security Agency via email. Additionally, TSSSOC shared cyber threat information internally with Treasury bureaus and offices (including OCCIP), and externally via OCCIP who further shared with the FSS. When appropriate, TSSSOC shares cyber threat information with the Federal Bureau of Investigation, and National Security Agency primarily through collaboration with Treasury's Office of Counterintelligence (CI) via email and meetings.

For CYs 2023 and 2024, TSSSOC shared four TEWIs containing cyber threat indicators and defensive measures. These TEWIs were

[15] *Audit of the Department of the Treasury's Cybersecurity Information Sharing* (OIG-25-007) (November 14, 2024)

[16] MISP is an open-source threat intelligence and sharing platform.

[17] A Security Information and Event Management software tool centrally collects, stores, and analyzes logs from various sources. It monitors for security threats in real time for quick attack detection, containment, and response.

appropriately designated using the Traffic Light Protocol (TLP).[18] One TEWI was designated TLP: AMBER, which stipulates that the receiving entity cannot share the information with anyone outside of their organization and its clients, and was shared with the Cybersecurity and Infrastructure Security Agency. Two TEWIs were designated TLP: CLEAR, which stipulates that the information is free to share, and were shared internally with Treasury bureaus and offices (including OCCIP). One TEWI was designated TLP: AMBER+STRICT, which stipulates the receiving entity cannot share the information with anyone outside of their organization, and was shared with the FSS via OCCIP.[19]

We reviewed the four TEWIs shared and determined that TSSSOC followed its CONOPS document; and the TEWIs were shared as soon as possible, in an adequate manner, and with the appropriate entities.

OCCIP used and disseminated cyber threat indicators and defensive measures shared by other Federal agencies. However, they did not directly receive cyber threat indicators and defensive measures from other Federal agencies. They received declassified information from Treasury's Office of Intelligence and Analysis. Although OCCIP receives cyber threat indicators and defensive measures, they do not actively use the cyber threat information to mitigate threats, as OCCIP's role is solely to share information and not to directly mitigate potential threats.

OCCIP shared cyber threat information with Finance and Banking Infrastructure Committee (FBIIC) members and the Cybersecurity and Infrastructure Security Agency using email and the Financial Services Information Sharing and Analysis Center. Furthermore, OCCIP has supplemented the process of sharing cyber threat indicators from a variety of sources through its Automated Threat Information Feed (ATIF) program that was launched on May 9, 2024. The ATIF program is intended to help financial institutions

[18] 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).

[19] The TEWI was created by TSSSOC and shared with OCCIP on December 30, 2024; but OCCIP did not share the resulting Indicator Notice, containing the indicators from the TEWI, with the FSS until January 3, 2025. As such, the TEWI was counted for TSSSOC this audit period, but the corresponding Indicator Notice was not counted for OCCIP.

improve their network defense by aggregating data sources tailored to the needs of financial institutions in a single place to enable faster and more efficient detection of malicious activity targeting the sector.

For CYs 2023 and 2024, OCCIP shared 118 products in the form of Circulars, CTIIN-FINs, Indicator Notices, and Spotlight Reports. These products were designated using the TLP. Of the 118 products, 110 were designated TLP: AMBER and eight items were designated TLP: GREEN, which stipulates that recipients may share the information with peers and partner organizations within their sector or community, but not via publicly accessible channels. We reviewed the products shared and determined that OCCIP followed its procedural documents and shared the information in a timely and adequate manner with the appropriate entities.

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

1. 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 directed 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 share them with other Federal entities.

The DHS Automated Indicator Sharing (AIS) initiative is the Federal Government's primary mechanism for exchanging unclassified cyber threat indicators and defensive measures with Federal and non-Federal entities, enabling the automated exchange of machine-readable information sharing, as required by CISA, Section 105(c).

While CISA 105(c) requires DHS to provide the AIS capability and process, neither TSSSOC nor OCCIP are required to use AIS. TSSSOC opted not to use either AIS 1.0 or 2.0 during CYs 2023 and 2024. TSSSOC reported that AIS 2.0 has not resolved the previously experienced issue with high volume of unactionable cyber threat indicators; instead, they used a threat intelligence aggregator to receive cyber threat indicators from DHS for CYs 2023 and 2024. OCCIP reported that they did not

have access to either AIS 1.0 or 2.0 during CYs 2023 and 2024. However, OCCIP's ATIF aggregates cyber threat indicators from various open sources and U.S. government data sources, which are inclusive of CISA/DHS indicator releases tailored to the needs of financial institutions in a single place to enable faster and more efficient detection of malicious activity targeting the sector.

2. **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 indicators and defensive measures, including the removal of PII that does not relate to a cybersecurity threat.

   TSSSOC requires the redaction or removal of PII and sensitive internal data and the obfuscation of all threat information and indicators of compromise to prevent unwanted interaction according to the CONOPS document. While neither the *OCCIP Original Production and Information Dissemination Procedures* nor their *Unclassified Threats Exchange SOP* state how instances of PII are handled, OCCIP follows Treasury's requirements to ensure the removal of PII that does not relate to a cybersecurity threat.

   TSSSOC and OCCIP reported that no Federal or non-Federal entity shared information with them that contained PII that was not directly related to a cybersecurity threat.

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

   This question is applicable to DOJ only.

4. **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 in coordination with heads of the appropriate Federal entities 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, updated November 2022), 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 U.S. laws, orders, directives, and policies.

PTR reported that there were no privacy and civil liberties of any individuals affected due to sharing cyber threat indicators or defensive measures during CYs 2023 and 2024 by TSSSOC or OCCIP. PTR also reported that there were no notices received regarding the failure to remove information that was not directly related to a cybersecurity threat during CYs 2023 and 2024 by either TSSSOC or OCCIP.

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

   TSSSOC and OCCIP reported there were no adverse effects on the privacy and civil liberties of U.S. persons due to the activities carried out under Section 107 of CISA during CYs 2023 and 2024. PTR confirmed that there were no adverse effects. As such, we did not assess whether adequate steps were taken to mitigate 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.

Section 107 of CISA requires Inspectors General (IG) of the appropriate Federal entities to assess the sharing of cyber threat indicators or defensive measures among Federal entities to identify

inappropriate barriers[20] to sharing information. We identified several potential barriers but found that they did not significantly or adversely affect Treasury's ability to share cyber threat indicators and defensive measures among Federal entities.

TSSSOC reported that many sharing partners continue to operate under the assumptions of an outdated threat landscape and provide inaccurate, sloppy and/or unspecific reporting that can overwhelm a security operations center. Additionally, TSSSOC noted that trusted third party's cyber threat information is passed along without independent verification, then upon investigation by TSSSOC, said cyber threat information did not represent a threat. Lastly, TSSSOC reported that indicator sourcing is inherently problematic – the fewer controls on the upload side, the higher the probability of bad indicators becoming part of the product.

OCCIP has reported in previous years that they have experienced difficulties due to reluctance of sharing information from the private sector due to concerns over potential misuse of sensitive information. However, during CYs 2023 and 2024, OCCIP did not report any reluctance from private sector partners as they implemented a FBIIC memorandum regarding the treatment of non-public information shared among the federal agency members of the FBIIC.

Conclusion

Overall, we concluded that Treasury carried out the cyber information sharing provisions of CISA during CYs 2023 and 2024. Specifically, we determined that TSSSOC and OCCIP complied with Treasury's policies and procedures, which aligned with the DHS joint procedures, when sharing 4 TEWIs, 61 Circulars, 19 CTIIN-FINs, 27 Indicator Notices, and 11 Spotlight Reports.

* * * * * *

I would like to extend my appreciation to the officials and personnel within the Office of Chief Information Officer, TSSSOC, OCCIP, and PTR for the cooperation and courtesies extended to my

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

staff during the audit. If you have any questions, please contact me at (202) 972-0361 or Mitul Patel, Information Technology Audit Manager, at (202) 503-7840. 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 objective was to assess the Department of the Treasury's (Treasury) activities during calendar years (CYs) 2023 and 2024 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 cybersecurity information sharing policies and procedures issued by Treasury Shared Services Security Operations Center (TSSSOC) and the Office of Cybersecurity and Critical Infrastructure Protection (OCCIP). The scope of our audit also included TSSSOC's and OCCIP's activities for sharing cyber threat indicators and defensive measures contained in TSSSOC's 4 Treasury Early Warning Indicators (TEWIs) and OCCIP's 118 products, comprised of 61 Circulars, 19 Cyber Threat Intelligence & Indicators Notices (CTIIN-FINs), 27 Indicator Notices, and 11 Spotlight Reports during CYs 2023 and 2024.

To accomplish these objectives, we performed the following activities during audit fieldwork conducted from December 2024 through August 2025:

- 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, updated October 2021); (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* (June 2016, updated April 2024); and (4) *Privacy and Civil Liberties Final Guidelines: Cybersecurity Information Sharing Act of 2015* (June 15, 2018, updated November 2022);
- reviewed TSSSOC's *Threat Indicator Sharing Concept of Operations* (February 15, 2023 and February 6, 2025) 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 and Information Dissemination Procedures* (January 7, 2022) and *Unclassified Threats Exchange SOP* (March 28, 2025) policy, procedures, guidelines, and practices for sharing cyber threat indicators and defensive measures with Non-Federal Government entities in the Financial Services sector (FSS) and within the Federal Government;
- applied the common question set created by the Intelligence Community Inspector General for the purpose of the Section 107 joint report (see Appendix 2);
- evaluated the responses to the common question set applicable to TSSSOC, OCCIP, and the Office of Privacy, Transparency, and Records;
- conducted interviews with (1) TSSSOC 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 (FSS);

- performed walkthroughs of TSSSOC's and OCCIP's processes for sharing and receiving cyber threat indicators and defensive measures with Federal and Non-Federal Government entities;
- reviewed all four TEWIs that were shared by TSSSOC during CYs 2023 and 2024;
- reviewed all 118 products that were shared by OCCIP during CYs 2023 and 2024;
- reviewed the Government Accountability Office's *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 and procedures against the following principles in which management should:
    - establish an organizational structure, assign responsibility, and delegate authority to achieve the entity's objectives;
    - identify, analyze, and respond to risks related to achieving the defined objectives;
    - identify, analyze, and respond to significant changes that could impact the internal control system;
    - design control activities to achieve objectives and respond to risks;
    - design activities for the information system;
    - implement control activities through policies;
    - use quality information to achieve the entity's objectives;
    - internally communicate the necessary quality information to achieve the entity's objectives;
    - externally communicate the necessary quality information to achieve the entity's objectives;
    - establish and operate monitoring activities to monitor the internal control system and evaluate the results; and
    - remediate identified internal control deficiencies on a timely basis.

- reviewed the Government Accountability Office'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 TSSSOC's Threat Indicator Sharing Concept of Operations (February 15, 2023 and February 6, 2025), OCCIP's *OCCIP Original Production and Information Dissemination Procedures* (January 7, 2022) and its *Unclassified Threats Exchange SOP* (March 28, 2025) to DHS's four policy and procedure documents to determine whether they were sufficiently designed and implemented for the sharing of cyber threat indicators and defensive measures; (2) conducted walkthroughs of TSSSOC 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 all the products and reports (i.e., Circulars, CTIIN-FINs, Indicator Notices, and Spotlight Reports) shared by TSSSOC and OCCIP to validate timeliness within Treasury; 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

The common question set, described below, was 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 related to executive branch agencies' cybersecurity information sharing activities in calendar years (CYs) 2023 and 2024. 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 (Commerce, DoD, Energy, DHS, Justice, Treasury, and 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 title1. 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). Section 107(b)(2)(A) (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. Section 107(b)(2)(B) (Steps 9-13)

C. A review of the actions taken by the Federal Government based on cyber threat indicators and defensive measures shared with the Federal Government, to include a determination on the timeliness, adequacy, and appropriateness of the actions. Section 107(b)(2)(C) (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). Section 107(b)(2)(D)(i) (Steps 18-21)

   II. Instances of sharing PII not directly related to a cybersecurity threat. Section 107(b)(2)(D)(ii) (Steps 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. Section 107(b)(2)(D)(iii) (DOJ only)

   IV. A quantitative and qualitative assessment of the effect of sharing cyber threat indicators or defensive measures on privacy and civil liberties. Section 107(b)(2)(D)(iv) (Steps 23-24)

   V. The adequacy of steps taken to reduce adverse effect on the privacy and civil liberties. Section 107(b)(2)(D)(v) (Steps 25)

E. An assessment of the sharing of cyber threat indicators and defensive measures within the Federal Government to identify barriers to sharing information. Section 107(b)(2)(E) (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 [See 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 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 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 procedure document, Privacy and Civil Liberties Final Guidelines: CISA.

Procedure Documents:

1. Final Procedures Related to the Receipt of Cyber Threat Indicators and Defensive Measures by the Federal Government (June 2016, updated October 2021) provides a process for receiving, handling, and disseminating information shared with and from DHS, including the use of the AIS capability.
2. Privacy and Civil Liberties Final Guidelines: Cybersecurity Information Sharing Act of 2015 (June 2018, updated November 2022) addresses limiting the impact on privacy and civil liberties in the receipt, retention, use, and dissemination of cyber threat information.
3. Guidance to Assist Non-Federal Entities to Share Cyber Threat Indicators and Defensive Measures with Federal Entities under the Cybersecurity Information Sharing Act of 2015 (June 2016, updated April 2024) assists non-Federal entities with sharing CTIs and DMs with Federal entities and describes the protections non-Federal entities receive under the statute.
4. Sharing of Cyber Threat Indicators and Defensive Measures by the Federal Government under the Cybersecurity Information Sharing Act of 2015 (February 2016) facilitates and promotes the timely sharing of classified and unclassified CTIs and DMs. The procedures include details on existing government programs that facilitate the sharing of information on cybersecurity threats and the periodic publication of cybersecurity best practices.

Project Steps:

1. What is the agency's process in practice for sharing cyber threat indicators within the Federal Government? Define "sharing" for the purposes of your agency.

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

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 were not the agency's response for question 2, is the agency aware of the documents?

5. Does the process for sharing cyber threat indicators within the Federal Government determined from question 1 align with the policies, procedures, and guidelines from question 2?

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? (OIGs can first determine whether not using the four procedure documents impacts the sharing - IC IG will coordinate additional follow-up, if necessary, and include in joint report)

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 examples 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?

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, determine whether the agency used and disseminated the shared cyber threat information appropriately? Provide results.

    b. If yes, 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, 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, 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 2023 & 2024? Provide results.

19. (For DHS only) How many of those cyber threat indicators and defensive measures reported for question 18 did Department of Homeland Security share with other Federal entities CYs 2023 & 2024? Provide results.

20. (Agencies other than DHS) How many cyber threat indicators and defensive measures did Department of Homeland Security relay to the agency via AIS CYs 2023 & 2024?

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 affected the sharing of cyber threat indicators and defensive measures among Federal entities? Provide a description of the barriers and the impact the barriers have on the sharing of cyber threat indicators and defensive measures. Examples of barriers could include:

    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 receive unclassified cyber threat information from ICoast? If not, why? (resources, system incompatibility, lack of information)

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

Appendix 3: Management Response

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C.

Samuel J. Corcos
Digitally signed by Samuel J. Corcos
Date: 2026.02.27 08:51:55 -05'00'

February 26, 2026

MEMORANDUM FOR LARISSA KLIMPEL, DIRECTOR, INFORMATION TECHNOLOGY AUDIT

FROM: Sam Corcos, Deputy Assistant Secretary for Information Systems and Chief Information Officer

CC: John W. York, PhD., Assistant Secretary for Management

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

Thank you for the opportunity to comment on the draft report *Audit of the Department of the Treasury's Cybersecurity Information Sharing.* We are pleased the report states that Treasury cyber threat sharing and defensive measures in calendar year 2023 and 2024 were deemed adequate and aligned with the Cybersecurity Information Sharing Act (CISA).

We have carefully reviewed the draft and agree with the report discussion about the lack of barriers to sharing information and defensive measures. Despite some reported difficulties in receiving cyber threat information, there have not been any adverse impacts. The agency remains committed to complying with Treasury policies and procedures.

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 Inspector General for their thorough analysis and professionalism throughout this audit.

Appendix 4: Major Contributors to This Report

Mitul Patel, Audit Manager
Adam Leesman, Auditor-In-Charge
Brittany Lawrence, IT Specialist/Auditor
Lawrence Delva-Gonzalez, Auditor
Dana Neufville, IT Specialist/Auditor
Veleria Tettey, Referencer

Appendix 5: Report Distribution

Department of the Treasury

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

Office of Management and Budget

Office of the Inspector General Budget Examiner

U.S. Senate

Chairman and Ranking Member
Committee on Finance

Chairman and Ranking Member
Committee on Appropriations

Chairman and Ranking Member
Subcommittee on Financial Services and General Government
Committee on Appropriations

U.S. House of Representatives

Chairman and Ranking Member
Committee on Financial Services

Chairman and Ranking Member
Committee on Appropriations

Chairman and Ranking Member
Subcommittee on Financial Services and General Government
Committee on Appropriations

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

Access Treasury OIG reports and other information online: https://oig.treasury.gov/