



DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

OFFICE OF
INSPECTOR GENERAL

January 10, 2018

OIG-CA-18-011

MEMORANDUM FOR DEPARTMENT OF DEFENSE
LEAD INSPECTOR GENERAL

FROM: Eileen Kao /s/
Acting Audit Director

SUBJECT: Operation Inherent Resolve - Summary of Work Performed by
the Department of the Treasury and Office of Inspector
General Related to Terrorist Financing, ISIS, and Anti-Money
Laundering

This summary provides an update to the Department of the Treasury (Treasury) programs to combat terrorist financing and specific examples of activities to disrupt the Islamic State of Iraq and Syria's (ISIS)¹ financing, and work performed by Treasury Office of Inspector General (OIG) to review these programs. These activities occurred subsequent to our October 2017 summary.

As previously discussed, Treasury has global terrorism authorities to target the activities of extremist groups, including ISIS. Treasury's Office of Terrorism and Financial Intelligence (TFI) disrupts the ability of terrorist organizations to fund their operations. Within TFI, the Office of Foreign Assets Control (OFAC) administers the U.S. foreign sanction programs and the Financial Crimes Enforcement Network (FinCEN) administers the Bank Secrecy Act (BSA).²

¹ Using ISIS instead of Islamic State of Iraq and the Levant (ISIL) to be consistent with the *Presidential Memorandum Plan to Defeat the Islamic State of Iraq and Syria* (January 28, 2017).

² The Currency and Foreign Transactions Reporting Act of 1970, commonly referred to as BSA, requires U.S. financial institutions to assist U.S. government agencies to detect and prevent money laundering. Specifically, the act requires financial institutions to keep records of cash purchases of negotiable instruments, file reports of cash transactions exceeding \$10,000 (daily aggregate amount), and report suspicious activity (SARs) that might signify money laundering, tax evasion, or other criminal activities. BSA is also referred to as the "anti-money laundering" (AML) law. Several AML acts, including provisions in Title III of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act), have been enacted to amend the BSA.

Treasury's Efforts to Combat Terrorism

The following notable events took place for Treasury this quarter:

- On October 25, 2017, pursuant to Executive Order (E.O.) 13224,³ Treasury designated eight individuals and one entity for acting for or on behalf of ISIS in Yemen (ISIS-Y), or al-Qa'ida in the Arabian Peninsula (AQAP), or both. This action was taken in partnership with the Kingdom of Saudi Arabia, as the co-chair of the recently established Terrorist Financing Targeting Center (TFTC),⁴ as well as all other TFTC member states: the Kingdom of Bahrain, the State of Kuwait, the Sultanate of Oman, the State of Qatar, and the United Arab Emirates. The following eight individuals and one entity were designated on October 25, 2017, for acting on behalf of ISIS-Y, AQAP, or both:

Adil Abduh Fari Uthman al-Dhubhani - As of early June 2016, Fari served with ISIS-Y in Taiz Governorate, Yemen, where his deputies, along with a large number of other ISIS-Y fighters, fought under the Sunni resistance. Fari also made payments to various Sunni militants and ISIS-Y affiliates in Taiz Governorate to secure continued support for ISIS-Y activities in Taiz in late October 2016. Recently, he has conducted fundraising for AQAP in his role as a military instructor.

Radwan Muhammad Husayn Ali Qanan – As of mid-2017, Qanan was a key ISIS-Y leader in Aden Governorate, Yemen, deputy field commander for ISIS-Y, and also a regional ISIS-Y field commander in southern Yemen. In late 2015, Qanan was one of the most senior officials within ISIS-Y and was operating in Aden, Yemen. He was considered to be one of the most dangerous members of ISIS-Y who intended to target and kidnap foreigners. As of early 2016, he was an ISIS-Y leader responsible for assassination operations in Yemen and also received funds from multiple sources in support of his role as a senior leader.

Khalid al-Marfadi – As of mid-2017, al-Marfadi was an ISIS-Y leader in charge of the movements of ISIS-Y fighters. He gave orders to the ISIS-Y commander of operations and was involved in an ISIS-Y assassination cell targeting Yemeni security forces located in southern Yemen. Between 2015 and 2016, al-Marfadi was the ISIS-Y leader of Yafa, Yemen, was involved in the recruitment of fighters from Yafa for ISIS-Y, and ran a training camp in Yafa. He was in charge of and prepared the vehicle-borne improvised explosive devices used by ISIS-Y. Al-Marfadi was one of the individuals responsible for, or had advance knowledge of the majority of ISIS-Y attacks in Yemen. He was considered to be

³ Executive Order 13224, *Blocking Property and Prohibiting Transactions With Persons Who Commit, Threaten To Commit, or Support Terrorism*

⁴ The TFTC was announced on May 21, 2017 to expand and strengthen the seven member states' cooperation to counter the financing of terrorism.

a decision-maker within ISIS-Y and conducted many functions on behalf of the group. He had approximately 50-60 ISIS-Y fighters working for him in Lahij Governorate.

Sayf Abdulrab Salem al-Hayashi – In mid-2015, al-Hayashi facilitated a weapons deal on behalf of ISIS-Y. Since 2016, he has been a weapons dealer and financier of AQAP.

Al Khayr Supermarket – Supermarket is owned or controlled by al-Hayashi.

Abu Sulayman al-Adani – As of early March 2017, al-Adani was the overall head of ISIS-Y, who was reportedly nominated in 2013 by Abu Bakr al-Baghdadi. The State Department designated al-Baghdadi as a Specially Designated Global Terrorist pursuant to E.O. 13224 on October 4, 2011.

Nashwan al-Wali al-Yafi'i – As of early 2017, al-Yafi'i was a finance leader of ISIS-Y. As of late 2016, he served as an ISIS-Y militant and chief financial officer for ISIS-Y in Yafi'i' District, Lahij Governorate, Yemen. Al-Yafi'i reported directly to ISIS-Y leader Khalid al-Marfadi, also designated on October 25, 2017.

Khalid Sa'id Ghabish al-Ubaydi – As of early 2017, Ghabish transported and secured shipments of smuggled weapons to ISIS-Y's secret locations and storage depots. As of late 2016, he was one of the most senior ISIS-Y members in al Ghaydah, al Mahrah Governorate, Yemen and was an ISIS-Y leader in Hadramawt Governorate, Yemen. In 2014, he recruited youths to support ISIS-Y.

Bilal Ali Muhammad al-Wafi- Wafi was assessed to be a key member of AQAP in Taiz Governorate.

- On December 5, 2017, Treasury designated Abdullah Ibrahim al-Faisal, a Jamaica-based Islamic cleric, as a Specially Designated Global Terrorist pursuant to E.O. 13224 for assisting in, sponsoring, or providing financial, material, or technological support for, or other services to or in support of ISIS. In 2016, Faisal assisted one of his followers in identifying a funding source to travel to ISIS-controlled territory. In addition to his actions for ISIS, Faisal has directly or indirectly influenced numerous terrorists.

Treasury OIG Products

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) – Issued October 30, 2017

This was the first of three reports we plan to issue related to our audit objective of assessing Treasury's Office of Intelligence and Analysis (OIA) progress in meeting its statutory responsibilities. 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 that OIA initiated a mass revocation of FinCEN's intelligence community public key infrastructure (IC PKI) certificates that prevented FinCEN employees from effectively responding to law enforcement requests on the London and Manchester terrorist attacks. 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 TFI and the White House regarding Venezuela.⁵

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. However, 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.

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 requests related to Venezuela.

⁵ 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.

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.

We recommended 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.

Financial Institutions Used FinCEN Guidance Designed To Avoid Duplicate Filing of Reports With OFAC and FinCEN, but BSA Data Users Did Not Have Access to All Data (OIG-18-032) – Issued December 19, 2017

This report presents the results of our audit of OFAC and FinCEN's sharing of blocked transaction reports for suspicious activity reporting. Our audit objectives were to determine (1) the extent to which financial institutions have availed themselves of FinCEN's 2004 guidance to avoid duplicative reporting and (2) whether controls are in place to ensure blocked transaction information filed with OFAC is made available to BSA data users through FinCEN's BSA database.

OFAC administers and enforces economic and trade sanctions based on U.S. foreign policy goals. A major component of these sanctions, the Specially Designated Nationals and Blocked Persons List (referred to as the SDN list), contains the names of individuals, government entities, and companies with which U.S. businesses and citizens are prohibited from engaging in trade under certain OFAC programs, including, among others, Specially Designated Global Terrorists, Narcotics Traffickers, and Narcotics Trafficker Kingpins as well as Foreign Terrorist Organizations. Financial institutions are required to block transactions of individuals or entities subject to U.S. sanctions and report the transactions to OFAC. The blocked transaction data is used by OFAC for enforcement purposes, in making licensing determinations, and in reporting to Congress.

FinCEN administers the BSA, which established the framework to combat criminal use of the financial system. The BSA requires financial institutions to report certain

financial transactions made by their customers. FinCEN oversees the management, processing, storage, and dissemination of BSA data, which are collected through Suspicious Activity Reports (SAR) filed by financial institutions. FinCEN, law enforcement agencies, counter-terrorism agencies, financial regulators, and the intelligence community (collectively known as BSA data users) use these data to identify trends and develop intelligence information on money laundering and terrorist financing.

In 2003, FinCEN instructed financial institutions to file SARs for any verified match with an entity on OFAC's SDN list. In December 2004 FinCEN issued interpretive guidance, *Interpretation of Suspicious Activity Reporting Requirements to Permit the Unitary Filing of Suspicious Activity and Blocking Reports* (2004 guidance), to alleviate the burden of filing duplicative reports with both OFAC and FinCEN.

We concluded that financial institutions, with few exceptions, avoided duplicative reporting consistent with FinCEN's 2004 guidance. However, controls were not in place to ensure blocked transaction information filed with OFAC was made available to BSA data users through FinCEN's BSA database. Specifically, FinCEN did not reconcile reports in its system to ensure required information was available to BSA data users.

Because periodic reconciliations were not performed by FinCEN, FinCEN was unaware that it did not upload to the BSA database information related to approximately 3,220 (88 percent) of the 3,653 blocked transaction reports received from OFAC between January 2010 and December 2012 because of information technology related problems. Accordingly, we recommended that the Director of FinCEN, in collaboration with the Director of OFAC, reconcile the blocked transaction data to ensure FinCEN makes all data available to BSA data users.

We noted two other matters of concern from our review of blocking reports and SARs. First, the 2004 guidance does not consider OFAC sanctions programs implemented after the guidance was issued. Accordingly, we recommended that the Director of FinCEN, in collaboration with the Director of OFAC, review the 2004 guidance and information sharing agreement based on changes to sanctions programs and update accordingly.

As another matter of concern, we identified 387 SARs describing transactions processed by the filing institutions that potentially violated an OFAC sanctions program. We referred these potential violations to OFAC and the appropriate regulator for consideration of enforcement action.

For this quarter's summary, we also used information provided in previous quarters' summaries, testimonies, and press releases. For reference, we are providing copies

of the following documents (as separate attachments) used to prepare this summary:

- October 25, 2017, Treasury Press Release, *Treasury and Terrorist Financing Targeting Center Partners Issue First Joint Sanctions Against Key Terrorists and Supporters*
- December 5, 2017, Treasury Press Release, *Treasury Sanctions Jamaica-based ISIS Recruiter for Terror Support*
- Treasury OIG Report OIG-18-006 (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*
- Treasury OIG Report OIG-18-032 (December 19, 2017) *Financial Institutions Used FinCEN Guidance Designed To Avoid Duplicate Filing of Reports With OFAC and FinCEN, but BSA Data Users Did Not Have Access to All Data*