Audit Memorandum

OIG-18-044

TERRORIST FINANCING/MONEY LAUNDERING

Audit of the Office of Intelligence and Analysis' Authorities and Actions Related to U.S. Persons' Financial Information

April 9, 2018

Office of Inspector General

Department of the Treasury

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

OFFICE OF
INSPECTOR GENERAL

April 9, 2018

OIG-18-044

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' Authorities and Actions Related to U.S. Persons' Financial Information

This report presents results from our ongoing audit of the Department of the Treasury (Treasury) Office of Intelligence and Analysis (OIA). Our audit objective is to assess OIA's progress in meeting its statutory responsibilities. This is the second of three audit reports related to our objective.[1] We are issuing this report to respond to a November 2017 request from the Chairman and Ranking Member of the U.S. Senate Committee on Finance. We plan to issue a third and final report related to our audit objective by the end of fiscal year 2018. The committee requested information from our audit of OIA authorities and actions related to the collection, retention, and review of domestic financial information on U.S. Persons (USP).[2] The request cited an article published by *BuzzFeed News* (*BuzzFeed*) in October 2017[3] claiming that OIA "repeatedly and systematically violates domestic surveillance laws by snooping on the private financial records of U.S. citizens and companies." More specifically, the *BuzzFeed* claim states that OIA analysts are (1) illegally collecting and retaining domestic financial information from the Bank

---

1 We issued the first report related to our objective on October 30, 2017, *Audit of the Office of Intelligence and Analysis' Management of the Office of Terrorism and Financial Intelligence Employees' Intelligence Community Public Key Infrastructure Certificates* (OIG-18-006), https://www.treasury.gov/about/organizational-structure/ig/Audit%20Reports%20and%20Testimonies/OIG-18-006.pdf

2 For purposes of this report, the term "financial information" refers to customer information held by a financial institution, such as bank accounts and transactions. The term "USP" or "U.S. persons" means a U.S. citizen, an alien known by the intelligence element concerned to be a permanent resident alien, an unincorporated association substantially comprising U.S. citizens or permanent resident aliens, or a corporation incorporated in the United States, except for a corporation directed and controlled by a foreign government or governments.

3 Jason Leopold and Jessica Garrison, "U.S. Intelligence Unit Accused of Illegally Spying on Americans' Financial Records," *BuzzFeed News* (October 6, 2017), https://www.buzzfeed.com/jasonleopold/us-intelligence-unit-accused-of-illegally-spying-on?utm_term=.icO44m4V3L#.krn22v2Gab

Secrecy Act (BSA) database maintained by the Financial Crimes Enforcement Network (FinCEN)[4] because OIA does not have USP procedures approved by the Attorney General of the United States (Attorney General), (2) contacting financial institutions to make inquiries about individual bank accounts and transactions involving U.S. citizens, and (3) exceeding the limits of the agreement between OIA and FinCEN that allows OIA access to FinCEN's banking database.[5]

To address the three *BuzzFeed* claims against OIA, we (1) reviewed applicable intelligence community (IC), Treasury, and other Federal guidance; (2) reviewed the *Memorandum of Understanding Between the Financial Crimes Enforcement Network and the Office of Intelligence and Analysis* (MOU) and OIA's draft version of *Procedures for U.S. Department of the Treasury Intelligence Activities* (USP Procedures); (3) interviewed officials and personnel within OIA, Treasury's Office of General Counsel (OGC), the Office of the Director of National Intelligence (ODNI), and FinCEN; (4) surveyed FinCEN employees to gather information about the claims; and (5) non-statistically selected BSA queries made during January 2017 through March 2017 for testing. We made our selection from a population of BSA queries run by OIA analysts who perform intelligence and counterintelligence work. The population comprised 462 queries,[6] and we tested 44, or approximately 10 percent of the population. To test the queries in our selection, we interviewed OIA analysts and reviewed available documentation supporting the purpose for each query. Because our selection was non-statistical, the results of our testing cannot be projected to the population.

---

[4] 31 U.S.C. 310 requires FinCEN to maintain a government-wide data access service and provide access to information collected by FinCEN under the BSA. *The Currency and Foreign Transactions Reporting Act of 1970* (commonly referred to as the "Bank Secrecy Act" or "BSA") requires U.S. financial institutions to assist U.S. government agencies to detect and prevent money laundering. FinCEN is responsible to implement, administer, and enforce compliance with the BSA.

[5] *Memorandum of Understanding Between the Financial Crimes Enforcement Network and the Office of Intelligence and Analysis,* September 21, 2009.

[6] OIA analysts ran 964 queries during the scope of our review. Using a report generated from the BSA database, we were able to identify queries that resulted in a document being viewed or downloaded. We removed any queries that did not result in an analyst reviewing or downloading any documents. This resulted in a population of 462 queries. Analysts often do not review or download most (and in some cases any) documents related to their searches. They must limit the BSA information they obtain through a query to only the information useful in connection with the specific matter prompting the query.

Results In Brief

We found that the *BuzzFeed* claims were not supported. Specifically, we did not find evidence to substantiate the claims that OIA analysts are (1) illegally collecting and retaining domestic financial information from FinCEN's BSA database, (2) contacting financial institutions to make inquiries about individual bank accounts and transactions involving U.S. citizens, or (3) violating the MOU with FinCEN.

However, OIA's USP Procedures have not been approved by the Attorney General as required by Executive Order (EO) 12333, "United States Intelligence Activities."[7] Despite the lack of approved USP procedures, OIA's statutory authorities under the *Consolidated Appropriations Act of 2005*[8] and EO 12333 permit OIA to legally collect, retain, and disseminate USP information until its USP Procedures are approved. Furthermore, EO 12333 does not prescribe a deadline for approving USP procedures and instructs IC elements that until its USP procedures are approved, USP activities[9] shall be conducted in accordance with an agency's existing procedures or requirements established under EO 12333. OIA is conducting its USP activities under the requirements established in EO 12333. Specifically, OIA's intelligence effort is to focus on providing necessary information meant for the development and conduct of foreign, defense, and economic policies, as well as the protection of U.S. national interests from foreign security threats.

OIA has a working draft of its USP Procedures, which includes guidelines on collecting, retaining, and disseminating USP information. A Treasury OGC official told us that although OIA's USP Procedures are in draft form, Treasury's OGC looks to both section 2.3 of EO 12333, *Collection of Information*, and their draft USP Procedures when resolving particular questions involving the collection, retention, or dissemination of USP information. Although not yet implemented, OIA's draft USP Procedures state that OIA will conduct periodic reviews to verify continued compliance with the procedures. A compliance program is not required by EO 12333, but we believe it is prudent for OIA to implement such oversight.

Accordingly, we recommend that as expeditiously as possible the Under Secretary for Terrorism and Financial Intelligence ensure that (1) OIA's USP Procedures are finalized and submitted for approval to the Attorney General and (2) OIA implements a compliance monitoring program to assess whether intelligence analysts' activities are conducted in accordance with OIA authorities, and

---

7 As amended, July 2008

8 P.L. 108-447, Consolidated Appropriations Act, 2005 (December 8, 2004)

9 For purposes of this report, USP activities refers to the collection, retention, and dissemination of USP information.

electronic searches and other queries are performed in a manner that fully protects the rights of U.S. persons.

Management's Response

Management concurs with and has taken action to implement our recommendations, including providing its draft USP Procedures to the Department of Justice (DOJ) and ODNI for review and Attorney General approval. Management has assigned an Oversight Coordinator to work with Treasury's OGC on developing a compliance monitoring program. Management's written response, in its entirety, is included as an attachment to this memorandum.

Background

The *Intelligence Authorization Act of 2004*[10] established OIA as an office within Treasury and as an element of the IC. The *Consolidated Appropriations Act of 2005* established Treasury's Office of Terrorism and Financial Intelligence (TFI), headed by an Under Secretary to whom OIA, FinCEN, the Office of Terrorist Financing and Financial Crimes, the Office of Foreign Assets Control (OFAC), and the Treasury Executive Office for Asset Forfeiture all report.

In July 2008, EO 12333 was amended and formally recognized OIA as Treasury's IC element, responsible for serving as a liaison to the IC and as the Treasury representative in various intelligence-related activities. In 2004, Congress tasked OIA with two primary functions: (1) build a robust analytical capability on terrorist finance by coordinating and overseeing work involving intelligence analysts in all Treasury components and ensuring that the existing intelligence needs of OFAC and FinCEN are met; and (2) provide intelligence support to Treasury senior officials.[11]

On a broader scale, EO 12333 provides guidelines for the effective conduct of U.S. intelligence activities and for the protection of constitutional rights. EO 12333 assigns the goals, directions, duties, and responsibilities with respect to U.S. intelligence efforts and provides requirements for the conduct of intelligence agencies in the collection, protection, and dissemination of intelligence information. According to section 1.1 of EO 12333, *Goals*, the U.S. intelligence effort is meant to provide necessary information for the development and conduct of foreign,

[10] P.L. 108-177, Intelligence Authorization Act for Fiscal Year 2004 (December 13, 2003)
[11] P.L. 108-447, Consolidated Appropriations Act, 2005 (December 8, 2004)

defense, and economic policies, as well as the protection of U.S. national interests from foreign security threats.

Audit Results

An October 2017 *BuzzFeed* article claims that OIA analysts are (1) illegally collecting and retaining domestic financial information from FinCEN's BSA database because it does not have approved USP procedures, (2) contacting financial institutions to make inquiries about individual bank accounts and transactions involving U.S. citizens, and (3) exceeding the limits of the agreement between OIA and FinCEN that allows OIA access to FinCEN's banking database.

Claim 1: OIA Is Illegally Collecting and Retaining Domestic Financial Information From FinCEN's BSA Database

According to the *BuzzFeed* claim, OIA is illegally collecting and retaining domestic financial information from FinCEN's BSA database because it does not have approved USP procedures. The article cites EO 12333 language authorizing IC elements to collect, retain, and disseminate USP information only in accordance with its USP procedures, which are to be developed by the head of the IC element and approved by the Attorney General after consultation with ODNI. We found that OIA's statutory authorities under the *Consolidated Appropriations Act of 2005* and EO 12333 permit OIA to legally collect, retain, and disseminate USP information until its USP Procedures are approved by the Attorney General. Furthermore, EO 12333 does not prescribe a deadline for approving USP procedures and instructs IC elements that until its USP procedures are approved, USP activities shall be conducted in accordance with an agency's existing procedures or requirements established under EO 12333.

Finding – OIA's USP Procedures Have Not Been Approved by the Attorney General

OIA does not have Attorney General-approved USP procedures; it has a working draft. Section 2.3 of EO 12333, *Collection of Information,* requires elements of the IC to establish USP procedures for its USP activities. In developing USP procedures, agencies are required to consult with the Director of ODNI and to have the

procedures approved by the Attorney General.[12] However, the lack of Attorney General-approved USP procedures does not prevent OIA from legally collecting and retaining domestic financial information from FinCEN's BSA database. OIA is legally conducting its USP activities within statutory authorities granted under the *Consolidated Appropriations Act of 2005* and EO 12333. The *Consolidated Appropriations Act of 2005* states that OIA shall be responsible for the receipt, analysis, collation, and dissemination of intelligence and counterintelligence information related to the operations and responsibilities of the Treasury. EO 12333 also permits OIA to collect, retain, and disseminate ten types of information, for example, information that constitutes foreign intelligence or counterintelligence or is obtained in the course of a lawful foreign intelligence, counterintelligence, international drug or terrorism investigation. Furthermore, Section 3.3 of EO 12333, *Procedures*, acknowledged that there would be a period of time where IC elements would be drafting USP procedures or updating existing USP procedures for approval by the Attorney General based on the 2008 revisions. As such, it instructed IC elements that until USP procedures are approved, USP activities shall be conducted in accordance with an agency's existing procedures or requirements established under EO 12333. The order does not prescribe a deadline for approving USP procedures, but it directs agencies to finalize them as expeditiously as possible.

Some legacy IC elements had existing USP procedures approved prior to the 2008 revision of EO 12333.[13] These legacy elements were required to operate under those existing procedures until updated procedures could be approved by the Attorney General. OIA did not have existing USP procedures approved prior to the 2008 EO revisions because it was a relatively new IC element.[14] Therefore, in accordance with Section 3.3 of EO 12333, to conduct USP activities within its statutory authority, OIA must follow the requirements established under EO 12333 until its USP procedures are approved by the Attorney General.

---

[12] The July 2008 revision to EO 12333 included the Director of ODNI to serve in a consultative role intended to help ensure that the rules for collecting, retaining, and disseminating USP information are consistent and harmonized in a manner that facilitates information sharing while protecting privacy and civil liberties. Previous versions of EO 12333 did not include the Director of ODNI as part of the approval process.

[13] Some of the larger IC elements that (1) were created prior to 1981, when EO 12333 was initially implemented, and (2) are traditional collectors of USP information, had USP procedures prior to the 2008 revision. The 2008 EO 12333 revisions required these existing procedures to be updated and approved by the Attorney General.

[14] OIA was established as Treasury's IC element in 2003. However, prior to revisions made in 2008, EO 12333 did not formally recognize OIA as an IC element.

OIA is not an outlier within the IC in its progress to finalize its USP Procedures. The Federal Bureau of Investigation was the only IC element to get its USP procedures approved immediately after the 2008 EO 12333 revisions. It was not until August 2016 when the next set of USP procedures, from the Department of Defense, were approved by the Attorney General. As of December 2017, the Attorney General approved USP procedures based on the 2008 EO 12333 revisions for only 5 of the 17 IC elements. An official from ODNI's OGC told us that the focus has been on approving and finalizing the USP procedures for IC elements that are traditional collectors of USP information, such as the Central Intelligence Agency.[15]

Our review of documentation found that Treasury has been working on draft procedures since 2008. A Treasury OGC[16] official told us that they have been actively working to finalize their draft USP Procedures with DOJ's National Security Division (NSD)[17] and ODNI's OGC. For example, they have been working together to develop template language for USP procedures to ensure consistency among IC elements. Emails between Treasury's OGC, NSD, ODNI's OGC, and other IC elements confirm that Treasury personnel have been communicating to discuss the mutual principles to guide IC element draft procedures, including common definitions and processes. Our review of emails between Treasury's OGC and ODNI's OGC show active review of and communication on OIA's draft USP Procedures.

A Treasury OGC official told us that, although OIA's USP Procedures are in draft form, they provide a framework through which Treasury's OGC advises OIA on its substantive USP requirements under EO 12333. OIA's draft USP Procedures provide guidance related to mission specific activities. Treasury's OGC looks to both paragraph 2.3 of EO 12333 and the draft USP Procedures when resolving particular questions involving the collection, retention, or dissemination of USP information and in crafting the annual training on the protection of USP information

---

[15] The Central Intelligence Agency is permitted to collect intelligence through clandestine means. OIA is only authorized to collect overtly or through publicly available sources.

[16] Although the head of an IC element is responsible for approving USP procedures, at Treasury, OGC is leading efforts to draft the agency's USP Procedures.

[17] NSD supports the Federal Government's national security efforts by ensuring greater coordination and unity of purpose between (1) prosecutors and law enforcement agencies and (2) intelligence attorneys and the IC.

provided to each OIA employee.[18] We reviewed OIA's draft USP Procedures and identified that they contain guidelines on collection, retention, and dissemination for the protection of USP information as stated in EO 12333.

In OIA's draft USP Procedures, it states that OIA will conduct periodic reviews to verify continued compliance with the procedures. This includes compliance with any memoranda of understanding or other agreements regarding access to datasets and compliance with all safeguards, procedures, and oversight mechanisms. OIA has not yet implemented this compliance program. According to the draft procedures, OIA has 6 months from the effective date of its Attorney General-approved USP procedures to implement compliance requirements. The draft procedures also more specifically require OIA to take reasonable steps, within 18 months from the effective date, to audit access to electronic data containing information concerning U.S. persons and to audit queries or other searches to assess compliance with these procedures.

A compliance program is not required by EO 12333; however, according to the Government Accountability Office's *Standards for Internal Control in the Federal Government,*[19] management should establish and operate monitoring activities to monitor the internal control system and evaluate the results. This can be achieved through ongoing monitoring built into the entity's operations, which is performed continually and is responsive to change. Management uses ongoing monitoring to obtain reasonable assurance of the operating effectiveness of the organization's internal controls over the assigned process. Independent of the timing of approval of its USP Procedures, we believe it is prudent for OIA to implement a monitoring program to provide management with reasonable assurance that intelligence activities are conducted in accordance with OIA's authorities and the rights of U.S. persons are protected. In the absence of a monitoring program, there is a risk that unauthorized activities will go undetected.

Although EO 12333 does not prescribe a deadline for establishing USP procedures, finalized Attorney General-approved USP procedures would provide OIA the

---

[18] Intelligence Community Directive 102*, Process for Developing Interpretive Principles and Proposing Amendments to Attorney General Guidelines Governing the Collection, Retention, and Dissemination of Information Regarding U.S. Persons* (November 19, 2007), states that the OGCs for the IC elements will work closely with those responsible for education and training in each IC element to ensure that effective and up-to-date USP training is available to all IC personnel who handle USP information.

[19] The Government Accountability Office's *Standards for Internal Control in the Federal Government* (September 2014), issued by the Comptroller General of the United States, is known as the Green Book and provides the overall framework for establishing and maintaining an effective internal control system.

opportunity to ensure that USP activities are being conducted in a manner approved by the Secretary of the Treasury and the Attorney General. The lack of approved USP procedures increases the risk of OIA exceeding its authorities related to USP activities.

Recommendations

We recommend that as expeditiously as possible the Under Secretary for Terrorism and Financial Intelligence ensure that (1) OIA's USP Procedures are finalized and submitted for approval to the Attorney General and (2) OIA implements a compliance monitoring program to assess whether intelligence analysts' activities are conducted in accordance with OIA authorities, and electronic searches and other queries are performed in a manner that fully protects the rights of U.S. persons.

Management's Response

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

1. OIA provided a revised draft of the USP Procedures to DOJ and ODNI for review and, ultimately, Attorney General approval.

2. OIA assigned an Oversight Coordinator to work with OGC on developing an appropriate compliance monitoring program.

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

OIG Comment

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

Claim 2: OIA Is Contacting Financial Institutions To Inquire About U.S. Citizens' Bank Accounts and Transactions

The *BuzzFeed* claim alleges that OIA analysts are contacting financial institutions to inquire about bank accounts and transactions involving U.S. citizens. Unnamed sources cited in the *BuzzFeed* article claim that banks are under the impression they are complying with requests for information made by FinCEN. Specifically, a source for the article alleges that OIA personnel sought information in 2016 from a Delaware financial institution.

According to OIA, Analysts Do Not Request Financial Information From Financial Institutions

We did not find evidence to substantiate the claim that OIA analysts contacted financial institutions to request USP information. OIA is not prohibited from directly requesting USP information from a financial institution without coordination with FinCEN. However, if doing so, OIA must comply with *The Right to Financial Privacy Act* (RFPA),[20] which provides substantial consumer protections. The act protects the confidentiality of personal financial records by requiring federal government agencies to provide individuals with a notice and an opportunity to object before a financial institution discloses their personal financial information.

We interviewed 13 OIA analysts, and they all told us that they do not reach out directly to financial institutions to request financial information. They said that they contact FinCEN if they require additional information from financial institutions beyond what is available in the BSA system. FinCEN may then solicit financial institutions for information related to a BSA report[21] on behalf of OIA.

We also surveyed all FinCEN employees from the Intelligence, Enforcement, Liaisons, and Policy divisions, requesting that they contact us to report any known instances of an OIA employee directly contacting a financial institution. Two FinCEN employees responded to our request, stating that OIA analysts directly contacted financial institutions. One employee stated that documented examples of such contact had previously been provided. The documentation provided for our review included examples of what the employee regarded as instances of OIA reaching out to financial institutions and attending financial institutions' presentations. However, the documentation did not support the FinCEN employee's or *BuzzFeed's* claim. For example, the *BuzzFeed* article claims that, in 2016, OIA personnel sought information from a Delaware financial institution. We were provided emails in which an OIA employee requested FinCEN's assistance in addressing a Federal Bureau of Investigation agent's request to discuss money-laundering vulnerabilities in Delaware. FinCEN responded to the email, providing points of contact and stating that FinCEN should take the lead. The email did not indicate that OIA took action to directly contact the financial institution to request financial information.

---

[20] 12 U.S.C. 3401 et seq.

[21] 31 CFR 1010.520, *Information Sharing Between Government Agencies and Financial Institutions*

The second employee that responded to our survey did not provide us with an example of a specific instance where an OIA employee directly contacted a financial institution. The employee provided us with a broad statement of hearsay that an OIA employee reached out to a financial institution, but the employee did not provide us with details, such as the financial institution's name, specific type of requested information, or date the contact occurred. The employee did not observe the claimed event or see documentation that the event occurred. We requested additional details related to the employee's assertion, but the employee did not provide us any additional information. Therefore, we were unable to validate this assertion.

Claim 3: OIA Is Violating the MOU

The *BuzzFeed* claim alleges that OIA exceeds the MOU's limits regarding its access to the BSA database beyond specific foreign intelligence purposes. Additionally, it claims that OIA permits other IC elements to work at OIA for short periods, thereby receiving unrestricted access to USP information that they otherwise could not collect without strict oversight.

OIA's BSA Queries Meet the Intent of the MOU
We reviewed OIA's BSA queries and found no evidence that any of the queries exceeded OIA's statutory authorities, violated USP protections under EO 12333, or exceeded authorities granted under the MOU with FinCEN. Our population was 462 OIA analyst queries made during January through March of 2017 that resulted in a review or download of BSA data. We non-statistically selected 44 queries, approximately 10 percent of the population, conducted by 11 out of 16 OIA analysts that have access to the BSA database. We found that each query tested was directly linked to OIA's mission, a final work product, and/or a documented justification for the query.

FinCEN is obligated under its statutory mandate to provide OIA certain reports or records that are highly useful to OIA's intelligence or counterintelligence activities, including analysis to protect against international terrorism.[22] Based on this responsibility, FinCEN provides OIA with direct electronic access to its BSA database. The terms of OIA's access are defined in an MOU between FinCEN and OIA. Under these terms, OIA may obtain and use the information in the database for any queries consistent with OIA's statutory authorities, EO 12333, and for a purpose consistent with the BSA. Specifically, OIA's intelligence efforts are to provide necessary information meant for the development and conduct of foreign,

[22] 31 U.S.C. 5311*, Declaration of Purpose*, and 31 U.S.C. 5319, *Availability of Reports*

defense, and economic policies, as well as the protection of U.S. national interests from foreign security threats. Information collected from the BSA database may contain USP information. OIA personnel authorized to have access to USP information in the BSA database have a responsibility to protect that information in accordance with the MOU.

When asked about potential violations of the MOU, OIA officials stated that they were not aware of any instances of an OIA analyst violating the MOU and that FinCEN, as administrator of the database, had not alerted them of any suspicious BSA queries performed by OIA analysts. FinCEN employees responsible for administration of the BSA database said that, although they have not reviewed OIA analyst queries, they were not aware of any instances of OIA analysts violating the MOU.

Short-term Assignments Not Used to Circumvent BSA Information Safeguards
We did not find evidence to support that OIA permitted other IC elements to work at OIA for "short periods of time, sometimes for as little as a week," allowing them to receive unrestricted access to information on USP that they otherwise could not collect without strict oversight.

We identified IC employees at OIA who participated in the IC Civilian Joint Duty Assignment (JDA) Program. The JDA program allows employees to rotate to another IC element to gain a wider understanding of the mission and function of that element and to build collaborative networks.

Prior to commencement, the parameters of each JDA program rotation, including responsibilities and the length of the rotation, are documented in an agreement between the employing IC element and the gaining IC element. Depending on the parameters of the agreement between OIA and an IC employee's home agency, an employee may be granted access to Treasury systems. In some cases, participants of the JDA program are granted access to the BSA database. Before being granted access to the BSA database, employees on joint duty assignments must sign the BSA user agreement from FinCEN and receive FinCEN training on the system. The employee is then granted access to the entire BSA dataset. These requirements are identical to those of full-time OIA analysts.

Our non-statistical selection of 44 OIA BSA queries conducted during January 2017 through March 2017 included 10 queries made by OIA's JDA participants. We reviewed documents related to the queries and interviewed the program participants and their supervisors. We determined that the queries were conducted in support of OIA's mission. Based on their assignments at OIA, the

program participants were authorized to have access to Treasury systems and were specifically granted access to the BSA database through a user agreement with FinCEN. The JDA participants were employed for at least 12 months and not the "short period" alleged by the article. Access to the BSA database is not limited to Treasury and OIA employees. FinCEN also has a memorandum of understanding with six other IC elements to provide access to the BSA database.

Conclusion

We did not find evidence to substantiate the *BuzzFeed* claims that OIA analysts are (1) illegally collecting and retaining domestic financial information from FinCEN's BSA database, (2) contacting financial institutions to make inquiries about individual bank accounts and transactions involving U.S. citizens, or (3) violating the MOU with FinCEN. While OIA does not have USP procedures approved by the Attorney General, OIA's statutory authorities under the *Consolidated Appropriations Act of 2005* and EO 12333 permit OIA to collect, retain, and disseminate USP information until USP procedures are established.

We conducted our fieldwork for this audit report from February 2017 through December 2017. 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 Greg Sullivan, Audit Director, at (202) 927-5369.

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C.

UNDER SECRETARY

MEMORANDUM FOR ASSISTANT INSPECTOR GENERAL DEBORAH L. HARKER

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

MAR 29 2018

SUBJECT: Management Response to the Audit of the Office of Intelligence and Analysis' (OIA) Authorities and Actions Related to U.S. Persons' Financial Information

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) formal draft audit report on OIA's authorities and actions, particularly related to allegations that OIA "repeatedly and systematically violates domestic surveillance laws."

We are committed to using all of our authorities to combat threats to national security, within the bounds of the law and with all due respect for the rights of U.S. persons. I appreciate your office's careful and thorough review of the allegations.

Your audit concluded that the allegations were not supported and made thoughtful recommendations for improving OIA's activities. I concur with your recommendation that OIA finalize and submit for approval to the Attorney General its procedures for handling U.S. person information as required by Executive Order (E.O.) 12333. As you note, OIA and the Office of General Counsel (OGC) have been actively engaged with the U.S. Department of Justice (DOJ) and the Office of the Director of National Intelligence (ODNI) to finalize them. In February 2018, OIA provided DOJ and ODNI its latest draft USP Procedures for review, which were revised and streamlined to reflect other approved procedures. This submission of the revised draft represents an important step in obtaining Attorney General approval to finalize the Procedures.

I also concur with OIG's recommendation that OIA implement an appropriate compliance monitoring program in the interim before its USP Procedures are approved. As you know, OIA intelligence analysts comply with the requirements of Executive Order 12333 regarding the handling of U.S. person information, and as a matter of practice OGC reviews all proposed disseminations of U.S. person information. At my direction, OIA has already identified a senior official to serve as Oversight Coordinator, who will work with OGC to establish an appropriate compliance monitoring program during this interim period.

In addition, improving collaboration between OIA and FinCEN remains a top priority. I will ensure the implementation of OIA's USP Procedures and the continued appropriate access by TFI employees, including OIA and FinCEN, to the information necessary to support TFI's national security mission.

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

TFI Management Response to the report recommendations:

Recommendation 1: Management concurs with the recommendation. OIA has provided a revised draft of the USP Procedures to DOJ and ODNI for review and, ultimately, Attorney General approval.

Recommendation 2: Management concurs with the recommendation. Pending approval of the USP Procedures, OIA intelligence analysts handle U.S. person information in accordance with Executive Order 12333 and all disseminations of U.S. person information are reviewed by the Office of General Counsel (OGC). OIA has assigned an Oversight Coordinator to work with OGC on developing an appropriate compliance monitoring program in the interim before the USP Procedures are approved.