Audit Memorandum

OIG-18-006

TERRORIST FINANCING/MONEY LAUNDERING: Audit of the Office of Intelligence and Analysis' Management of the Office of Terrorism and Financial Intelligence Employees' Intelligence Community Public Key Infrastructure Certificates

October 30, 2017

Office of
Inspector General

Department of the Treasury

THIS PAGE INTENTIONALLY LEFT BLANK

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

OFFICE OF
INSPECTOR GENERAL

October 30, 2017

OIG-18-006

MEMORANDUM FOR SIGAL P. MANDELKER, UNDER SECRETARY FOR TERRORISM AND FINANCIAL INTELLIGENCE

FROM: Deborah L. Harker, Assistant Inspector General for Audit /s/

SUBJECT: Audit of the Office of Intelligence and Analysis' Management of the Office of Terrorism and Financial Intelligence Employees' Intelligence Community Public Key Infrastructure Certificates

In June 2017, a staff member of the U.S. House of Representatives Committee on Financial Services, Subcommittee on Terrorism and Illicit Finance, emailed our Inspector General with specific concerns related to the Department of the Treasury's (Treasury) Office of Intelligence and Analysis (OIA) and the Financial Crimes Enforcement Network (FinCEN). Specifically, the email expressed concern that OIA initiated a mass revocation of FinCEN's intelligence community public key infrastructure (IC PKI)[1] certificates that prevented FinCEN employees from effectively responding to law enforcement requests on the London and Manchester terrorist attacks.[2] IC PKI certificates are issued to government and contractor employees in the intelligence community (IC) who demonstrate a mission need to have direct electronic access to certain classified information held by other members of the IC. Some Treasury employees, including some in FinCEN and OIA, require direct electronic access to classified information to carry out their responsibilities.

In August 2017, our Office of Inspector General Counsel's office was copied on a second email, this time from a FinCEN employee, claiming that delays in providing FinCEN employees with IC PKI certificates prevented FinCEN from fully responding to the Under Secretary for Terrorism and Financial Intelligence (TFI) and the White

---

[1] IC PKI is a tool to, among other things, authenticate users and support user identification and provide user access to data.

[2] The Manchester terrorist attack occurred on May 22, 2017. The London terrorist attack occurred on June 3, 2017, and our Inspector General received the staff member's email on June 4, 2017.

House regarding Venezuela.[3] To address the concerns documented in the June and August 2017 emails, we expanded the scope of an ongoing audit of OIA.[4] This report is the first of two reports that we plan to issue related to this audit.

To accomplish our objective, we (1) reviewed laws and regulations and Treasury and IC policies and procedures and other documents related to intelligence gathering and IC PKI certificates; (2) interviewed key officials and staff within OIA, FinCEN, and Treasury's external service provider with responsibilities for the IC PKI process and supporting law enforcement inquiries; and (3) surveyed TFI employees about their experiences with the IC PKI certificates issued in 2015 and renewed in 2017. We conducted our fieldwork between June 4, 2017 and October 25, 2017.

Results in Brief

We found that OIA did not initiate a mass revocation of FinCEN's IC PKI certificates as claimed in the June 2017 email. Instead, a large number of Treasury employees, including 25 FinCEN employees, had IC PKI certificates that expired in April, May, or June 2017. Many of these FinCEN employees were unaware that their IC PKI certificates were expiring in May and June 2017 until after the expiration date. Reminders were sent by OIA's Office of Special Security Programs (SSP) to OIA employees that expiration dates were approaching, however no reminders were sent to most FinCEN employees. Although 25 FinCEN employees' IC PKI certificates expired during the May to June 2017 timeframe, a FinCEN official responsible for the London and Manchester response told us that FinCEN was able to effectively provide law enforcement-related information in response to these terrorist attacks. By late June 2017, SSP resolved 21 of the 25 FinCEN employees' expired IC PKI certificates. Although SSP staff contacted the remaining four FinCEN employees, as of the end of June 2017 these FinCEN employees had not completed the required renewal appointment with SSP.

In addition to the 25 IC PKI certificates that expired in May and June 2017, during this same timeframe FinCEN initiated or had pending requests for OIA to approve new IC PKI access for 78 employees. We found that OIA is working with FinCEN to process and approve requests for new IC PKI certificates where appropriate. While the progress is slow, a FinCEN official told us that FinCEN was able to support

---

[3] Venezuela is experiencing widespread public corruption. Venezuela faces severe economic and political circumstances due to the rupture of democratic and constitutional order by the government and its policy choices.

[4] Our ongoing audit is entitled "Audit of the Office of Intelligence and Analysis" and the audit was initiated on August 11, 2016. The audit objective is to assess OIA's progress in meeting its statutory responsibilities under the *Intelligence Authorization Act of 2004*.

requests related to Venezuela. OIA and FinCEN officials and staff continue to work together to approve access to new IC PKI certificates where appropriate.

During our audit we observed that the present working relationship between OIA and FinCEN related to the IC PKI process is strained. Understanding the basic differences in the way that FinCEN and OIA officials view the need for IC PKI access to support their roles and responsibilities, including FinCEN's autonomy, will improve cooperation between the two offices and enhance relationships between the two entities. The lack of documented policies and procedures related to IC PKI access are contributing to fundamental disagreements between the two components. We are concerned that if these fundamental differences related to IC PKI access are not addressed timely, the disagreements could negatively impact employee morale, reduce information sharing, and hamper TFI's ability to fulfill its overall mission.

Accordingly, we recommend that the Under Secretary for TFI ensures that (1) OIA and SSP clarify, formalize, and distribute IC PKI process policies and procedures; (2) employees at all levels are trained on the process and documentation required to efficiently gain IC PKI access; (3) an assessment is performed to determine the adequacy of staffing and system resources, as well as cross-training of SSP employees responsible for reviewing and renewing IC PKI certificates; and (4) OIA and FinCEN officials work together to ensure that they understand their roles and responsibilities.

Management's Response

Management concurs with and has taken action to implement our recommendations, including drafting policies and procedures, developing training, reviewing resources, and making a commitment to foster collaboration within TFI. Management's written response, in its entirety, is included as an attachment to this memorandum.

Background

Treasury's Process to Manage IC PKI Certificates

Within OIA, SSP is responsible for issuing and renewing IC PKI certificates to Treasury employees who need access to classified information held by other members of the IC. SSP determines the level of IC PKI certificate support it should provide to Treasury certificate holders. The Intelligence Community Standard

500-25*, Issuance of Intelligence Community Public Key Infrastructure Certificates,*[5] states that employees who demonstrate a mission need to access classified information held by other members of the IC shall be issued an IC PKI certificate. According to this standard, each IC element[6] shall integrate the issuance of IC PKI certificates into its respective business processes; document it in policies; and manage IC PKI certificates in a manner to ensure accuracy, security, privacy, and confidentiality through their lifecycle.

To be eligible to receive an IC PKI certificate, Treasury employees must possess Top Secret/Sensitive Compartmented Information (TS/SCI) access to classified information and a Treasury secured network account. When an employee meets these requirements, his or her manager must submit a written request for an IC PKI certificate to SSP demonstrating a mission need, to include information about the employee's assigned responsibilities and work topic areas, such as counterterrorism. SSP personnel then reviews the request to determine adequacy and support for the mission need. Once approved, SSP notifies the employee and requests that the employee schedule an in-person meeting with SSP staff to establish the IC PKI certificate and create his or her password. The IC PKI certificate process typically takes about two weeks assuming that the employee already has TS/SCI access, the employee's manager provides adequate justification for the mission need in the request, and the employee is responsive to SSP's notification to schedule the in-person meeting.

2015 Server Upgrade

In April and May 2015, Treasury had to issue new IC PKI certificates when Treasury's external service provider completed a server upgrade. One of the changes made with the upgrade was a shorter expiration period for the IC PKI certificates, going from 3 to 2 years. In other words, IC PKI certificates issued on the old server, expired 3 years from the date of issue, whereas certificates issued on the upgraded server, expire after 2 years. Because of the upgrade in 2015, approximately 300 Treasury employees needed new IC PKI certificates.

---

[5] Issued by the Office of the Director of National Intelligence and applies to the IC (July 12, 2012).

[6] Executive Order 12333, *United States Intelligence Activities,* as amended, establishes OIA as an element of the IC (July 30, 2008).

Audit Results

House of Representatives Committee June 2017 Email of Concern

In June 2017, a staff member of the U.S. House of Representatives Committee on Financial Services, Subcommittee on Terrorism and Illicit Finance, emailed our Inspector General and claimed that OIA initiated a mass revocation of FinCEN's IC PKI certificates that prevented FinCEN employees from effectively responding to law enforcement requests on the London and Manchester terrorist attacks.

OIA Did Not Revoke FinCEN Employees' IC PKI Access En Masse

OIA did not initiate a mass revocation of FinCEN's employees' IC PKI access; instead, a large number of Treasury employees, including 25 FinCEN employees, had IC PKI certificates that expired in April, May, or June 2017. Many of these FinCEN employees were unaware that their IC PKI access was expiring in May and June 2017 until after the expiration date. A reminder was sent by SSP to some OIA employees that expiration dates were approaching, however no such reminder was sent to FinCEN employees.

The expiration of IC PKI certificates was concentrated in the 3 month period from April to June 2017 as a result of actions SSP took in 2015 in response to the external server upgrade. Specifically, in April 2015, SSP and the external service provider notified Treasury IC PKI certificate holders, via email, of the server upgrade and that certificates were set to expire in May 2015. SSP met with Treasury employees to issue new IC PKI certificates. At the time, some employees were told that the expiration date was 2 years from the date of issue. SSP staff told us that when they met with IC PKI users[7] in 2015 to issue the new certificates, they verbally told the users that the certificates expired in 2 years. If asked, the SSP staff also let the users know that the user was responsible to track the expiration date of their IC PKI certificate. The responsibility for tracking IC PKI expiration dates is an important issue because in 2015 the external service provider notified SSP that users would receive no system reminders of expiration dates of their IC PKI certificates.

[7] The term "user(s)" means "certificate holder(s)".

In July 2017, we interviewed 19 TFI IC PKI certificate holders[8] out of a total of 135 Treasury employees[9] whose certificates were due to expire between April and June 2017. We interviewed the employees to confirm SSP's statements related to informing users of the IC PKI expiration dates and the responsibility for tracking the expiration date. Of the 19 certificate holders, 10 confirmed that SSP told them that the IC PKI certificate expired in 2 years, 6 could not remember if SSP relayed this information, and 3 said SSP did not give them this information. In addition, 3 of the 19 employees confirmed that SSP told them that it was the user's responsibility to remember the expiration date, 6 could not remember if SSP relayed this information, and 10 said SSP did not inform them of the responsibility to track the expiration date. Although we cannot extrapolate the results of these interviews to the total population of TFI IC PKI certificate holders, we were able to conclude that SSP did not consistently inform all IC PKI certificate holders of the 2 year expiration date and that the user was responsible to track the expiration date.

In 2017, when the IC PKI certificates issued in 2015 expired, SSP did not timely notify all users that their certificates were expiring. While SSP notified OIA employees in advance of the IC PKI certificates expiring, other employees within TFI were notified as their certificates were expiring or after their certificates expired. In prioritizing which employees to notify, SSP staff told us that they first reviewed the expiration dates and the employees' need for access. SSP staff also told us that notifications to OIA employees were prioritized over other TFI employees because of OIA's work in the IC and responsibility to perform intelligence-related functions. SSP did not send notifications to many other TFI IC PKI certificate holders, including the 25 FinCEN employees whose certificates expired in May and June 2017, until after their certificates expired. Immediately after the London terrorist attack on June 3, 2017, some FinCEN employees whose IC PKI certificates had expired were notified. SSP personnel told us that the notifications were sent after the IC PKI certificates expired because of SSP time and resource constraints. Specifically, SSP has two employees with responsibilities for issuing and renewing IC PKI certificates, in addition to other responsibilities. According to SSP staff, it takes 20 to 30 minutes to issue or renew an IC PKI certificate and SSP only has one computer reserved for these tasks. The SSP staff also told us that in May and June 2017 they were busy renewing IC PKI certificates for previously contacted employees whose certificates expired or were about to expire. Personnel from SSP and Treasury's external service provider told

---

[8] The 19 employees that we interviewed work for OIA, FinCEN, the Office of Foreign Assets Control, and the Office of Terrorist Financing and Financial Crimes.

[9] Between March and June 2017, SSP identified 135 Treasury employees whose certificates were set to expire in April, May, and June 2017.

us that it is the Treasury IC PKI user's responsibility to remember their expiration date because the IC PKI system does not provide automatic reminders to its users.

While there is no policy or procedure that requires SSP to remind IC PKI users that their certificates are expiring, we found that users were not consistently aware that it was the user's responsibility to track the expiration date. This resulted in FinCEN users' IC PKI certificates expiring without their knowledge. We believe that SSP should have informed every user of the responsibility to track the expiration date. SSP is currently developing IC PKI certificate policies and procedures, and with the 2017 renewals, SSP is informing users of the next expiration date and the user's responsibility for tracking the expiration date in 2019. SSP staff also told us that they plan to maintain a list of IC PKI certificate expiration dates going forward, and to the extent possible and practical, will remind IC PKI users before certificates expire.

FinCEN Effectively Provided Information to Law Enforcement Related to the London and Manchester Attacks

Although 25 FinCEN employees' IC PKI certificates expired in May and June 2017, FinCEN was able to effectively provide law enforcement-related information on the London and Manchester terrorist attacks. Contrary to the claim in the June 2017 email that the revocation prevented FinCEN from effectively responding to law enforcement requests on the London and Manchester terrorist attacks, the Associate Director of FinCEN's Intelligence Division told us that FinCEN was able to respond to law enforcement requests by using an employee who had a valid and working IC PKI certificate.

By late June 2017, SSP resolved 21 out of the 25 FinCEN employees' expired IC PKI certificates. Although SSP staff contacted the remaining four FinCEN employees, as of the end of June 2017 these FinCEN employees had not completed the required renewal appointment with SSP.

FinCEN Employee August 2017 Email of Concerns

In August 2017, our Office of Inspector General Counsel's office was copied on an email from a FinCEN employee claiming that some key FinCEN staff did not have IC PKI certificates even though the Acting Director of FinCEN submitted IC PKI requests to SSP before February 2017. The email also stated that the lack of IC PKI access prevented FinCEN from fully responding to the Under Secretary for TFI and the White House regarding Venezuela. Even though the author of the email

claimed that the request for IC PKI access was sent to OIA as far back as February 2017, our audit found evidence that FinCEN sent the IC PKI request in April 2017.

According to SSP, FinCEN IC PKI Certificate Requests Are Inadequate

In April 2017, the Acting Director of FinCEN gave OIA a list identifying 66 FinCEN employees with "pending" requests for IC PKI certificates as of March 21, 2017. After April, FinCEN requested IC PKI certificates for 12 more employees, bringing the total to 78 employees. While reviewing information to validate FinCEN's requests, SSP identified inadequacies with FinCEN's requests that slowed the process. For example, the requests for the 78 new IC PKI certificates did not always include justifications explaining why the employees needed the IC PKI certificate, specifically the mission need. The 78 IC PKI requests also included errors. For example, FinCEN included employees who already had IC PKI certificates and employees who needed only a secured network account or did not have a secured network account which is a prerequisite to requesting IC PKI access.

To get a secured network account, an employee must have TS/SCI access. To validate FinCEN employees having TS/SCI access, SSP staff verified the names of FinCEN employees with the Treasury employee directory and SCI database. In some cases, the names on FinCEN's lists could not be verified against Treasury databases. SSP management told us FinCEN could have either spelled the name wrong or listed a nickname for the employee. To better understand FinCEN's roles and responsibilities related to the need to access intelligence information, SSP met with some FinCEN employees and managers in May 2017. In June 2017, OIA and FinCEN management met to discuss pending IC PKI certificate requests. An OIA official told us that at one of the meetings, the Acting Director of FinCEN told OIA officials that additional justifications would be provided. On July 28, 2017, OIA emailed the Acting Director of FinCEN an updated list that included 62 FinCEN employees whose requests needed additional information. The majority of these employees were either waiting for their TS/SCI approval or had inadequate justification for the IC PKI access request. When we interviewed the Acting Director of FinCEN on August 24, 2017, he told us that he was not aware that OIA was waiting for FinCEN to provide additional justification on such a large number of employees.

In response to our audit, FinCEN conducted a comprehensive review of the 78 IC PKI requests and determined that more than half, specifically 44, were included in error. In fact, FinCEN only needed IC PKI certificates for 34 employees. According to FinCEN officials, IC PKI requests submitted erroneously included requests for

employees who did not need IC PKI certificates. The FinCEN officials also told us that the errors were caused by internal FinCEN miscommunication as many employees only needed a secured network account. As of September 25, 2017, SSP approved new IC PKI certificates for 14 of the 34 employees. FinCEN continues to meet with OIA and FinCEN is working towards providing OIA with additional information needed for SSP to approve IC PKI certificates for 15 employees. The details on the status of FinCEN requests as of September 25, 2017, are summarized in Table 1 below.

Table 1. Status of FinCEN IC PKI Requests as of September 25, 2017

Status of FinCEN IC PKI Requests	**Number of Employees**
Employee approved for a new certificate	14
SSP waiting for support/justification from FinCEN	15
Pending SSP approval	2
Requested and employee later left FinCEN	3
FinCEN IC PKI Requests in Error	44
Total	**78**

Source: SSP and FinCEN Personnel

FinCEN Provided Timely Information Related to Venezuela

We found that the August 2017 email claim that the lack of IC PKI access prevented FinCEN from fully responding to the Under Secretary for TFI and the White House related to Venezuela is not entirely accurate. A FinCEN official told us that the White House requested the Office of Foreign Assets Control (OFAC) to provide information on Venezuela and OFAC subsequently requested FinCEN's support in this effort. According to the FinCEN official, FinCEN was able to support OFAC's request, although the FinCEN subject matter experts did not have IC PKI access.

Roles and Responsibilities Regarding IC PKI Need Further Clarification

One of OIA's statutory responsibilities per U.S.C. §312[10] is to provide intelligence support to FinCEN. Some of FinCEN's statutory responsibilities in U.S.C. §310[11] relating to financial intelligence and financial criminal activities include maintaining a government-wide data access service, analyzing and disseminating data to law enforcement, assisting financial institutions and law enforcement and regulatory entities with research and combatting illegal transfers of funds, and coordinating with financial intelligence units in other countries. In addition, the *Treasury Intelligence Enterprise Management Guidelines* state that certain activities should be conducted in consultation with OIA, such as interaction with IC members related to the receipt, analysis, collation, or dissemination of intelligence or counterintelligence information.[12] An OIA official told us that FinCEN rarely consults with OIA and often times does not provide their intelligence needs to OIA. But according to FinCEN officials, FinCEN should be able to conduct their own intelligence research, without relying on OIA.

FinCEN officials also told us that FinCEN employees with TS/SCI access and a Treasury secured network account should automatically be granted an IC PKI certificate given the nature of FinCEN's work. A FinCEN official stated that providing additional justifications for an IC PKI certificate after FinCEN has already provided a justification for TS/SCI access is a duplication of effort. However, according to the OIA staff, the majority of justifications that FinCEN provided to request IC PKI certificates are not adequate or do not demonstrate mission need.

Understanding these basic differences in the way that FinCEN and OIA officials view the need for IC PKI access to support their individually defined roles and responsibilities, including FinCEN's autonomy, will improve cooperation between the two offices and enhance the relationship between the two entities. Policies and procedures related to IC PKI access are not documented. We are concerned that if these fundamental differences related to IC PKI access are not addressed timely,

---

[10] 31 U.S.C. §312 (b)(3)(A), *Terrorism and financial intelligence,* requires OIA to build a robust analytical capability on terrorist finance by coordinating and overseeing work involving intelligence analysts in all components of Treasury, focusing on the highest priorities of the Department, as well as ensuring that the existing intelligence needs of OFAC and FinCEN are met (December 8, 2004).

[11] 31 U.S.C. §310 (b)(2), *Financial Crimes Enforcement Network* (July 1, 2010)

[12] Former Acting Under Secretary for TFI, Adam Szubin, issued the *Treasury Intelligence Enterprise Management Guidelines* on January 12, 2017, to provide employees with a framework for a future Treasury Order and to govern applicable activities for Treasury until an order is issued.

the disagreements could lead to poor morale, reduced information sharing, and TFI's inability to fulfill its overall mission.

Recommendations

We recommend that the Under Secretary for TFI ensures that:

1. OIA and SSP clarify, formalize, and distribute IC PKI process policies and procedures;
2. employees at all levels are trained on the process and documentation required to efficiently gain IC PKI access;
3. an assessment is performed to determine the adequacy of staffing and system resources, as well as cross-training of SSP employees responsible for reviewing and renewing IC PKI certificates; and
4. OIA and FinCEN officials work together to ensure that they understand their roles and responsibilities.

Management's Response

Management concurs with the recommendations and has taken action to implement the recommendations:

1. At TFI's direction, OIA SSP drafted standard operating procedures (SOP) that clarify the IC PKI processes to include detailed information about the procedures for requesting an IC PKI certificate. The draft SOPs were shared with OIG and are in the process of being finalized.
2. OIA SSP is developing and will deliver training on the process for requesting, receiving, and renewing IC PKI certificates to all supervisors and employees who require IC PKI certificates or who are involved in the issuance and maintenance of IC PKI certificates. TFI will deliver the training immediately upon development and will provide the training on a regular basis going forward.
3. At TFI's direction, OIA has initiated a review of staffing and system resources with an identified project manager to assess SSP capabilities for processing and managing the IC PKI certificates. TFI plans to closely monitor this assessment.

4. The SOPs and training will better define roles and responsibilities of OIA and FinCEN relating to the IC PKI certificates. Moreover, the Under Secretary has made fostering greater collaboration among all TFI components, including OIA and FinCEN, a top priority. Among other things, TFI is developing and executing strategies that calibrate broad economic authorities so that components are proactively working together to enhance TFI's effectiveness and maximize the offices' impact.

Management's response is included as an attachment to this memorandum.

OIG Comment

The corrective actions taken and planned are responsive to the recommendations.

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.

We appreciate the cooperation and courtesies extended to our staff during this audit. If you have any questions, you may contact me at (202) 927-5400 or Kieu Rubb, Audit Director, at (202) 927-5904.

UNDER SECRETARY

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C.

October 27, 2017

MEMORANDUM FOR ASSISTANT INSPECTOR GENERAL DEBORAH L. HARKER

FROM: Sigal P. Mandelker
Under Secretary
Office of Terrorism and Financial Intelligence

SUBJECT: Management Response to the Audit of the Office of Intelligence and Analysis' Management of the Office of Terrorism and Financial Intelligence Employees' Intelligence Community Public Key Infrastructure Certificates

Thank you for providing the Office of Terrorism and Financial Intelligence (TFI) with an opportunity to review the Office of the Inspector General's (OIG's) formal draft audit report on the Office of Intelligence and Analysis' (OIA's) management of TFI's employees' IC Public Key Infrastructure (IC PKI) certificate. TFI shares the OIG's commitment to ensuring our programs operate efficiently and effectively to meet our national security mission. This letter provides our official response to the draft report.

I concur with the OIG's recommendations for strengthening the processes and training relating to applying for and issuing IC PKI certificates. This effort was already underway at my direction and at the direction of OIA leadership. I also concur with the OIG's recommendation to conduct an assessment of the adequacy of the responsible staffing and supporting systems, and we have assigned a project manager to accomplish this task. We have initiated actions with a specific implementation plan in place to strengthen the program and expeditiously complete the recommendations.

Specifically, OIA has drafted Standard Operating Procedures, which will be finalized shortly, that clarify the IC PKI processes to include detailed information about the procedures for requesting an IC PKI certificate. Additionally, OIA's Office of Special Security Programs (SSP) is developing and will deliver training on the process for requesting, receiving, and renewing IC PKIs to all supervisors and employees who require IC PKI certificates or who are involved in the issuance and maintenance of IC PKI certificates. OIA also has underway an assessment of staffing and systems resources to include a review of any additional requirements for cross-trained SSP employees to ensure that an adequate number of appropriately trained personnel are available to efficiently and accurately process requests for IC PKI certificates.

In addition to strengthening management of the IC PKI program, fostering greater collaboration within TFI, including between OIA and FinCEN, is one of my top priorities. Among other things, we are working on and executing strategies that calibrate our broad economic authorities so that our components are proactively working together to enhance our effectiveness and maximize our impact. We are that much more successful when we bring our tools together to inform our decision-making and achieve long-term strategic impact.

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C.

UNDER SECRETARY

I will personally monitor the implementation of these actions closely to ensure that TFI employees are efficiently granted access to the data required for performing their mission in a way that safeguards the security of our systems. The professionals of TFI will continue working together to further enhance our economic and national security and safeguard the integrity of the international financial system.

We appreciate the role of the OIG in providing oversight of our programs and look forward to continuing to work with our office in the future.

TFI Management Response to the report recommendations:
Recommendation 1: Management concurs with the recommendation. At TFI's direction, OIA SSP drafted an SOP that clarifies the IC PKI processes to include detailed information about the procedures for requesting an IC PKI certificate. This draft SOP has been shared with OIG and is in the process of being finalized.

Recommendation 2: Management concurs with the recommendation. OIA SSP is developing and will deliver training on the process for requesting, receiving, and renewing IC PKIs to all supervisors and employees who require IC PKI certificates or who are involved in the issuance and maintenance of IC PKI certificates. The training will take place immediately upon development and be provided on a regular basis going forward.

Recommendation 3: Management concurs with the recommendation. At TFI's direction, OIA has initiated a review of staffing and system resources with an identified project manager to assess SSP capabilities for processing and managing the IC PKI certificates. TFI will closely monitor this assessment.

Recommendation 4: Management concurs with the recommendation. The SOPs and training will better define roles and responsibilities of OIA and FinCEN relating to the IC PKI certificates. Moreover, the Under Secretary has made fostering greater collaboration among all TFI components, including OIA and FinCEN, a top priority. Among other things, TFI is developing and executing strategies that calibrate our broad economic authorities so that our components are proactively working together to enhance our effectiveness and maximize our impact. We are that much more successful when we bring our tools together to inform our decision-making and achieve long-term strategic impact.

Treasury OIG Website

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

Report Waste, Fraud, and Abuse

OIG Hotline for Treasury Programs and Operations – Call toll free: 1-800-359-3898
Gulf Coast Restoration Hotline – Call toll free: 1-855-584.GULF (4853)
Email: Hotline@oig.treas.gov
Submit a complaint using our online form:
https://www.treasury.gov/about/organizational-structure/ig/Pages/OigOnlineHotlineForm.aspx