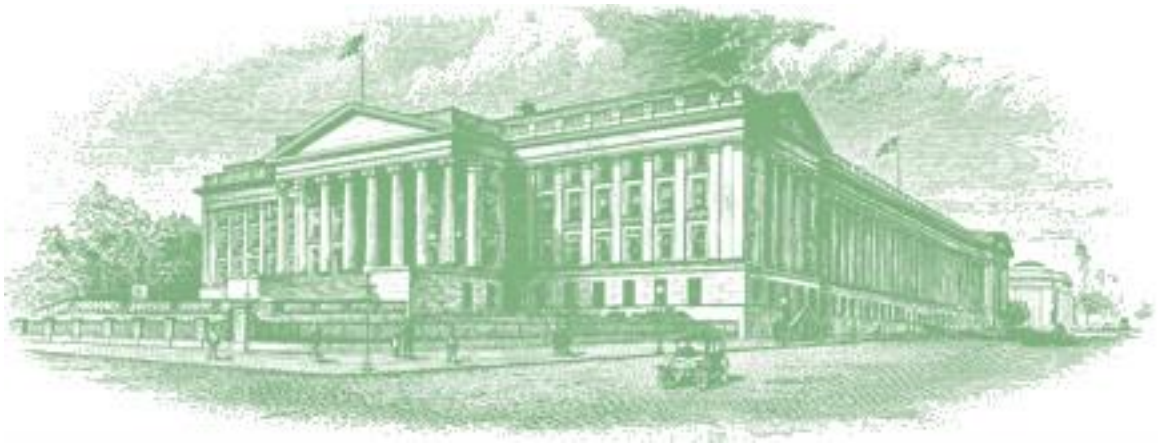
# Audit Report



OIG-20-019

**CYBERSECURITY/INFORMATION TECHNOLOGY**

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

December 10, 2019

Office of Inspector General
Department of the Treasury

This Page Intentionally Left Blank

# Contents

## Audit Report

Results in Brief ....3

Background ....4

Audit Results ....6

## Appendices

Appendix 1: Objectives, Scope, and Methodology ....17
Appendix 2: Common Question Set ....20
Appendix 3: Management Response ....28
Appendix 4: Major Contributors to This Report ....29
Appendix 5: Report Distribution ....30

## Abbreviations

| | |
|---|---|
| AIS | Automated Indicator Sharing |
| CY | calendar year |
| CIG | Cyber Information Group |
| CISA | Cybersecurity Information Sharing Act of 2015 |
| ICOAST | Intelligence Community Analysis and Signature Tool |
| CONOPS | *Threat Indicator Sharing Concept of Operations* |
| DIB CS | Defense Industrial Base Cybersecurity |
| DoD | Department of Defense |
| DHS | Department of Homeland Security |
| DOE | Department of Energy |
| FBI | Federal Bureau of Investigation |
| FinCEN | Financial Crimes and Enforcement Network |
| FS-ISAC | Financial Services – Information Sharing and Analysis Center |
| GAO | Government Accountability Office |
| GSOC | Government Security Operations Center |
| HSIN | Homeland Security Information Network |
| IC IG | Inspector General of the Intelligence Community |
| OCCIP | Office of Cybersecurity and Critical Infrastructure Protection |
| OCIO | Office of the Chief Information Officer |
| ODNI | Office of the Director of National Intelligence |

| | |
|---|---|
| OIA | Office of Intelligence and Analysis |
| 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 |
| TD | Treasury Directive |
| TEWI | Treasury Early Warning Indicator |
| TLP | Traffic Light Protocol |
| Treasury | Department of the Treasury |
| US-CERT | United States Computer Emergency Readiness Team |

# Audit Report

December 10, 2019

Eric R. Olson
Deputy Assistant Secretary for Information Systems and Chief Information Officer

Brian J. Peretti
Director, Office of Cybersecurity and Critical Infrastructure Protection

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) 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. This report represents our second biennial report to support the joint report.[3]

Our audit objective was to assess Treasury's activities during calendar years (CY) 2017 and 2018 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

[1] Pub. 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] *Survey Results–Department of the Treasury's Activities to Implement the Cybersecurity Act of 2015* (OIG-CA-17-020; June 15, 2017).

measure is an action, device, procedure, technique, or other measure that detects, prevents, or mitigates a known or suspected cybersecurity threat or security vulnerability.[4] 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] 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;

d) the specific aspects of cyber threat indicators or defensive measures shared with the Federal Government;[5] and

e) barriers affecting the sharing of cyber threat indicators or defensive measures.[6]

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

[5] 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 personally identifiable information (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.

[6] 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."

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 2017 and CY 2018. 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) *Threat Indicator Sharing Concept of Operations* (CONOPS) (March 20, 2017) document; and the Cyber Information Group (CIG) within the Office of Cybersecurity and Critical Infrastructure Protection (OCCIP), hereinafter collectively referred to as CIG/OCCIP *CIG Circular Procedures* (May 21, 2015). 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, CIG/OCCIP, and the Office of Privacy, Transparency, and Records (PTR). We reviewed all eight Treasury Early Warning Indicators (TEWI) containing cyber threat indicators and defensive measures that were prepared by GSOC of which four were shared externally in CY 2017 (two TEWIs) and CY 2018 (two TEWIs). We reviewed all six CIG Circulars containing cyber threat indicators and defensive measures that CIG/OCCIP shared externally in CY 2017 (two circulars) and CY 2018 (four circulars). We conducted this audit between February 2019 and October 2019 at Departmental Offices and the Office of Inspector General (OIG) office in Washington, D.C., and at GSOC in Vienna, Virginia. 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 2017 and CY 2018 were adequate and aligned with provisions of CISA. Specifically, GSOC and CIG/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[7] 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.

As part of our reporting process, we provided Treasury management an opportunity to comment on a draft of this report. In a written response, management acknowledged the report's conclusions and expressed its intention to continue to carry out the cyber information provisions of CISA. Management's response, in its entirety, is included as 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 Inspector General of the Intelligence Community (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 (DoD), 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

[7] Timely is defined by DHS as "as quickly as operationally practicable."

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 the (1) GSOC under the Office of the Chief Information Officer (OCIO), (2) the CIG/OCCIP, and (3) the 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 DHS' United States Computer Emergency Readiness Team (US-CERT) and other Federal Agency incident response teams.

CIG/OCCIP obtains and analyzes information related to cyber threats to the financial services sector received from Treasury's Office of Intelligence and Analysis (OIA), the Financial Crimes and Enforcement Network (FinCEN) as well as federal law enforcement sources. CIG/OCCIP shares cyber threat indicators and defensive measures at the unclassified level with the financial services sector. CIG/OCCIP also holds meetings where classified and unclassified information is discussed.

PTR provides Treasury library services and manages the Orders and Directives program, 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 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 2017 and CY 2018. Specifically, GSOC and CIG/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.

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, DoD, 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 DHS' policies and procedures documents discussed below, for sharing cyber threat indicators and defensive measures both within and outside the Federal Government. That said, GSOC and CIG/OCCIP developed

and implemented their own standard policy and procedures in alignment with DHS' policies and procedures for sharing cyber threat indicators and defensive measures both within and outside the Federal Government in the CONOPS document and *CIG Circular 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' four policies and procedures documents (hereinafter referred to as 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 (June 15, 2016); and (4) *Privacy and Civil Liberties Final Guidelines: Cybersecurity Information Sharing Act of 2015* (June 15, 2016).[8] We found no discrepancies between the CONOPS and DHS' policy and procedures documents. That said, GSOC tailored the CONOPS to Treasury's operating environment and included guidance for removing PII. We also noted that PTR personnel were involved with the joint review of DHS' four policy and procedure documents, as required by Section 105 of CISA.

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 2017 and CY 2018.

We determined that CIG/OCCIP's *CIG Circulars Procedures* were sufficiently designed for the sharing of cyber threat indicators and defensive measures with Non-Federal Government entities in the financial services sector and within the Federal Government, and that the procedures aligned with DHS' joint procedures. CIG/OCCIP does not address PII in its *CIG Circular Procedures*. However, CIG/OCCIP officials stated that the office does not receive or handle PII. We confirmed that the six CIG Circulars shared

[8] Developed by DHS in conjunction with the departments of Justice, Defense, Commerce, Energy, and the Treasury, and the Office of the Director of National Intelligence as a result of the enactment of CISA.

externally did not contain any PII. We concluded that CIG/OCCIP followed its *CIG Circular Procedures* for sharing cyber threat indicators and defensive measures during CY 2017 and CY 2018.

Section c below provides a more detailed discussion of the procedures that GSOC and CIG/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 entities, 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. That said, CISA does not require that all the appropriate entities, including Treasury, follow DHS' joint-procedures for sharing cyber threat indicators and defensive measures both within and outside the Federal Government.

In practice, GSOC and CIG/OCCIP share unclassified cyber-related information indirectly with the private sector via the Homeland Security Information Network (HSIN) and the Financial Services - Information Sharing and Analysis Center (FS-ISAC) portals.[9] 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,"[10] 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

[9] 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.
[10] TLP is a classification method used by the DHS 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.

adhered to." We noted that the four TEWIs that were shared externally in CY 2017 and CY 2018 were unclassified and did not contain information that required classification at a higher level.

When sharing cyber threat indicators and defensive measures with the financial services sector, CIG/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 information in a *CIG Circular*, CIG/OCCIP submits a request for declassification to OIA. Once declassified, cyber information is shared via CIG 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." Occasionally, CIG Circulars are designated as TLP: WHITE, which is "Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction." We noted that 5 out of the 6 CIG Circulars shared were TLP: GREEN, and 1 was TLP: WHITE. We reviewed the content of all six unclassified CIG Circulars that were shared externally to ensure that they did not contain information that required classification at a higher level.

While CIG Circulars are not classified, CIG/OCCIP also holds classified meetings with financial services sector leaders, representatives, and regulators who either have active security clearances issued by another Federal agency or are issued clearances under DHS' Private Sector Clearance Program for Critical Infrastructure.[11] As such, Treasury does not administer the list of authorized security clearances, 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, CIG/OCCIP officials stated that information discussed at these meetings is not actionable. As such, the information is not re-disseminated.

[11] 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.

As GSOC 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.

**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 joint procedures contained in DHS' four policies and procedures documents for sharing cyber threat indicators and defensive measures both within and outside the Federal Government.

GSOC follows its CONOPS policy and procedures for sharing cyber threat indicators within the Federal Government. GSOC does not specifically redistribute cyber threat indicators or defensive measures that it receives from other Federal agencies and the private sector. GSOC only issues TEWIs related to threats detected against Treasury's network. Therefore, GSOC's subsequent uses and disseminations is applicable to Treasury's network. We found that GSOC followed its CONOPS for sharing the eight TEWIs in CY 2017 and CY 2018, and as such, the subsequent use and dissemination were appropriate as described in section (ii).

CIG/OCCIP follows its *CIG Circular Procedures* for sharing cyber threat indicators with non-Federal government entities in the financial services sector as well as other Federal agencies. In practice, CIG/OCCIP analyzes cyber information from its sources and repackages the cyber information at an unclassified level into CIG Circulars, which are shared via the FS-ISAC portal. As noted in section (b), CIG/OCCIP also conducts classified meetings with financial services sector leaders, representatives, and regulators as another means of communication as needed.

We concluded that CIG/OCCIP appropriately used and disseminated cyber threat indicators and defensive measures contained in its six CIG Circulars shared with the financial services sector in CY 2017 and CY 2018 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.**

We determined that GSOC shared cyber threat indicators and defensive measures in a timely and sufficient manner with the appropriate entities during CY 2017 and CY 2018. Notifications of cyber threat indicators and defensive measures were received from other Federal agencies and the private sector via an email inbox that is monitored by GSOC and via DHS' Automated Indicator Sharing (AIS) portal at the unclassified level. According to a GSOC official, nearly 10,000 unique cyber threat indicators and defensive measures were received via email, and over 1.1 million unique cyber threat indicators and defensive measures were relayed through the AIS portal over the course of CY 2017 and CY 2018. However, alerts on the AIS portal consistently lacked context or actionable information for agencies to use. The AIS alerts also generally did not indicate the source of the information. While GSOC does not share classified cyber-related information, it receives classified cyber threat indicators and defensive measures via its classified network.

GSOC's process is to use an internal ticketing system to enter and track cyber threat indicators and defensive measures. Each ticket is then run through a Security Information and Event Management (SIEM)[12] tool which scans Treasury's network for matching events related to the cyber threat indicators and defensive measures. In addition, GSOC analysts manually search the SIEM for historical matches within the previous 365 days. If GSOC analysts determine that cyber threat indicators and defensive measures are serious, a TEWI is developed by a GSOC analyst. A TEWI is a document that includes a brief description of the event(s) and other details such as source Internet Protocol (IP)[13] addresses, timestamps, and attachments from relevant tickets. As required in the CONOPS, TEWIs are then shared within a reasonable timeframe (i.e. as quickly as possible) with other Federal and non-Federal entities via the following portals as applicable:

[12] SIEM software collects and aggregates log data generated throughout the organization's technology infrastructure.
[13] 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 Internet Protocol.

- US-CERT HSIN Portal: Access is available to government agencies (Federal, State, and Local) and contractors supporting Federal agencies.

- 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.

There were eight TEWIs developed by GSOC analysts during CY 2017 and CY 2018. We found that GSOC shared two TEWIs in CY 2017 and two TEWIs in CY 2018 using the US-CERT HSIN portal. Due to the sensitive nature of the other four TEWIs, GSOC shared them internally with bureau SOCs only via the GSOC portal. Based on our review of the externally-shared TEWIs, their associated tickets, and the delivery method/portals used, we determined that GSOC shared cyber threat information and defensive measures within reasonable timeframes (i.e. approximately one week) with the appropriate entities. GSOC also followed its CONOPS document for sharing the sensitive TEWIs internally with bureau SOCs.

We determined that CIG/OCCIP shared cyber threat indicators and defensive measures in a timely and sufficient manner with the appropriate financial services sector entities during CY 2017 and CY 2018. CIG/OCCIP's process is to obtain and analyze information related to cyber threats to the financial services sector received primarily from Treasury's OIA as well as FinCEN and Federal law enforcement sources. CIG/OCCIP compiles cyber information at the unclassified level into CIG Circulars before sharing with the financial services sector. Once information is compiled into a CIG Circular, it is shared with the original source(s) to verify that the information is unclassified. After verification, the CIG Circular must be approved by officials within CIG/OCCIP and the Office of General Counsel prior to sharing. Once approved, CIG/OCCIP then sends the CIG Circular to the FS-ISAC and HSIN Financial Services portals to be shared externally with appropriate financial services sector entities. CIG/OCCIP also shares CIG Circulars internally with other Federal and non-Federal government partners and cybersecurity centers, including the National Cybersecurity and Communications Integration Center under DHS. These cybersecurity centers also receive FS-ISAC information, and

therefore, will receive the CIG Circulars more than once. Additionally, CIG/OCCIP conducts classified meetings with financial services sector leaders and representatives as another means of communication as needed.

**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 in real time cyber threat indicators and defensive measures from any non-Federal entity, and be the process by which the Federal Government receives these indicators and defensive measures. AIS is the capability and process DHS certified for this purpose.

As discussed above, GSOC received over 1.1 million indicators and defensive measures via AIS, which were unclassified. CIG/OCCIP's cybersecurity information is received via multiple sources. In both cases, we confirmed that both GSOC and CIG/OCCIP were not required to use AIS, and did not use AIS, to share the four external TEWIs and six CIG Circulars, respectively. The US-CERT HSIN and FS-ISAC portals were used instead.

**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. While DHS' 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, CISA does not require the appropriate Federal entities, including Treasury, to follow DHS' procedures. That said, GSOC requires the removal of PII not directly related to a cybersecurity threat in the CONOPS document. CIG/OCCIP does not address PII in its *CIG*

*Circular Procedures*. However, CIG/OCCIP officials stated that the office does not receive or handle PII.

We confirmed that GSOC removed PII from the four TEWIs shared externally, discussed in section c. As such, GSOC did not share any PII. We also confirmed that the six CIG Circulars shared externally did not contain any PII.

**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 who 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 (TD) 25-07, and its related publication require a Privacy and Civil Liberties Impact Assessment (PCLIA)[14] 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 requirements[15] which require, among other things, a PCLIA to be conducted before:

[14] TD 25-07, *Privacy Impact Assessment (PIA)* (August 6, 2008) and TD Publication 25-07, *Privacy Impact Assessment (PIA) Manual* (June 30, 2009). Treasury is in the process of updating these documents to change the titles from the PIA to the PCLIA. It is a change in title only and not the assessments.

[15] 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*.

- 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 reported a PCLIA performed 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.[16] As noted above in section d (ii), we concluded that GSOC removed all PII from the four TEWIs shared externally. We also verified that the six CIG Circulars that were shared externally did not contain any PII that would require a PCLIA. As such, a qualitative and quantitative assessment of the effect on privacy and civil liberties from sharing TEWIs and CIG Circulars was not required. That said, Treasury complied with all Federal privacy and civil liberty requirements.

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

GSOC, CIG/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 2017 and CY 2018. Therefore, there were no steps taken by GSOC or CIG/OCCIP to reduce any adverse effects.

[16] Privacy and Civil Liberties Impact Assessment for the Treasury Government Security Operations Center Network (November 28, 2017).

**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[17] to sharing information. We found no barriers that impeded GSOC's and CIG/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.

**Conclusion**

Overall, we concluded that Treasury's sharing of cyber threat indicators and defensive measures and protecting PII aligned with the provisions of CISA. Specifically, we determined that GSOC and CIG/OCCIP followed applicable policies, procedures, and practices when sharing all eight TEWIs and all six CIG Circulars in CY 2017 and CY 2018. Furthermore, Treasury complied with all Federal privacy and civil liberty requirements.

* * * * * *

I would like to extend my appreciation to the officials and personnel within the offices of the OCIO, the GSOC, the CIG/OCCIP, and the 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 Tom Tucci, IT Audit Manager, at (202) 927-8770. Major contributors to this report are listed in appendix 4.

/s/

Larissa Klimpel
Director, Cyber/Information Technology Audit

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

## Appendix 1: Objectives, Scope, and Methodology

Our audit objective was to assess the Department of the Treasury's (Treasury) activities during calendar years (CY) 2017 and 2018 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 Cyber Information Group (CIG) within the Office of Cybersecurity and Critical Infrastructure Protection (OCCIP), hereinafter collectively referred to as CIG/OCCIP. The scope of our audit also included GSOC's and CIG/OCCIP's activities for sharing cyber threat indicators and defensive measures contained in the eight Treasury Early Warning Indicators (TEWI) and the six CIG Circulars during CY 2017 and CY 2018. We conducted this audit between February 2019 and October 2019 at Departmental Offices and the Office of Inspector General in Washington, D.C., and at GSOC in Vienna, Virginia.

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 referred to as 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 2015* (June 15, 2016); 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* (CONOPS) (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 CIG/OCCIP's *CIG Circular Procedures* (May 21, 2015) 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;
- reviewed *Standards for Internal Control in the Federal Government* (GAO-14-704G; September 10, 2014);
- 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, CIG/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) CIG/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 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 2017 and CY 2018;
- reviewed the CIG Circulars that were shared by CIG/OCCIP during CY 2017 and CY 2018;
- conducted a data call with PTR official responsible for conducting Privacy and Civil Liberties Impact Assessments; and
- reviewed the Privacy and Civil Liberties Impact Assessment for all information systems and projects that collect, maintain, or disseminate personally identifiable information.

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[18] related to executive branch agencies cyber information activities in calendar years (CY) 2017 and 2018.

**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. 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 9-14)

C. A review of the actions taken by the Federal Government to share cyber threat indicators and defensive measures, to include a determination on the timeliness, adequacy, and appropriateness of the sharing. (Steps 15-22)

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

[18] Pub. L. 114-113, Division N (December 18, 2015)

i. The number of cyber threat indicators and defensive measures shared using the capability and process developed in accordance with 105(c). (Steps 23-26)

ii. Instances of sharing PII not directly related to a cybersecurity threat. (Steps 27-28)

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 29-32)

v. The adequacy of steps taken to reduce adverse effect on the privacy and civil liberties. (Steps 33-34)

E. An assessment of the sharing of cyber threat indicators and defensive measures within the Federal Government to identify barriers to sharing information. (Step 35)

**Definitions:**

Question 16 – *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 19 – *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 19 – *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 19 - *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 19 can be obtained from procedure document, *Sharing of Cyber Threat Indicators and Defensive Measures by the Federal Government under CISA*.

Question 22 – *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 22 – *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 22 – *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 22 can be obtained from procedure document, *Final Procedures Related to the Receipt of Cyber Threat Indicators and Defensive Measures by the Federal Government.*

Question 34 - 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*.

**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?

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

4. If the agency uses policies, procedures, and guidelines different from the CISA procedure documents, do they include guidance for removing information not directly related to a cybersecurity threat that is personal information of a specific individual or information that identifies a specific individual?

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 (only if different from the four CISA procedure documents) sufficient and complying with the guidance in CISA Section 103(a) & (b) and 105(a), (b), & (d)? (GAO [Government Accountability Office] report documents the sufficiency of the CISA procedure documents already)

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

8. If there are differences in the policies, procedures, and guidelines implemented among the agencies (different from the CISA procedure documents), does it impact the sharing of cyber threat information? (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)

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?

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

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

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

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

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

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

19. If yes, review a sample to determine whether the agency shared the cyber threat information in a timely and adequate manner with appropriate entities or, if appropriate, made publicly available. Provide results.

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

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

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

23. (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 2017 & 2018? Provide results.

24. (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 2017 & 2018? Provide results.

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

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

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

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

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

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

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

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

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

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

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

    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?

36. Any cybersecurity best practices identified by the agency through ongoing analyses of cyber threat indicators, defensive measures, and information related to cybersecurity threats? Did the agency share or receive any cybersecurity best practices? [Section 103(a)(5)] Also see procedure document, Sharing of Cyber Threat Indicators and Defensive Measures by the Federal Government under CISA, on Periodic Sharing of Cybersecurity Best Practices, which includes some best practices from Department of Commerce, DHS, [Defense Industrial Base Cybersecurity] DIB CS, [Federal Bureau of Investigation] FBI, and National Security Agency.

37. What capabilities/tools does the agency use to share and/or receive cyber threat indicators and defensive measures? Are the capabilities/tools providing the agency with the necessary cyber threat information? Also see procedure document, Sharing of Cyber Threat Indicators and Defensive Measures by the Federal Government under CISA, which lists some sharing programs from DHS, DIB CS, FBI, [Department of Energy] DOE, and Treasury.

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

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

39. 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. 20220**

December 5, 2019

Larissa Klimpel
Director, Cyber Information Technology
Office of the Inspector General
U.S. Department of the Treasury
1500 Pennsylvania Avenue, NW
Washington, DC 20220

Dear Ms. Klimpel:

Thank you for the opportunity to review the draft report entitled *Audit of the Department of the Treasury's Cybersecurity Information Sharing* (the Report). This letter provides the official response of the Department of the Treasury (Treasury).

The Report examines Treasury's activities to carry out the cybersecurity information sharing provisions of the Cybersecurity Information Sharing Act (CISA). We are pleased that the Report found that Treasury's activities to share cyber threat indicators and defensive measures during calendar years 2017 and 2018 were adequate and aligned with provisions of CISA. Treasury will continue to carry out the cyber information provisions of CISA.

Thank you once again for the opportunity to review the Report. We look forward to continuing to work with your office in the future.

Sincerely,

Eric R. Olsen
Deputy Assistant Secretary for Information Systems and Chief Information Officer

Brian Peretti
Director, Office of Cybersecurity and Critical Infrastructure Protection

## Appendix 4: Major Contributors to This Report

Mitul "Mike" Patel, Supervisory IT Specialist
Tom Tucci, Supervisory IT Specialist
Kevin May, IT Specialist
Harry J. Jeffreys, IT Specialist
Brittany N. Lawrence, IT Specialist
Joshua A. Matadial, IT Specialist
Jeffrey Hawkins, Referencer
Lawrence Gonzalez, 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
Deputy Director, Office of Cybersecurity and Critical Infrastructure Protection, Cyber Information Group
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**

**Treasury OIG Hotline: 1-800-359-3898**
Hotline@oig.treas.gov

**Gulf Coast Restoration Hotline: 1-855-584.GULF (4853)**
gulfcoastrestorationhotline@oig.treas.gov

Access Treasury OIG reports and other information online:
www.treasury.gov/about/organizational-structure/ig