DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

OFFICE OF
INSPECTOR GENERAL

June 15, 2017

OIG-CA-17-020

MEMORANDUM FOR MARK A. KRULIKOWSKI
INSPECTOR GENERAL FOR THE INTELLIGENCE COMMUNITY
ACTING ASSISTANT INSPECTOR GENERAL FOR AUDIT

FROM: Deborah Harker /s/
Assistant Inspector General for Audit

SUBJECT: Survey Results—Department of the Treasury's Activities to Implement the Cybersecurity Act of 2015

We are pleased to transmit the results of our survey of the Department of the Treasury's (Treasury) activities to implement the information sharing provisions under Title I, the Cyber 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 Intelligence Community Inspector General (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 requirements of CISA. The first report is due December 2017 and biennially thereafter.

To meet our reporting obligation under Section 107 in support of the joint report, we conducted a survey of Treasury's actions taken to carry out the provisions of CISA. The objective of our survey was to answer the common question set developed by the IC IG for developing the first joint report. Responses to the common question set included in this memorandum will establish a baseline to further evaluate Treasury's activities and results going forward. It is expected that the second biennial report, due December 2019, will be either an audit or evaluation in which we may provide recommendations as appropriate based on any findings.

We conducted this survey between April 2017 and June 2017 at Treasury Departmental Offices and the Office of Inspector General office in Washington, D.C. The scope of our work included all Treasury information sharing policies and

[1] Pub. L. 114-113, Division N (December 18, 2015)
[2] The Office of the Director of National Intelligence and the Departments of Commerce, Defense, Energy, Homeland Security, Justice, and Treasury.

procedures as well as activities covering the most recent 2-year period (calendar years 2015 and 2016). As part of our survey, we reviewed applicable provisions of CISA and Treasury's responses to the common question set developed by the IC IG. Although not an audit, we followed generally accepted government auditing standards specific to the general standards and fieldwork standards for performance audits in conducting this survey.

Officials and staff within the Government Security Operations Center (GSOC)– Office of the Associate Chief Information Officer, Cybersecurity– and the Office of Privacy, Transparency, and Records (PTR) were responsible for responding to this survey. GSOC serves as Treasury's primary computer security incident response capability and is responsible for department-wide security monitoring and incident reporting. GSOC provided responses to questions 1 - 8 and 10 - 11 regarding Treasury's policies, procedures, guidelines, and practices for sharing, classification, and use of cyber threat indicators and defensive measures within the Federal government. 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.[3] 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.[4] PTR serves both the public and the Federal government community by determining and setting the standards for protecting, facilitating access, preserving, retaining, and disclosing Treasury information. As such, PTR provided responses to question series 9 related to Treasury's effects on the privacy and civil liberties of U.S. persons.

Survey Results

1.

a. Does Treasury have policies, procedures, and guidelines for sharing cyber threat indicators within the Federal Government? Please list.

Yes, since November 2011, GSOC has followed a "Threat Indicator Sharing Concept of Operations" (CONOPS) document that provides the standard policy and procedures for sharing cyber threat indicators both within and outside the Federal Government.

[3] Pub. L. 114-113, Division N (December 18, 2015), SEC.102. Definitions, (6) Cyber Threat Indicator

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

b. Do these policies, procedures, and guidelines include guidance for removing information not directly related to a cybersecurity threat that is personal information of a specific individual or information that identifies a specific individual? Please provide title of policy, procedure, or guidance.

No, the CONOPS does not include guidance specific to removing information not directly related to a cybersecurity threat that is personal information of a specific individual or information that identifies a specific individual. However, the CONOPS does specifically state, "A [shared] report should generally not contain names of Treasury targets [or] roles/offices of Treasury targets."

c. Are the policies, procedures, and guidelines for sharing cyber threat indicators within the Federal Government sufficient?

Yes, according to GSOC the CONOPS is sufficient for sharing cyber threat indicators within the Federal Government. GSOC has been using the CONOPS document to facilitate information sharing with its partners for more than five years. While specific sharing relationships with other Federal and non-Federal organizations such as the Department of Homeland Security (DHS) and the Financial Services Information Sharing and Analysis Center (FS-ISAC)[5] have changed over time, the basic principles to which GSOC adheres have remained consistent, well-established and understood.

d. How did Treasury determine sufficiency?

GSOC determined that the CONOPS is sufficient since only minor adjustments to the document were ever needed to incorporate emerging new agreements and sharing mechanisms.

2.

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

Yes, GSOC shares cyber threat indicators and defensive measures, but only with trusted communities as required by the CONOPS. Specifically, GSOC shares cyber threat indicators and defensive measures with FS-

[5] 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.

ISAC and permits DHS to redistribute its reports to the Cyber Information Sharing and Collaboration Program participants (CISCP).[6]

However, Treasury is not sharing cyber threat indicators and defensive measures with the DHS Automated Indicator Sharing (AIS) private sector participants as required by CISA because it is not a trusted community since its participants may include foreign and domestic adversaries.

b. Did your agency properly classify the cyber threat indicators and defensive measures shared with the private sector?

Yes, GSOC determined that all cyber threat indicators and defensive measures shared with the private sector are unclassified.

c. How did your agency determine whether the shared cyber threat indicators and defensive measures were properly classified?

All of GSOC's shared cyber threat indicators and defensive measures are unclassified as they were created by performing unclassified methods on unclassified data that yielded unclassified output. Additionally, GSOC released indicator reports that contained only unclassified attributes and not information about the identity of the people or groups behind the cyber threats or their intent. Therefore, GSOC has not needed to classify the shared cyber threat indicators and defensive measures. Furthermore, Treasury's Office of Intelligence and Analysis is aware of the described practices and has never raised an objection to the information produced at the unclassified level, either individually or in aggregate.

3. How does your agency account for the number of security clearances authorized for sharing cyber threat indicators and defensive measures with the private sector?

This is not applicable to GSOC since all cyber threat indicators and defensive measures are unclassified, and as such, security clearances are not required. Note that while GSOC may receive classified cyber threat indicators and defensive measures from outside sources, it does not redistribute them.

[6] CISCP is a DHS flagship program for public-private information sharing and complements ongoing DHS information sharing efforts. To join the program, companies are required to sign a Cooperative Research and Development Agreement.

4.

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

Yes, GSOC has used cyber threat indicators and defensive measures received from other Federal agencies for network defense purposes, which includes dissemination to internal stakeholders. In accordance with the CONOPS, cyber threat indicators and defensive measures shared by other Federal agencies are not re-distributed by GSOC outside of Treasury.

b. Did your agency use and disseminate the shared cyber threat indicators and defensive measures appropriately?

GSOC used and disseminated shared cyber threat indicators and defensive measures appropriately. GSOC's main function is to detect malicious activity within Treasury. When GSOC receives cyber threat indicators and defensive measures from other Federal agencies, it applies those cyber threat indicators and defensive measures to detect and prevent malicious activity from affecting Treasury's own systems. GSOC only disseminates cyber threat indicators and defensive measures it receives to components within Treasury.

c. How did your agency determine if the use and dissemination of shared cyber threat indicators and defensive measures was appropriate?

GSOC determined that the use of shared cyber threat indicators and defensive measures was appropriate by following the guidance provided in the "Enhance Shared Situational Awareness Multilateral Information Sharing Agreement" (dated March 2015), of which Treasury is a signatory. The agreement was established by multiple Federal agencies[7] to enhance cybersecurity information sharing among Federal agencies in order to better protect the United States from malicious cyber actors in a manner that is fully consistent with the Constitution and laws of the United States, Executive Orders and other Executive Branch directives and policies, court orders, and all other legal, policy, and oversight requirements.

[7] Other Federal agency signatories include the Department of Defense, the National Security Agency, the Federal Bureau of Investigation, the United States Cyber Command, the Department of Energy, the Office of the Director of National Intelligence, the Defense Information Systems Agency, and DHS.

Since GSOC does not redistribute cyber threat indicators and defensive measures received from other organizations, a need to determine the appropriateness of dissemination is not necessary.

5.

a. Has your agency shared cyber threat indicators and defensive measures with other Federal agencies?

Yes, GSOC has shared cyber threat indicators and defensive measures it has identified with other Federal agencies.

b. Did your agency share the cyber threat indicators and defensive measures in a timely and adequate manner with appropriate entities or, if appropriate, made publicly available?

Yes, GSOC shared cyber threat indicators and defensive measures within Treasury as well as FS-ISAC and CISCP as quickly as possible after discovery, with a target time of four hours but not more than 24 hours after indicator discovery. GSOC has determined that it is not appropriate to make cyber threat indicators and defensive measures publicly available and has no intention of sharing cyber threat indicators and defensive measures publicly. Furthermore, GSOC does not have a planned mechanism for doing so. In the event sharing with the public becomes necessary, it would likely be in coordination with or performed by DHS.

c. Have other Federal entities shared cyber threat indicators and defensive measures with your agency in a timely, adequate, and appropriate manner?

Yes, GSOC believes that other Federal entities have shared cyber threat indicators and defensive measure in a timely, adequate, and appropriate manner. However, GSOC noted that there is no easy way to calculate or categorize the reporting that was received, short of an extensive and time-consuming manual review. Some reports received do not include the discovery time, and therefore, make it impossible to determine if the information was shared in a timely, adequate, and appropriate manner.

d. How did your agency determine timeliness, adequacy and appropriateness of sharing the information?

According to GSOC, the evaluation of timeliness, adequacy, and appropriateness "is more of an art rather than a science, although the government community is actively discussing ways to 'score' or otherwise rate indicators to help in this analysis." In many cases, a quick cyber threat indicator or defensive measures report is released within hours or days of a detected attack. Longer-term trending reports are released much

later. GSOC noted that the trouble is not necessarily sharing bad indicators, which can have value, but not being able to distinguish which received indicators are good or bad without the use of intensive manual processes, which reduce the usefulness of automated sharing.

GSOC's main goal is to use cyber threat indicators to detect and prevent malicious activity, and a cyber threat indicator's usefulness is in the context of meeting that goal. Therefore, GSOC's determination of the usefulness is not performed using clearly-defined rules and scores but by the following considerations:

- Timeliness: The usefulness of indicators is often measured in hours, not days or months. While older information can have value, expediency is very important.

- Adequacy: Even without attribution, information such as how indicators relate to each other, how an indicator was used, when the activity was observed (not when reported), all add useful information to help investigate potential alerts.

- Appropriateness/reliability: Adversaries are increasingly using shared or legitimate infrastructure to launch attacks, which limits the usefulness of some indicators due to high false positive rates.

6.

a. How many cyber threat indicators and defensive measures have non-Federal entities shared with the Department of Homeland Security through the capability and process developed under section 105(c)?

This question is not applicable to Treasury.

b. How many of those cyber threat indicators and defensive measures reported for 6.a. above did the Department of Homeland Security share with other Federal entities?

This question is not applicable to Treasury.

7. **How many cyber threat indicators and defensive measures from non-Federal entities did the Department of Homeland Security relay to your agency?**

   As of March 2017, GSOC had received 19,855 cyber threat indicators and defensive measures from non-Federal entities via DHS. However, private sector submissions via the DHS National Cybersecurity and Communications Integration Center may have details identifying the reporter removed. Therefore, it is possible that multiple reported indicators were condensed into a single indicator. As such, the actual number of cyber threat indicators and defensive measures could be higher than the 19, 855 reported by DHS.

8.

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

      No, all shared information containing personal information of a specific individual or identifying a specific individual was directly related to cyber threat indicators and defensive measures. As such, no information shared with or by Treasury was in violation of CISA.

   b. **Please include a description of the violatio**n.

      There were no violations of CISA to report.

9.

   a. **Was there an effect of your agency sharing cyber threat indicators and defensive measures with the Federal Government on privacy and civil liberties of specific individuals?**

      Thus far, PTR has identified a limited potential impact in the event that a GSOC report adversely affects a Treasury employee based on the information. PTR is in the final stages of its review of GSOC's Privacy and Civil Liberties Impact Assessment (PCLIA). The PCLIA is a formal document that fulfills the requirements set forth in Section 208 of the E-Government Act of 2002, Office of the Management and Budget (OMB) Memorandum 03-22, "OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002," and Treasury Directive 25-07, "Privacy and Civil Liberties Impact Assessment (PCLIA)." The PCLIA provides the following information regarding the system or project:

1. an overview of its purpose and functions;
2. a description of the information collected;
3. a description of the how information is maintained, used, and shared;
4. an assessment of whether the system or project is in 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 will more definitively be able to answer this question upon the completion of the PCLIA. PTR will finalize and publish the PCLIA before the end of fiscal year 2017. Besides the privacy and civil liberties review of GSOC, PTR has found that the cyber security activities related to protection of critical infrastructure (that is, assets where their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof) have not negatively impacted specific individuals.

b. What was the effect on privacy and civil liberties of specific individuals?

As mentioned above, PTR is in the final stages of its review of the PCLIA. Based on the information PTR has so far, PTR has determined that the cyber security activities relating to GSOC could have a potential limited effect on the privacy and civil liberties of individuals. The potential limited effect stems from GSOC's use of personally identifiable information (PII) from Treasury's human resources system for all Treasury personnel, both government employees and contractors, to identify individuals whose employee identifications or email addresses have surfaced in a cyber incident investigation. GSOC processes PII to uncover indicators of potential issues and generates a report. The focus of the report is on cyber security incidents, their impact and remediation, which is then passed to the respective Treasury bureau for investigation. This investigation may lead to an adverse determination against a Treasury employee or contractor. Although the focus of the investigation is solely on the technical aspects of a cyber incident, PTR determined that GSOC's activities could have a limited effect on the privacy and civil liberties of individuals because GSOC uses PII to complete its report.

c. How did your agency quantitatively and qualitatively assess the effect?

As mentioned above, PTR has determined that the cyber security activities relating to GSOC could have a potential limited effect on the privacy and civil liberties of individuals. Although no actual effect has been found, PTR applies a qualitative analysis using the Fair Information Practice Principles (FIPPs) to identify and assess the potential privacy impact on individuals. The FIPPs are a set of internationally recognized principles designed to ensure the protection of information privacy. Treasury uses the FIPPs as the general framework to analyze Treasury's collection, use, maintenance, and sharing of PII.

In addition to its FIPPs analysis, PTR considers whether agency cyber security activities involve the monitoring or interception of communications, or compiling of information regarding lawful activities that may impact civil liberties. PTR also considers the legal authorities that support such activities and the procedures undertaken to safeguard individual rights in carrying out such activities.

Using the principles and considerations discussed above, PTR assesses the privacy and civil liberties impact of Treasury programs through the PCLIA.

d. Did your agency receive any notices regarding a failure to remove information that WAS NOT directly related to a cybersecurity threat AND were any of those notices related to personal information of a specific individual or information that identified a specific individual?

No, GSOC did not receive any notices from other organizations regarding a failure to remove information that was not directly related to a cybersecurity threat.

e. How many notices did you agency receive?

GSOC did not receive any such notices.

f. Did your agency issue any notices regarding a failure to remove information that WAS NOT directly related to a cybersecurity threat AND were any of those notices related to personal information of a specific individual or information that identified a specific individual?

No, GSOC did not issue any notices to other organizations regarding a failure to remove information that was not directly related to a cybersecurity threat.

g. How many notices did your agency issue?

GSOC did not issue any such notices.

10.

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

GSOC determined that steps taken to reduce the potential for adverse effects from the activities carried out under CISA on the privacy and civil liberties of U.S. persons were adequate.

b. How did your agency determine adequacy of the steps taken?

GSOC has never found that any reports shared or reports received contained inappropriate personal or other data.

11.

a. Has your agency identified any barriers that adversely affected the sharing of cyber threat indicators and defensive measures among Federal entities?

Yes, GSOC identified barriers, as discussed below, which adversely affected the sharing of cyber threat indicators and defensive measures among Federal entities.

b. Please describe the barriers and the effect the barriers have on the sharing of cyber threat indicators and defensive measures.

According to GSOC, there is a technical barrier that was exacerbated by having limited resources. To share cyber threat indicators and defensive measures with DHS AIS, DHS requires use of a specialized version of Structured Threat Information Expression (STIX) to format the information. The standard generated STIX report that GSOC built is not sufficient for sharing cyber threat indicators and defensive measures with DHS AIS. GSOC will need to build another report generation algorithm. This is on GSOC's roadmap for calendar year 2017. The lack of a new algorithm has delayed GSOC's ability to share with Federal partners via AIS. In the meantime, GSOC is sharing with Federal government partners via other channels.

In conclusion, we did not find any issues or matters of concern in Treasury's responses to this survey that are in need of immediate attention and would require our office to initiate a more in-depth audit or evaluation at this time. Should you have any questions or require further information, you may contact me at (202) 927-5400 or Larissa Klimpel, Director, Cyber/Information Technology Audit, at (202) 927-0361.

cc: Sanjeev "Sonny" Bhagowalia, Deputy Assistant Secretary for Information Systems and Chief Information Officer
Ryan A. Law, Deputy Assistant Secretary for Privacy, Transparency, and Records