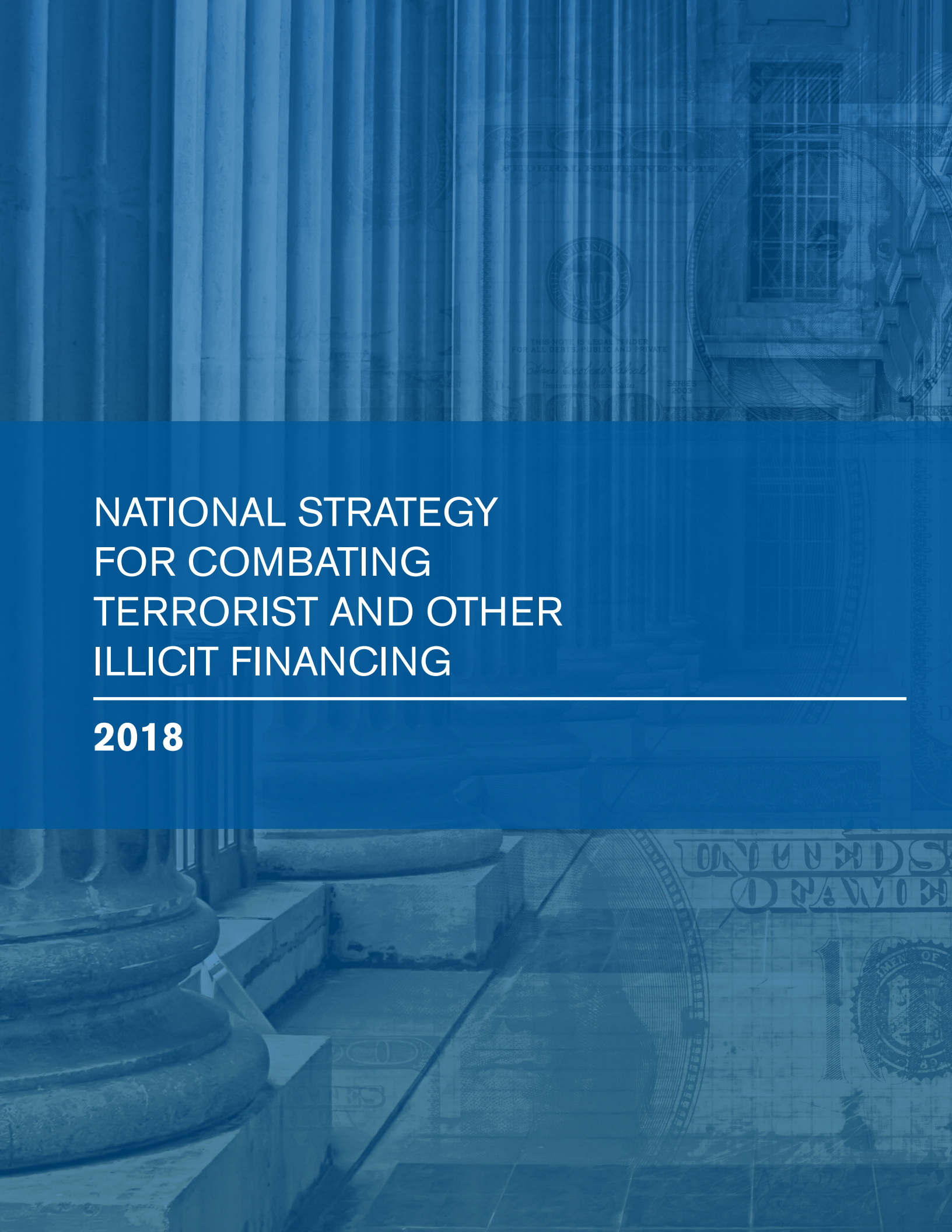


NATIONAL STRATEGY FOR COMBATING TERRORIST AND OTHER ILLICIT FINANCING

2018

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The United States has the world's largest financial system. On any given day, U.S. financial institutions process trillions of dollars of transactions originating both domestically and from all across the globe. The stability and transparency of the U.S. financial system make it an attractive destination for trade and investment, but also make the United States an attractive target for illicit finance activity. This activity can include fundraising by terrorist groups and their supporters and facilitators; financial transactions that facilitate weapons of mass destruction (WMD) proliferators; and money laundering by drug-trafficking organizations, organized crime groups, and perpetrators of fraud. To address the risk of these activities, the U.S. government has developed a robust anti-money laundering and countering the financing of terrorism (AML/CFT) framework built upon sound laws and regulations, effective implementation, and balanced enforcement.

This *2018 National Strategy for Combating Terrorist and Other Illicit Financing* (*Illicit Finance Strategy*) was prepared by the Office of Terrorism and Financial Intelligence (TFI) of the Department of the Treasury (Treasury) in consultation with the many agencies, bureaus, and departments of the federal government that also have roles in combating illicit finance. This *Illicit Finance Strategy* fulfills the requirements of Sections 261 and 262 of the Countering America's Adversaries Through Sanctions Act (Public Law No. 115-44) (CAATSA).[1] The *Illicit Finance Strategy* describes and assesses current U.S. government efforts to combat illicit finance[2] threats and risks and identifies priorities, objectives, and potential areas for future improvement. It also highlights U.S. interagency and intergovernmental efforts to combat illicit finance domestically and internationally, including enforcement measures that include sanctions, prosecutions, and asset forfeiture, as well as improvements in information sharing mechanisms and updated guidance to aid financial institutions in detecting and combating illicit finance threats.

ILLICIT FINANCE THREATS AND RISKS

The *Illicit Finance Strategy* is underpinned by three separate risk assessments coordinated by TFI, in collaboration with law enforcement, financial supervisors, and other relevant U.S. government agencies. The 2015 assessments of terrorist financing and money laundering risks were updated for this strategy and an assessment of proliferation financing risk was formally conducted for the first time in connection with developing this document.

The *2018 Terrorist Financing Risk Assessment* identifies the Islamic State of Iraq and Syria (ISIS) and its regional affiliates, Al-Qaida (AQ) and its regional affiliates, Al-Shabaab, and Hizballah

1. Public Law 115-44, August 2, 2017, directed the President, acting through the Secretary of the Treasury in consultation with the other relevant offices and departments of government, to develop a national strategy for combating the financing of terrorism and related forms of illicit finance.

2. Section 281(5) of CAATSA defines "illicit finance" as the financing of terrorism, narcotics trafficking, or proliferation, money laundering, or other forms of illicit financing domestically or internationally, as defined by the President.

as groups posing the most significant terrorist financing threat to the United States and U.S. financial system. In terms of global terrorist financing threats, Iran's Islamic Revolutionary Guard Corps-Qods Force (IRGC-QF) continues to provide hundreds of millions of dollars a year to Iran's terrorist proxies, such as Hizballah, as well as to the Assad regime in Syria. U.S.-based financial activity associated with these groups primarily involves raising and transmitting funds to supporters of these groups located outside of the United States. Banks and money services businesses (MSBs) are the most commonly used channels for moving these funds abroad. The primary risk for these U.S. banks and MSBs, which typically maintain robust AML/CFT compliance programs, results from challenges in distinguishing terrorism-related financial transactions from licit activity, as well as weak implementation by foreign financial institutions of key AML/CFT measures.

The *2018 Proliferation Financing Risk Assessment* finds that networks acting clandestinely to support state-sponsored WMD programs pose the most persistent threat to the U.S. financial system. These networks vary widely in size and sophistication, but all employ tradecraft meant to obfuscate the source and/or purpose of funds and to mask the underlying illicit activity that generates these funds in support of their respective weapons programs. Such networks often work on behalf of entities sanctioned by the United States or for countries on which the United States imposes stringent export controls with respect to military or dual-use technologies. These networks seek to exploit vulnerabilities in the global financial system. Their activities most frequently intersect with the U.S. financial system through attempts to finance the direct procurement of controlled U.S.-origin goods or technology, or through attempts to transact in U.S. dollars, regardless of the origin of the underlying goods, many of which do not have an obvious or direct link to WMD. While much of this activity takes place in foreign jurisdictions and involves non-U.S. persons, given the importance of the U.S. dollar and financial system to international trade and finance, these financial transactions are often processed through U.S. banks, which generally may be unwitting and can encounter difficulties in identifying the underlying illicit actors given the information available to them.

The *2018 Money Laundering Risk Assessment* identifies the most significant money laundering risks in the United States, including the misuse of cash; complicit merchants, professionals, and financial services employees; and lax compliance at some financial institutions. The United States continues to estimate that domestic financial crime, excluding tax evasion, generates approximately $300 billion of proceeds for potential laundering. Fraud, which encompasses a variety of crimes, including fraud against government programs, financial institutions, and individuals, is estimated to generate more illicit proceeds than any other category of crime. Drug trafficking is estimated to be the second largest proceeds-generating crime. Professional money launderers serve transnational criminal organizations that engage in all manner of criminal activity. They also often operate independently of the criminals they serve, rendering them dangerous criminal networks in their own right.

Emerging illicit finance risks include an increase in cybercrime and cyber-enabled crime, which encompass a variety of illicit activity. Cyber criminals' use of money mules complicates law enforcement investigations by placing throughout the ground level of the money laundering

activity individuals who know little or nothing of the underlying predicate activity and who may in fact be victims of crime themselves, unaware that they are being exploited.

Virtual currencies, in addition to being the preferred mechanism for buying illicit drugs and other illicit goods online and for paying the perpetrators of ransomware attacks, are emerging as a money laundering vehicle. For example, global money laundering syndicates are offering to move illicit proceeds into and through virtual currencies as another way to layer transactions in order to hide the origin of dirty money. Following the money trail in countries that do not impose effective AML/CFT requirements on virtual currency exchangers and administrators presents a significant challenge for U.S. law enforcement.

GOALS, OBJECTIVES, AND PRIORITIES

A great strength of the U.S. AML/CFT framework is that many departments and agencies each play a role in preventing, investigating, prosecuting, and recovering illicit proceeds related to terrorist and criminal actors. Combating illicit finance is integrated into each agency's strategic goals to enhance national security and counter the threat of terrorism. This strategy describes these lines of effort so that future iterations of the *Illicit Finance Strategy* can build upon them.

- Department of the Treasury: TFI[3] identifies, disrupts, and dismantles priority threats to, and identifies and reduces vulnerabilities in, the U.S. and international financial systems to prevent abuse by illicit actors. TFI's core mission focuses on countering illicit finance by utilizing Treasury's unique expertise, access to financial intelligence, and authorities, including financial sanctions and regulatory enforcement actions, to disrupt and disable terrorists, criminals, WMD proliferators, and other national security threats to the United States and to protect the U.S. and international financial systems from misuse. The Internal Revenue Service-Criminal Investigations Division (IRS-CI) investigates complex financial crimes associated with tax evasion, money laundering, and narcotics.
- Department of Justice (DOJ): DOJ utilizes the resources and expertise of various components, including the National Security Division, Money Laundering and Asset Recovery Section (MLARS), the U.S. Attorney's Offices, Federal Bureau of Investigation (FBI), Drug Enforcement Administration (DEA), and other prosecution and investigating components and agencies, to disrupt and prosecute terrorists, weapons proliferators, organized crime and drug networks, money launderers, and white collar criminals.
- Department of Homeland Security (DHS): U.S. Immigration and Customs Enforcement (ICE) focuses on protecting the homeland through counter-proliferation investigations; preventing terrorist organizations' efforts to move weapons, money, and people across international borders; and fighting financial crime. ICE seeks to prevent such activity

3. Treasury's Office of Terrorism and Financial Intelligence includes the Financial Crimes Enforcement Network (FinCEN), Office of Foreign Assets Control (OFAC), Office of Terrorist Financing and Financial Crimes (TFFC), the Office of Intelligence and Analysis (OIA), and the Treasury Executive Office for Asset Forfeiture (TEOAF).

at the border via Customs and Border Protection efforts and investigations conducted by Homeland Security Investigations. Further, U.S. Secret Service maintains a role in investigating financial crime to safeguard the U.S. currency and payment systems.

- Department of State: Pursues diplomatic solutions to proliferation challenges, terrorism, and transnational organized crime, and has the ability to impose certain financial and economic sanctions.
- Department of Defense: Supports counter-threat finance efforts with dedicated counter-threat finance teams.
- Supervisory Authorities: The Federal functional regulators[4] supervise, examine, and enforce compliance with applicable AML/CFT laws and regulations.

INTERAGENCY COORDINATION AND INTERGOVERNMENTAL COOPERATION

These lines of effort are supported by continued improvements in interagency cooperation and coordination, including information sharing between intelligence and law enforcement agencies, in support of a whole-of-government approach to combating domestic and international illicit finance.

As part of broader U.S. efforts to prevent terrorism and WMD proliferation, U.S. authorities have developed robust interagency processes and organizations to employ most effectively the full range of tools and authorities available to identify and act against terrorist financing and proliferation financing. In the case of terrorist financing, this includes, for example, coordination and information sharing by law enforcement and intelligence personnel at the National Counterterrorism Center and at FBI-led Joint Terrorism Task Forces, as well as the efforts of TFI and other interagency partners that collaborate through counterterrorism-focused interagency working groups. Similar coordination exists with respect to combating proliferation financing, with TFI, the FBI's Counterproliferation Center, the Department of Commerce's Bureau of Industry and Security, the Department of Homeland Security's Export Enforcement Coordination Center, and the National Counterproliferation Center helping to facilitate interagency cooperation in detecting and combating proliferation financing.

Long-standing interagency efforts to combat money laundering include DOJ's Organized Crime Drug Enforcement Task Forces (OCDETF), which funds and coordinates law enforcement task forces targeting high-priority drug trafficking and money laundering organizations. MLARS leads DOJ's asset forfeiture and AML enforcement efforts by prosecuting and coordinating complex, sensitive, multi-district, and international money laundering and asset forfeiture investigations and cases.

---

4. This includes the Commodity Futures Trading Commission (CFTC); the Board of Governors of the Federal Reserve System (FRB); the Federal Deposit Insurance Corporation (FDIC); the National Credit Union Administration (NCUA); the Office of the Comptroller of the Currency (OCC); and the Securities and Exchange Commission (SEC).

Cash seizure data is collected and analyzed by the National Bulk Cash Smuggling Center (BCSC) to provide tactical intelligence and expertise in support of investigations into bulk cash smuggling, while the El Paso Intelligence Center collects and analyzes cash seizure data from interdictions along the southwestern U.S. border coordinating with BCSC. This work is further supported by Suspicious Activity Report (SAR) Review Teams in all 94 federal judicial districts. SAR Review teams are frequently led by Internal Revenue Service-Criminal Investigations and include all federal law enforcement agencies that investigate financial crimes.

Regulatory and supervisory authorities also share information and cooperate in support of efforts to combat illicit finance. The Bank Secrecy Act Advisory Group (BSAAG) serves as a primary forum to facilitate the exchange of AML-related ideas and information among the federal government and industry. The Federal Financial Institutions Examination Council Bank Secrecy Act/Anti-Money Laundering (BSA/AML) Working Group coordinates communications among financial regulators with respect to BSA/AML policy matters and training.

The United States also engages in robust bilateral and multilateral international engagement to encourage other jurisdictions to establish and improve AML/CFT regimes in line with international standards to promote a level playing field around the world. In coordination with counterparts across the government, Treasury advances this strategic objective primarily through the Financial Action Task Force (FATF), the multilateral body that sets international standards for AML/CFT safeguards, and works for their adoption and implementation by jurisdictions around the world.

ENFORCEMENT AND TARGETED ACTIONS

The U.S. has been successfully combating illicit finance using a broad range of powerful tools, including sanctions, AML measures, enforcement actions, foreign engagement, intelligence and analysis, and private sector partnerships, among others. For example, at the time of publication, OFAC has issued more than 800 designations under its counter terrorism sanctions (Executive Order [E.O.] 13224); designated more than 700 entities for their support to, or facilitation of, proliferation of WMD (E.O. 13382); designated 9 Transnational Criminal Organizations (TCOs) and more than 200 targets related to those TCOs (E.O. 13581); and identified 118 significant foreign narcotics traffickers ("drug kingpins") for sanctions and designated more than 2,000 companies and individuals in dozens of sanctions investigations related to those drug kingpins around the world (Kingpin Act).

Regarding money laundering prosecutions, DOJ charged, on average, 2,256 defendants with money laundering annually between FY 2015 and FY 2017. These included several large-scale, precedent-setting prosecutions in recent years. The first nationwide undercover operation to target vendors of illicit goods on clandestine e-commerce marketplaces, referred to as the Darknet, led to 90 active investigations around the country and the arrest and impending prosecution of more than 35 Darknet vendors. In 2018, for example, 21 individuals were sentenced to terms of imprisonment of up to 20 years for their part in an India-based fraud and money laundering conspiracy that defrauded thousands of U.S. residents out of hundreds

of millions of dollars in various telephone fraud schemes. The largest 2017 health care fraud enforcement action charged 412 defendants, including 115 doctors, nurses and other licensed medical professionals, for their alleged participation in health care fraud and money laundering schemes involving approximately $1.3 billion in false billings.

Information Sharing And Guidance

The Bank Secrecy Act (BSA) establishes requirements for recordkeeping and reporting by private individuals, banks, and other financial institutions, all of which help authorities identify the source, volume, and movement of funds into and out of the United States or processed by financial institutions. U.S. financial institutions subject to the BSA play a critical role in detecting a wide variety of illicit finance activities and assisting U.S. authorities in combating money laundering and terrorist financing threats. The number of financial institutions sharing information with each other for the purpose of reporting suspicious activity to FinCEN (the bureau of Treasury authorized to receive BSA reports) has been increasing, along with the number of Suspicious Activity Reports (SARs) filed referencing shared information.[5]

Under Section 314 of the USA PATRIOT Act, FinCEN—on its own behalf, on behalf of other Treasury components, or assisting federal, state, local, and foreign law enforcement agencies—can require financial institutions to identify accounts and transactions of persons that may be involved in terrorism or significant money laundering. FinCEN has used this authority to organize and host two-way information sharing discussions with financial institutions and recently formalized such outreach in the form of a new public-private information sharing program called FinCEN Exchange, which brings together law enforcement, FinCEN, and different types of financial institutions from across the country to share information that can help identify vulnerabilities and disrupt money laundering, terrorist financing, proliferation financing, and other financial crimes.

Treasury, often in coordination with federal financial regulators, state agencies, and law enforcement, issues guidance to financial institutions and other relevant nonfinancial businesses regarding regulatory requirements and expectations under the BSA, helping support a high-quality reporting regime. These clarifications frequently apply existing rules or guidance to particular facts and circumstances; provide new information and guidance on recent regulatory or reporting changes; and address gaps and vulnerabilities identified through governmental cooperation.

Treasury also undertakes public-private engagement to understand new business models, and identify and address obstacles to the development and adoption of responsible products and services, including those designed to enhance compliance. Innovations in financial technology (FinTech) and technology for regulatory compliance (RegTech) can potentially strengthen AML/CFT compliance and reduce costs. U.S. policymakers and regulators support the development of responsible FinTech and RegTech applications that further policy objectives, including protecting

5. FinCEN, *314(b) References in Suspicious Activity Reports (SARs) Suggest Increased Information Sharing Among Financial Institutions*, available at https://www.fincen.gov/sites/default/files/shared/314bInfographic.pdf.

the integrity of the financial system with effective AML/CFT controls and promoting financial inclusion.

Conclusion

Illicit transactions are often hard to distinguish from legitimate day-to-day transactional activity. This challenge extends to activity by individual terrorist supporters executing funds transfers from their personal accounts; WMD procurement networks that resemble legitimate trade in what are often highly technical industries; and professional money launderers and complicit insiders. As this *Illicit Finance Strategy* describes, U.S. authorities are working to address this challenge using the full range of tools and authorities, including regular engagement and information sharing with U.S. financial institutions. Emerging and continuing risks that require further action include the growing misuse of virtual currencies, exacerbated by a lack of regulation and supervision of virtual currency providers in many foreign jurisdictions; complicit insiders at financial institutions facilitating sanctions evasion and money laundering; complicit merchants facilitating money laundering; and the recruitment of unwitting and unquestioning individuals to facilitate money laundering.

A strong, current, and efficient AML/CFT framework aids in keeping illicit actors out of the financial system and allows U.S. authorities to track and target those who nonetheless slip through. The United States pioneered regulations to combat money laundering with the BSA in 1970, and since that time the Treasury Department has worked to ensure that U.S. regulations evolve with financial threats. For example, in May 2018, financial regulators started examining against and enforcing Treasury's 2016 Customer Due Diligence rule that, among other things, adds a new requirement for covered financial institutions to identify and verify the beneficial ownership information when companies open accounts. This rule is a significant step in improving financial transparency and preventing criminals and terrorists from misusing companies to disguise their illicit activities and launder their ill-gotten gains.

More broadly, Treasury and its interagency partners are currently working to identify ways to improve the effectiveness of the AML/CFT safeguards in place. This includes a Treasury and the Federal Banking Agencies Working Group on BSA/AML that is exploring ways to modernizing the regulatory regime in ways that support efforts by financial institutions to devote their resources toward addressing the areas of highest risk for illicit finance activities. There are also efforts already under way within the BSAAG, which is chaired by FinCEN and is comprised of members from financial institutions, trade groups, and law enforcement, to obtain feedback on opportunities to improve the BSA framework. Treasury is also conducting outreach with financial institutions and businesses in the FinTech and regulatory RegTech sector in order to understand and assess the potential of technological innovations coming to market.

INTRODUCTION

The *Illicit Finance Strategy* is a report to Congress mandated by Sections 261 and 262 of the Countering America's Adversaries Through Sanctions Act (Public Law No. 115-44) (CAATSA). The content of the report is specified under Section 262 of CAATSA. The *Illicit Finance Strategy* was prepared by the Office of Terrorism and Financial Intelligence (TFI) of the Department of the Treasury (Treasury) in consultation with the many agencies, bureaus, and departments of the federal government that have roles in combating illicit finance.[6] TFI's core mission is to counter illicit finance by marshaling Treasury's intelligence, enforcement, and national security functions to combat a variety of national security threats and safeguard the financial system from abuse.

The *Illicit Finance Strategy* is consistent with the President's *National Security Strategy* (NSS), which prioritizes combating terrorism, the proliferation of weapons of mass destruction, and transnational criminal organizations, as well as supporting several of the priority actions identified in the President's *National Strategy for Counterterrorism*.[7] The intelligence, law enforcement, and policy offices of government dedicated to combating national security threats play a critical role in deterring and countering the associated illicit financing. Federal functional regulators also work to deter illicit finance in order to ensure a safe and sound U.S. financial system.

This *Illicit Finance Strategy* addresses the statutorily required topics under the following headings: threats; illicit finance risks; emerging illicit finance risks; enforcement efforts and targeted actions; interagency coordination and intergovernmental cooperation; information sharing and guidance; and technology enhancements. Priority initiatives are included in the various sections, and a stocktaking of goals and objectives drawn from strategic planning and budget documents is included as an appendix. A separate appendix provides agency budget allocations of selected programs aimed at combating illicit finance. The information on illicit finance threats and risks and corresponding mitigation measures in the *Illicit Finance Strategy* is drawn from risk assessments coordinated by TFI with broad interagency participation. TFI coordinated updates to the 2015 national terrorist financing and money laundering risk assessments,[8] and worked with the interagency to produce the first-ever *National Proliferation Financing Risk Assessment* (NPFRA).

Much of the strategic planning and performance target data in the *Illicit Finance Strategy* is drawn from relevant agencies' reports prepared in accordance with the Government Performance

---

6. Section 281(5) of CAATSA defines "illicit finance" as the financing of terrorism, narcotics trafficking, or proliferation, money laundering, or other forms of illicit financing domestically or internationally, as defined by the President.

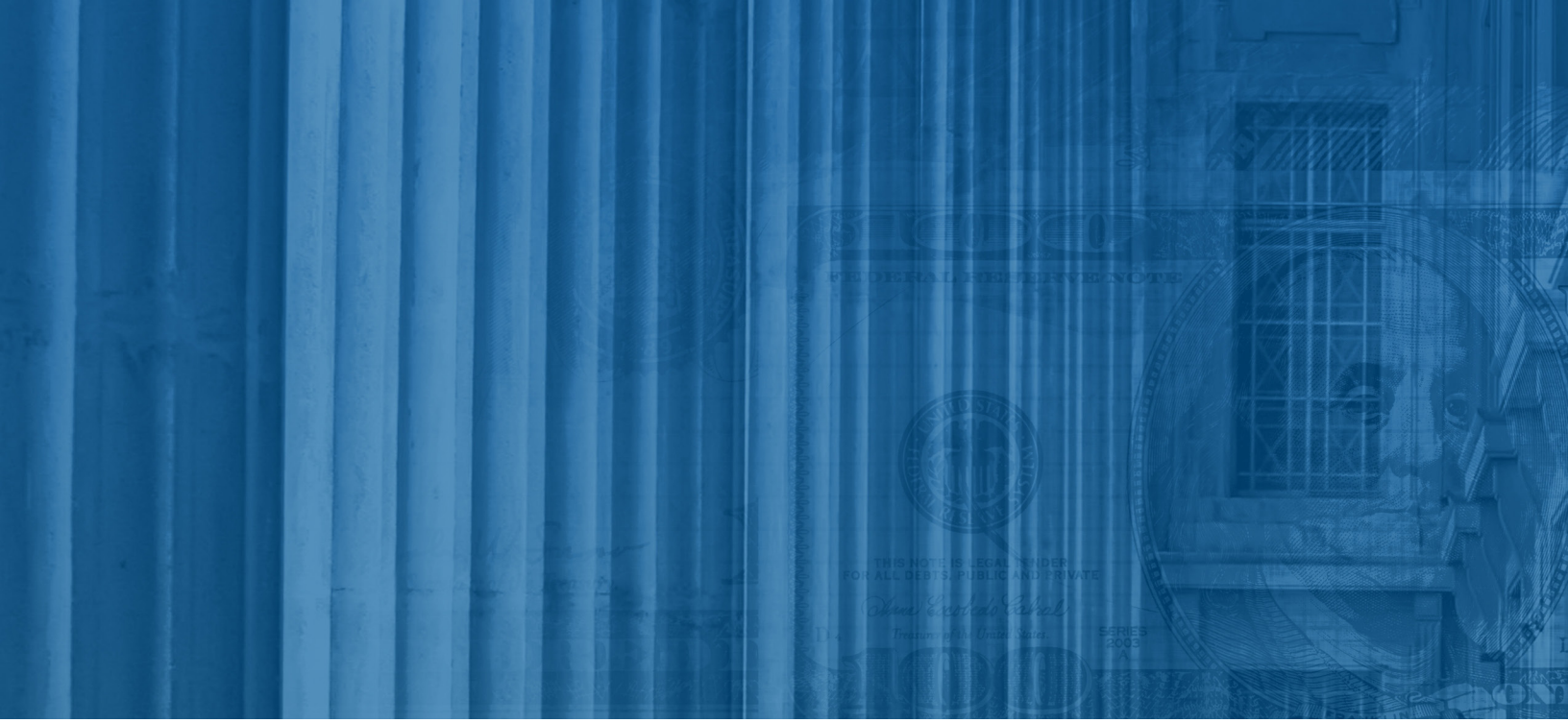
7. The White House, The White House, National Security Strategy, December 2017; *National Strategy for Counterterrorism*, October 2018, available at https://www.whitehouse.gov/wp-content/uploads/2018/10/NSCT.pdf.

8. The 2015 National Money Laundering Risk Assessment (NMLRA) is available at https://www.treasury.gov/resource-center/terrorist-illicit-finance/Documents/National%20Money%20Laundering%20Risk%20Assessment%20%E2%80%93%2006-12-2015.pdf; the 2015 National Terrorist Financing Risk Assessment (NTFRA) is available at https://www.treasury.gov/resource-center/terrorist-illicit-finance/Documents/National%20Terrorist%20Financing%20Risk%20Assessment%20%E2%80%93%2006-12-2015.pdf.

and Results Modernization Act (GPRA). Under the GPRA, each agency is required to develop a five-year strategic plan outlining its mission, long-term goals for major functions, performance measures, and reporting results. The strategic plan is updated every three years. In addition to its strategic plan, each agency submits an annual performance report to the Office of Management and Budget.

The Illicit Finance Funding Allocations for Select Programs extrapolates from the President's annual budget and agency justifications submitted to Congress to reach a rough approximation of what is spent combating illicit finance. Given that many departments and agencies do not separately track budget data related to illicit finance, there are challenges with identifying illicit finance-related funding for most programs. Other challenges stem from the nature of various budget presentations, and operational realities and uncertainties.

The *Illicit Finance Strategy* describes the strengths of U.S. counter-illicit finance efforts, including the robust U.S. anti-money laundering and countering the financing of terrorism (AML/CFT) framework, and identifies areas where there may be opportunity for improvement. U.S. financial institutions subject to the Bank Secrecy Act (BSA) play a critical role in that framework, detecting a wide variety of illicit finance and assisting U.S. authorities in combating those threats. There may be opportunities to leverage new technologies and broader information sharing arrangements among the private sector to improve both public and private sector effectiveness while reducing cost and burden. New payment technologies are a growing concern, particularly virtual currencies and associated services that enhance anonymity. Although U.S. regulators have moved quickly to apply domestic AML controls to this burgeoning area, many other countries have not taken similar steps. Safeguarding the U.S. financial system requires robust bilateral and multilateral engagement, as well as effective domestic policies and procedures, to urge other countries to implement and maintain similar practices in line with global standards.



SECTION 1.
THREATS

The greatest transnational threats to the United States as identified in the President's NSS[9] include jihadist terrorists; hostile state and nonstate actors who are trying to acquire nuclear, chemical, radiological, and biological weapons; and transnational criminal organizations (TCOs). The NSS states that these threats will be targeted at their source, before they reach the borders of the United States or harm the American people. U.S. authorities take a similar approach whenever possible in combating those who finance terrorism and the proliferation of weapons of mass destruction (WMD), and provide money laundering services essential to TCOs, while recognizing that each area presents unique challenges that must be taken into account. The crimes in which TCOs are engaged, including corruption, drug trafficking, fraud, extortion, human smuggling, and human trafficking, are also perpetrated by domestic criminals who misuse the U.S. financial system to launder their illicit proceeds.

TERRORISM[10]

Terrorist groups designated by the United States as Foreign Terrorist Organizations (FTOs) include the Islamic State of Iraq and Syria (ISIS) and its regional affiliates, Al-Qaida (AQ) and its regional affiliates, Al-Shabaab, the Al-Nusrah Front (ANF), Hizballah, and Hamas, pose a continuing terrorist threat to U.S. interests and partners worldwide.[11] The U.S. intelligence community assess that many of these groups are still intent on attacking the U.S. homeland and U.S. interests overseas, but their attacks will be most frequent in or near conflict zones or against enemies that are more easily accessible.[12]

U.S. authorities assess that ISIS poses a continuing terrorist threat to the United States and its allies because of its ideological appeal, media presence, its global enterprise of almost two dozen affiliates and networks, and proven ability to direct and inspire attacks.[13] Moving forward, the U.S. intelligence community believes that ISIS will focus on regrouping in Iraq and Syria, enhancing its global presence, championing its cause, planning international attacks, and encouraging its members and sympathizers to attack in their home countries.[14] ISIS derives most of its revenue from the extortion and taxation of civilian populations and economies in Iraq and Syria, and the smuggling and sale of oil and oil products, but does receive limited financial support from within the United States.

---

9. The White House, *National Security Strategy* – December 2017, available at https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf.
10. See the 2018 NTFRA for a complete discussion of terrorist financing threats.
11. Several regional affiliates of ISIS and AQ have been separately designated as FTOs, including ISIS Sinai Province, ISIS-Libya, ISIS-Khorasan, ISIS-Philippines, ISIS-Bangladesh, ISIS-West Africa, AQ in the Arabian Peninsula (AQAP), and AQ in the Indian Subcontinent.
12. Daniel Coats, Director of National Intelligence, "Worldwide Threat Assessment of the United States Intelligence Community," February 13, 2018 ("Worldwide Threat Assessment"), available at https://www.dni.gov/files/documents/Newsroom/Testimonies/2018-ATA---Unclassified-SSCI.pdf.
13. Christopher Wray, Director, Federal Bureau of Investigation, Testimony before the Senate Committee on Homeland Security and Governmental Affairs, "Current Threats to the Homeland," September 27, 2017, available at https://www.fbi.gov/news/testimony/current-threats-to-the-homeland.
14. Daniel Coats, Director of National Intelligence, "Worldwide Threat Assessment of the United States Intelligence Community," February 13, 2018 ("Worldwide Threat Assessment"), available at https://www.dni.gov/files/documents/Newsroom/Testimonies/2018-ATA---Unclassified-SSCI.pdf.

Hizballah continues to present a significant terrorism threat to the United States and U.S. interests globally.[15] It has demonstrated its intent to foment regional instability by deploying thousands of fighters to Syria and by providing weapons, tactics, and direction to militant and terrorist groups. Hizballah probably also emphasizes its capability to attack U.S., Israeli, and Saudi Arabian interests.[16] Hizballah receives the majority of its funding, upwards of $700 million a year, from Iran, which is the world's foremost state sponsor of terrorism.[17] In addition to funding from Iran, Hizballah receives money from a global network of supporters and businesses.[18] In terms of global terrorist financing threats[19], Iran's Islamic Revolutionary Guard Corps-Qods Force (IRGC-QF) continues to provide hundreds of millions of dollars a year to Iran's terrorist proxies, such as Hizballah and the Assad regime in Syria.

AQ and its regional affiliates, including AQ in the Arabian Peninsula (AQAP) as well as other terrorist groups associated with AQ, such as ANF, also continue to pose a threat to the United States and its allies.[20] The primary threat to U.S. and Western interests from AQ and its regional affiliates will be in or near affiliates' operating areas. Not all affiliates will have the intent and capability to pursue or inspire attacks in the US homeland or elsewhere in the West.[21]

While AQ and its regional affiliates generate their funding from individual fundraisers in Gulf countries and supporters throughout the world, they also continue to seek funds and other resources from U.S.-based supporters.

Other terrorist groups such as Hamas, the Taliban, and Islamic Jihad Union also seek to raise funds in the United States. While a significant and difficult to detect terrorism threat, attacks by radicalized individuals in the United States are less of a terrorist financing threat because this activity is typically self-funded.

WEAPONS OF MASS DESTRUCTION PROLIFERATION[22]

The United States intelligence community identifies the efforts of China, Iran, North Korea, Pakistan, Russia, and Syria to modernize, develop, or acquire WMD, their delivery systems, or their underlying technologies as a major threat to the security of the United States, its deployed

15. *Id,* p. 10.
16. *Id*.
17. Sigal Mandelker, Under Secretary for Terrorism and Financial Intelligence, Speech before the Foundation for the Defense of Democracies, June 5, 2018, available at https://home.treasury.gov/news/press-releases/sm0406.
18. Press Release, Treasury, "Treasury Targets Hizballah Financial Network in Africa and the Middle East," February 2, 2018, available at https://home.treasury.gov/news/press-releases/sm0278.
19. As noted in the methodology of the 2018 NTFRA, the focus is on threats to the United States and U.S. financial system, not on global terrorist financing threats. Since 1996, the U.S. has maintained a robust sanctions program and broad primary embargo against Iran, which has made it difficult for Iranian-linked entities to conduct TF-related activities with a U.S. nexus.
20. Worldwide Threat Assessment, pp. 9–10.
21. *Id,* p. 10.
22. See the NPFRA, which includes a discussion of PF threats.

troops, and its allies.[23] In the proliferation financing (PF) context, proliferation support networks acting clandestinely to support state-sponsored weapons programs such as these pose the most persistent threat to the U.S. financial system.

These networks vary widely in size and sophistication, but all employ tradecraft meant to obfuscate the source and/or purpose of funds and to mask the underlying illicit activity. They seek to exploit vulnerabilities in the global financial system and their activities most frequently intersect with the U.S. financial system in two principal ways, (1) attempts to acquire sensitive or controlled technologies from U.S. firms, which almost always involve the use of U.S. financial institutions and transactions denominated in U.S. dollars, and (2) attempts to move or transfer funds denominated in U.S. dollars, which generally results in U.S. financial institutions having to "clear" or facilitate these transactions whether or not the final "destination" of those funds is within the United States.

For example, North Korea[24] has sought to acquire U.S.-origin materials or technology that would directly advance its WMD and ballistic missile development, including specialized industrial machinery used in the metallurgic process to fabricate these weapons.[25] However, North Korean PF networks also intersect with U.S. entities for less specialized financing needs due to the prominence of U.S. financial institutions in providing U.S. dollar-denominated international banking services. Many of the most recent case examples involve complex North Korean-linked networks utilizing U.S. correspondent banks to facilitate sales of North Korean-origin goods that are prohibited by sanctions; moving these ill-gotten gains across multiple jurisdictions (and sometimes eventually back to the Democratic People's Republic of Korea [DPRK]); and acquiring other goods for the North Korean regime that are seemingly devoid of WMD applications.[26] While these activities may on the surface look like traditional money laundering or smuggling schemes without an obvious connection to the DPRK's WMD programs, they often violate the global sanctions architecture put in place to counter Pyongyang's WMD-related ambitions and can thus be considered "proliferation financing."

Iran's efforts to exploit the U.S. commercial, technological, and financial systems have traditionally involved both procurement and sanctions evasion in support of regime entities associated with WMD and ballistic missile development.[27] After the implementation of the Joint Comprehensive Plan of Action (JCPOA) in 2016 and the corresponding easing of many international sanctions targeting Iran, there were other, less difficult options open to the Iranian regime to raise and move funds globally and therefore less of a need to employ the same covert fundraising and fund movement practices. However, even prior to the U.S. withdrawal from the JCPOA in May 2018 and the gradual re-imposition of U.S. nuclear-related sanctions thereafter, the U.S.

---

23. Worldwide Threat Assessment, p. 7.

24. North Korea and 'DPRK are used interchangeably throughout the *Illicit Finance Strategy* and NPFRA.

25. For example, see the Alex and Gary Tsai case study in the NPFRA.

26. For example, see the cases of Dandong Hongxiang Industrial Development Co. Ltd. (DHID), Mingzheng International Trading Limited (Mingzheng) and Dandong Chengtai Trading Co. Ltd, also known as Dandong Zhicheng Metallic Material Co., Ltd (Zhicheng), all detailed in the NPFRA.

27. See the NPFRA for Iran-related procurement (Karl Lee) and broader sanctions evasion case studies (Foreign Bank case and Zarrab case).

maintained a robust sanctions program and broad primary embargo against Iran, designating several additional entities linked to Iran's ballistic missile program during the time the U.S. remained a party to the JCPOA. As a result, the U.S. has consistently maintained a proactive posture of isolating the Iranian regime from the U.S. financial system, which has made it difficult for Iranian-linked entities to conduct PF-related activities with a U.S. nexus.[28] Recent cases, however, indicate that networks tied to Iran's weapons programs and involving U.S. entities have sought to evade U.S. sanctions, including on behalf of entities designated for WMD purposes.[29]

Syria's efforts to exploit the U.S. financial system for WMD-related purposes have also generally been limited, due to a number of U.S. export control and sanctions regulations directed at Syrian entities. For example, the United States maintains a robust sanctions program targeting Syrian individuals and entities, including for WMD-related activities, which has served as a key preventative measure for Syrian-related PF activities transecting the U.S. financial system. Ongoing efforts, including multiple separate designations between 2015 and 2018, have focused on targeting key facilitation networks of Syria's Scientific Studies and Research Center (SSRC), which is the Syrian government agency responsible for developing and producing nonconventional weapons and the means to deliver them.[30] Despite these efforts, there have been some attempts by PF networks to exploit the U.S. financial system and to acquire sensitive or controlled goods on behalf of Syrian entities, including two recent procurement cases, one of which involved individuals with business connections to SSRC-linked companies.[31]

There have been relatively few publicly reported cases in recent years of the U.S. financial system being used to facilitate the development of China's or Russia's indigenous WMD programs.[32] With respect to China, there are several important examples in recent years of Chinese entities and individuals engaging in PF activities with a U.S. nexus, but the activity in question has been

28. See the NPFRA for further detail on recent U.S. sanctions actions targeting Iranian networks overseas. These measures help to isolate malignant Iranian activity and cut off PF networks from the U.S. financial system.

29. See the NPFRA for Iran-related sanctions evasion case studies (Foreign Bank case and Zarrab case).

30. See Treasury, Press Release, Treasury Targets Syrian Regime Financial and Weapons Networks, March 31, 2015, available at https://www.treasury.gov/press-center/press-releases/Pages/JL10013.aspx; Treasury, Press Release, Treasury Sanctions Networks Providing Support to the Government of Syria, July 21, 2018, available at https://www.treasury.gov/press-center/press-releases/Pages/jl0526.aspx; Treasury, Press Release, Treasury Sanctions Additional Individuals and Entities in Response to Continuing Violence in Syria, Dec. 23, 2016, available at https://www.treasury.gov/press-center/press-releases/Pages/jl0690.aspx; Treasury, Press Release, The United States and France Take Coordinated Action on Global Procurement Network for Syria's Chemical Weapons Program, July 25, 2018, available at https://home.treasury.gov/index.php/news/press-releases/sm443.

31. See the NPFRA for the two Syria PF cases.

32. However, as demonstrated in the NPFRA, there have been several instances of Chinese individuals or entities being involved in PF networks working on behalf of other countries' WMD programs. The UN Panel of Experts on North Korea has also pointed to North Korean overseas banking representatives operating in China, Russia, and other jurisdictions, where they control bank accounts and facilitate transactions supporting the DPRK's weapons programs (see March 2018 Panel of Experts Report, p. 60, available at http://www.un.org/ga/search/view_doc.asp?symbol=S/2018/171). These are North Korean individuals, however, so their operations within these jurisdictions are not assessed as China- or Russia-specific PF threats, per se.

for the benefit of other state-sponsored WMD programs, namely North Korea's and Iran's.[33] With respect to PF networks benefitting Russian WMD and delivery systems programs, a few recent, notable cases have involved procurement of U.S.-origin sensitive technology, some of which has WMD or missile technology applications. These networks tend to target sensitive U.S. technology, where there seemed to be both a lack of domestic capacity by the Russian industrial base and a lack of drive to develop an indigenous production capability.[34]

Like China and Russia, Pakistan is a nuclear weapons state, but there is no U.S. targeted financial sanctions program dedicated to Pakistan for the development and maintenance of its nuclear weapons program.[35] Unlike China and Russia, however, Pakistan is not a party to the Treaty on the Non-Proliferation of Nuclear Weapons (NPT) and therefore is not recognized under international law as having the right to the peaceful use of nuclear energy, including the transfer or acquisition of nuclear technology. This sequestration from regulated international channels has largely forced Pakistan to attempt to acquire technology and know-how through covert means and, in select cases, those acting for or on behalf of Pakistani government entities have sought to procure U.S.-origin goods and facilitate these illicit transactions by exploiting the U.S. financial system.[36]

TRANSNATIONAL CRIMINAL ORGANIZATIONS[37]

Mexican and Russian TCOs operating in the U.S. remain priority threats, with African and Asian organizations becoming more significant each year. Drug cartels in Colombia, Peru, and throughout Central America and the Caribbean also operate as independent TCOs. TCOs, including nation states, are also involved in various cybercrimes, including business e-mail compromise and corporate account takeovers.

---

33. For example, Chinese national Karl Lee operated a PF network on behalf of entities linked to Iran's ballistic missile program, while Chinese entities DHID, Mingzheng, and Zhicheng, as well as certain Chinese nationals associated with these companies, all worked on behalf of the DPRK. See the NPFRA for more details regarding these cases.

34. See the ARC Electronics case in the NPFRA for more details.

35. For example, unlike Iran, North Korea, and Syria, Treasury's Office of Foreign Assets Control (OFAC) does not administer a sanctions program targeted specifically at Pakistan. However, the United States has historically imposed other types of sanctions on Pakistan for its nuclear weapons and ballistic missile programs. The bulk of these nuclear-related sanctions were waived by President Bush on September 22, 2001, due to Pakistan's cooperation in the Global War on Terror. See Presidential Determination No. 2001–28 of September 22, 2001, Waiver of Nuclear-Related Sanctions on India and Pakistan, 66 Fed. Reg. 191 (Oct. 2, 2001). However, as with the other state-sponsored programs covered by the NPFRA, as well as this Strategy, the overall proliferation threat profile is derived from the ODNI's Worldwide Threat Assessment. See the NPFRA for more details.

36. See the NPFRA for a Pakistan-related PF case.

37. See the 2018 NMLRA for a full discussion of money laundering threats.

African TCOs

Nigerian criminal enterprises are the most significant of the African TCOs, according to the Federal Bureau of Investigation (FBI).[38] They are primarily engaged in drug trafficking and financial fraud, including business e-mail compromise schemes and various confidence scams in the United States.

Asian TCOs

Asian TCOs conduct racketeering activities normally associated with organized crime—extortion, murder, kidnapping, illegal gambling, prostitution, and loansharking, according to the FBI.[39] They also smuggle persons, traffic heroin and methamphetamine, commit financial fraud, steal automobiles and computer chips, counterfeit computer and clothing products, and commit money laundering. According to Drug Enforcement Administration's (DEA) 2017 National Drug Threat Assessment (NDTA), Asian organized crime groups in the United States are prominent in money laundering for Mexican, Colombian, and Dominican drug trafficking organizations (DTOs).[40]

Mexican and Colombian TCOs

Mexican TCOs dominate the U.S. drug trade and associated money movement. DEA investigations show that six major Mexican drug cartels maintain drug distribution cells in cities across the United States.[41] It is anticipated that Mexican TCOs will continue to grow in the United States through the expansion of distribution networks and relationships with intermediaries, such as U.S.-based Dominican traffickers and local gangs.

Colombian TCOs rely on their partnership with Mexican TCOs for the sale and distribution of wholesale quantities of cocaine and heroin in the United States. Colombian TCOs dominate the production and supply of the majority of cocaine shipped to U.S. markets. Colombian TCOs also maintain a physical presence in the United States to facilitate the laundering of illicit proceeds.

Eurasian TCOs

Based on Suspicious Activity Report (SAR) analysis, Treasury's Financial Crimes Enforcement Network (FinCEN) has determined that Russian organized crime groups in the United States engage in a variety of crimes including illegal gambling, money laundering, and various types of fraud. SARs indicate suspicious money laundering activity involving cross-border wires from bank accounts held by shell companies and trade-based money laundering (TBML) involving auto

---

38. FBI, What We Investigate: Transnational Organized Crime, available at https://www.fbi.gov/investigate/organized-crime.

39. *Id.*

40. DEA, National Drug Threat Assessment (October 2017), available at https://www.dea.gov/sites/default/files/docs/DIR-040-17_2017-NDTA.pdf.

41. These cartels are the Sinaloa Cartel, Jalisco New Generation Cartel (Cartel Jalisco Nueva Generación, or CJNG), Juarez Cartel, Gulf Cartel, Los Zetas Cartel, and Beltran-Leyva Organization.

sales. The roots of Eurasian organized crime in the United States are found in the *Vory V Zakone*, or "Thieves-in-Law," a global criminal organization that originated in the former Soviet Union.

PROCEEDS-GENERATING CRIMES

Fraud

Fraud is estimated to generate more illicit proceeds laundered in the United States than any other category of crime. It encompasses a wide range of criminal activity including health care fraud, which alone is estimated to generate as much as $100 billion in illicit proceeds.[42] Health care fraud, tax refund fraud, bank fraud, and credit card fraud, for example, often involve the use of stolen identities.

Drug Trafficking

The illicit drug market has changed significantly in recent years with the increase in domestic marijuana production following legalization or penalty reduction in many states, a rebound in cocaine sales, growth in the sale of heroin and synthetic opioids, an expanding market for methamphetamine, and the persistent creation and sale of new synthetic psychoactive substances.[43] Given these market dynamics, a current estimate of illicit drug proceeds in the United States available for laundering is $100 billion.[44]

Corruption

Public corruption investigations encompass bribery, extortion, embezzlement, and illegal kickbacks, and can involve local, county, state, federal, and foreign officials. Even if the person paying a bribe is not a U.S. person and the recipient is not a U.S. official, the conduct may violate federal laws, such as the Foreign Corrupt Practices Act (FCPA) and money laundering statutes if the proceeds are laundered through the U.S. financial system.

Human Smuggling/Trafficking

Human smuggling involves illegally transporting into the United States people who have consented to their transportation, and may also involve the subsequent harboring of those individuals in the United States. According to the Department of Homeland Security (DHS) Office of Immigration Statistics (OIS), increased border security has driven up the fees paid to smugglers to get migrants across the Southwest border.[45] Smuggling fees for Mexicans and Central

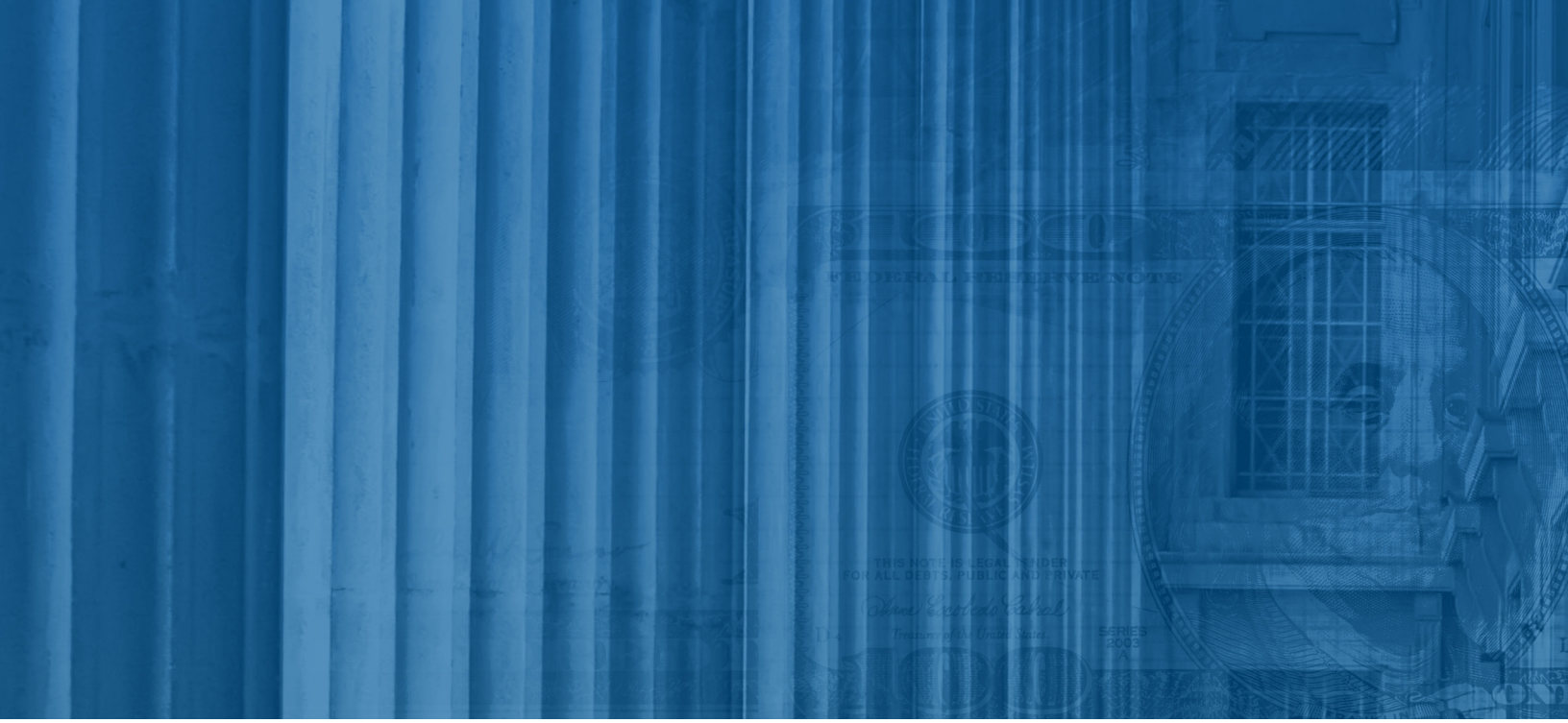
---

42. DOJ, Health Care Fraud Unit, available at https://www.justice.gov/criminal-fraud/health-care-fraud-unit.
43. DEA, National Drug Threat Assessment (October 2017).
44. RAND Corporation (prepared for the Office of National Drug Control Policy), *What America's Users Spend on Illegal Drugs: 2000–2010*, available at https://www.rand.org/pubs/research_reports/RR534.html.
45. DHS OIS, Efforts by DHS to Estimate Southwest Border Security between Ports of Entry, September 2017, available at https://www.dhs.gov/sites/default/files/publications/17_0914_estimates-of-border-security.pdf.

Americans reportedly have been as high as $1,200 for the initial staging payment and $8,000 at the final destination, but DHS/OIS finds the average fee is approximately $4,000.

Human trafficking is exploitation of nonconsenting persons, often across borders, and involves using force, fraud, or coercion to recruit individuals to provide labor or services, including prostitution, which may be prosecuted as sex trafficking. DHS Homeland Security Investigations (HSI) estimates that human trafficking generates $32 billion annually.[46]

46. ICE-HSI, Press Release, Using a financial attack strategy to combat human trafficking, January 29, 2015, available at https://www.ice.gov/news/releases/using-financial-attack-strategy-combat-human-trafficking.



SECTION 2.
ILLICIT FINANCE RISKS

The relative significance of any particular illicit finance risk is based on the probability of a vulnerability being exploited, the consequence of that vulnerability, and the effectiveness of U.S. authorities to mitigate the risk. The *Illicit Finance Strategy* relies in part on individual risk assessments of terrorist financing, proliferation financing, and money laundering. The 2018 National Terrorist Financing Risk Assessment (NTFRA) and 2018 National Money Laundering Risk Assessment (NMLRA) update risk assessments previously published in 2015. The 2018 *National Proliferation Financing Risk Assessment* (NPFRA) is the first of its kind.

TERRORIST FINANCING

The most common method of terrorist financing (TF) in the United States involves individuals who knowingly provide funds to terrorists, terrorist groups, or their supporters abroad. The groups receiving this support include organizations designated by the United States as FTOs, including ISIS and its regional affiliates, AQ and its regional affiliates Hizballah, Al-Shabaab, ANF, Hizballah, and Hamas.[47] These groups and their supporters target individuals sympathetic to humanitarian causes or vulnerable to violent messaging and utilize a variety of methods, including social media platforms, to recruit and/or solicit financial or other forms of material support.

ISIS

ISIS derives most of its revenue from two primary sources of funding, (1) the extortion and taxation of civilian populations and economies in Iraq and Syria, and (2) the smuggling and sale of oil and oil products. However, ISIS also receives limited financial support from within the United States. ISIS-related financial activity in the United States is most commonly associated with U.S. persons traveling or aspiring to travel abroad to join ISIS in Iraq, Syria, or other jurisdictions where ISIS regional affiliates are active, although the number of U.S. persons traveling or attempting to travel to Syria and Iraq has declined since 2015. Funds used to support this travel-related activity primarily come from legitimate activities, such as from personal savings. In other cases, U.S.-based individuals have raised or solicited funds specifically for the group itself. These funds are often derived from legitimate sources as well as from small-scale criminal activity. ISIS financiers and supporters abroad also send funds to other ISIS supporters or regional affiliates in foreign jurisdictions that may be routed through the U.S. financial system and may seek to procure sensitive or controlled goods from U.S.-based companies.

Hizballah

Hizballah receives the majority of its funding, upwards of $700 million a year, from Iran, which is the world's foremost state sponsor of terrorism.[48] In addition to funding from Iran,

47. See Footnote 11. See the 2018 NTFRA for additional information on the TF threat posed by each of these groups to the United States.

48. Sigal Mandelker, Under Secretary for Terrorism and Financial Intelligence, Speech before the Foundation for the Defense of Democracies, June 5, 2018, available at https://home.treasury.gov/news/press-releases/sm0406.

Hizballah receives money from a global network of supporters and businesses.[49] These supporters generate funds from both legitimate and illicit activities (much of which is not directly connected to Hizballah or conducted at the behest of Hizballah) and send funds to Hizballah operatives using a variety of funds transfer methods. Hizballah operatives are active in the United States and are looking to raise funds through donations, commercial activity, and criminal activity. Hizballah-affiliated networks continue to generate revenue from drug trafficking or organized criminal activity that has a U.S. nexus. Hizballah-affiliated networks also seek to procure sensitive or controlled goods from the United States.

AQ

AQ and its regional affiliates generate their funding from individual fundraisers in Gulf countries and supporters throughout the world, including in Afghanistan, Pakistan, Africa, Southeast Asia, and increasingly in Yemen and Syria.[50] These groups also continue to seek funds and other resources from U.S.-based supporters, as well as derive support from the territory they control.

Al-Shabaab

Al-Shabaab continues primarily to finance its operations through revenue from (1) charcoal and other natural resources, and (2) extortion of businesses and individuals. Al-Shabaab continues to work through U.S.-based facilitators to raise funds from witting supporters, as well as from unwitting donors under the false pretenses of charity but outside of any tax-exempt charitable organization.

Hamas

Hamas, which has historically raised funds in the United States through the creation of sham or fraudulent charities, continues to look to the United States as a venue for revenue generation.

Other Terrorist Groups

Other terrorist groups, such as the Taliban and Islamic Jihad Union, also continue to look to the United States as a venue for revenue generation.

MISUSE OF THE U.S. FINANCIAL SYSTEM

U.S.-based terrorist financiers and supporters seek to place their funds, often legitimately earned, into the U.S. financial system and transfer the money abroad. Due to prevalence and

49. Press Release, Treasury, "Treasury Targets Hizballah Financial Network in Africa and the Middle East," February 2, 2018, available at https://home.treasury.gov/news/press-releases/sm0278.

50. Daniel Glaser, Assistant Secretary for Terrorist Financing, Testimony before the House Committee on Foreign Affairs Subcommittee on Terrorism, Nonproliferation, and Trade, and the House Committee on Armed Services Subcommittee on Emerging Threats and Capabilities, June 9, 2016, available at https://www.treasury.gov/press-center/press-releases/Pages/jl0486.aspx.

accessibility, banks and money services businesses (MSBs) are the most commonly used channels.[51] Importantly, due to the nature of terrorist financing (often legitimately sourced funds later used to fund illicit activity), these entities face challenges in distinguishing terrorism-related financial transactions from licit activity.

Due to the centrality of the U.S. financial system and the U.S. dollar, U.S. banks continue to face TF risk due to their role in U.S. dollar clearing and processing international payments. For example, along with raising funds in the United States or through U.S. persons, ISIS financiers and supporters seek to access the U.S. and international financial systems, both directly and indirectly, to move funds in support of ISIS and its regional affiliates throughout the world.[52] U.S. authorities have also identified instances where ISIS operatives route transactions through third parties to avoid detection, as well as channel financial activity through neighboring localities (as ISIS operates in regions with limited access to the international financial system).[53]

Some U.S.-based MSBs face TF risk from the acts of complicit employees, as well as isolated compliance deficiencies in smaller online payment providers that provide person-to-person funds transfers.[54] Unlicensed money transmitters also remain an important channel for some terrorist groups and their supporters. Robust implementation of AML/CFT standards by U.S. financial institutions makes cash a relatively secure if inefficient alternative for terrorist groups or supporters that prioritize operational security over the speedy movement of funds.

Charities

U.S. tax-exempt charitable organizations that only operate and disburse funds domestically face low risk of TF abuse.[55] However, there continues to be greater TF risk for the small number of U.S. tax-exempt charitable organizations that operate in, send funds to, or have affiliated organizations in high-risk regions where ISIS and its regional affiliates, AQ and its regional affiliates, Al-Shabaab, ANF and other terrorist groups are most active, such asAfghanistan, Pakistan, Somalia, Syria, and Yemen.[56]

Virtual Currency[57]

While there have been isolated instances of terrorist groups and their supporters soliciting funds in virtual currencies, such as bitcoin, and using virtual currencies to move funds or purchase goods or services, virtual currencies do not currently present a significant TF risk, but they bear close monitoring as their use is only likely to grow. Lack of regulation and supervision in most

51. See the NTFRA section titled "Vulnerabilities and Risks".
52. See the 2018 NTFRA for additional information on ISIS-linked financial activity.
53. *Id.*
54. See the 2018 NTFRA section titled "Vulnerabilities and Risks".
55. *Id.*
56. *Id.*
57. See *Emerging Illicit Finance Risks: Virtual Currency* for further information.

jurisdictions worldwide exacerbates the illicit finance and sanctions evasion risks that virtual currency payments present.

PROLIFERATION FINANCING

The United States maintains a strong regulatory framework, effective supervision of financial institutions and other related industries, robust law enforcement and financial intelligence assets, and proactive preventative measures to mitigate proliferation financing (PF) activity before it reaches the U.S. financial system. However, the sheer size and scale of the global banking system, which is underpinned by cross-border banking relationships linking together virtually every jurisdiction in the world, mean that proliferation networks can make use of complex corporate and banking arrangements to mask their illicit activity and achieve their ends. While there are occasional instances where these networks have sought to rely on nonbanking channels to raise revenue and facilitate funds transfers, including select cases where PF networks have utilized MSBs and relied upon bulk cash transfers, these vulnerabilities were largely exploited outside of the United States.[58]

Most of the PF activity that touches the U.S. financial system has been the result of PF networks exploiting global correspondent banking relationships. In the United States, it is the banks, particularly large dollar-clearing banks operating on a global scale with correspondent relationships that are most at risk of PF-related activity.[59]

In some examples, access to the U.S. financial system was facilitated at banks by complicit insiders or due to systemic deficiencies within the bank's own AML/CFT compliance program. Most instances, however, are the result of difficulties in detecting sophisticated schemes and deceptive practices of PF networks. The cases in which this has occurred almost always involve U.S. banks settling transactions on behalf of the customers of foreign financial institutions, and where there are often multiple intermediary financial institutions involved in a given transaction or set of related transactions.

Another challenge contributing to PF risk in the United States relates to understanding how PF differs from other illicit financial activity, such as money laundering or terrorist financing. While U.S. banks—particularly the large dollar-clearing institutions that are likely to be exposed to PF activity—have some of the most sophisticated financial crimes compliance programs in the world, many of these institutions are only recently tailoring their internal controls to address more effectively the unique threat profile of PF networks. Smaller banks, other financial institutions, and other key industry stakeholders may be even less aware of the nuances between PF and other types of illicit activity. While this may not seem as great a challenge now, given the business profiles of these institutions, having more even implementation of counter-PF controls would

58. For instance, in the Zarrab case outlined in the NPFRA, the PF network utilized foreign MSBs. However, the network's exploitation of the U.S. financial system occurred through cross-border banking connections.

59. See the NPFRA for more details, particularly the "Threats" section where correspondent banking is the main vulnerability exploited in each of the case studies, but also the "Vulnerabilities and Risks" section under "Misuse of Foreign Correspondent Relationships."

strengthen the U.S. financial system and potentially provide law enforcement with additional means to detect and combat this unique threat.

MONEY LAUNDERING

The crimes that generate the bulk of illicit proceeds for laundering in the United States are fraud, drug trafficking, human smuggling, human trafficking, organized crime, and corruption. The many varieties of fraud, including bank, consumer, health care, securities, mortgage and tax refund fraud, are believed to generate the largest share of illicit proceeds. Health care fraud alone generates proceeds of approximately $100 billion annually. Prosecutions indicate that health care fraud often involves complicit health care professionals submitting fraudulent invoices to insurers. Insurance payments and subsequent transactions may flow through the banking system and look indistinguishable from legitimate funds transfers. When payments are made by check, the laundering can involve the help of complicit check cashers.

Law enforcement agencies have seen an increase in cybercrime, which encompasses a variety of illicit activity including phishing, malware attacks, cyber-enabled crime such as credit card fraud, business e-mail compromise; and various types of consumer scams, including fake romance and lottery schemes, and employment offers that all inevitably involve the victim receiving requests for money. These internet-based crimes can be perpetrated from anywhere in the world. Global money laundering syndicates employ complicit merchants, financial services professionals, and other individuals to launder illicit proceeds of various criminal schemes.

Mexico remains the dominant conduit for illegal drugs entering the United States. Professional money launderers often take possession of the drug proceeds in the United States and facilitate the laundering process. Such laundering can involve a combination of structured bank deposits, funnel accounts, and bulk cash smuggling. A typical scheme exemplifying how these money laundering methods work together involves the pooling of proceeds into a single account as the result of small cash deposits at bank branches throughout the country, then either wiring the collected funds to Mexico or withdrawing them in cash near the Southwest border for smuggling into Mexico. Another common method is trade-based money laundering, which involves using a cycle of money brokers and exporters of goods to disguise and move drug money. The sale of the goods outside the United States effectively launders the money and provides the drug suppliers with payment in their local currency. Merchants may knowingly accept large amounts of drug cash and willingly participate in the laundering. Others, receiving payment by check or wire for their goods, may be unaware they are facilitating money laundering.

The nature of synthetic drug trafficking and associated financial flows has changed with the rise of China as a supplier of fentanyl and its analogues and precursors. China is the primary source of fentanyl,[60] and payments to China for these drugs are made by bank and nonbank wires as well as by virtual currencies. Mexican drug cartels also obtain illicit fentanyl and precursor

60. Sean O'Connor, U.S.-China Economic and Security Review Commission, Fentanyl: China's Deadly Export to the United States, February 1, 2017.

materials required to manufacture fentanyl-related substances from China, and primarily use fentanyl as an adulterant in heroin produced in Mexico.[61] In October 2017, the Department of Justice (DOJ) announced its first indictments of Chinese nationals for fentanyl trafficking in the United States. After a series of deaths and overdoses that prompted the investigation, 32 defendants were charged. The Attorney General noted: "[t]his was an elaborate and sophisticated conspiracy. They allegedly used the internet, about 30 different aliases, cryptocurrency, offshore accounts, encrypted communications, and allegedly laundered funds internationally through third parties."[62] In April 2018, Office of Foreign Assets Control (OFAC) followed this action with the first designation of a Chinese fentanyl trafficker as a Significant Foreign Narcotics Trafficker pursuant to the Foreign Narcotics Kingpin Designation Act (Kingpin Act).[63]

Virtual currencies, in addition to being the preferred form of payment for buying illicit drugs and other illicit goods online, and paying the perpetrators of ransomware attacks, are also now used as money laundering vehicles. For example, global money laundering syndicates are offering to move illicit proceeds into and through virtual currencies as another way to layer transactions in order to hide the origin of dirty money.

The most significant money laundering risks in the United States include misuse of cash; complicit merchants, professionals, and financial services employees; and lax compliance at financial institutions. These are the residual risks after taking into consideration the scope and quality of U.S. anti-money laundering regulation, supervision, and enforcement. Although improvements can be made to diminish these risks, the fact that they exist to some extent should not be considered surprising.

Anonymity in transactions and funds transfers is the main risk that facilitates money laundering. Criminal actors involved in drug trafficking, human smuggling and trafficking, illicit retail transactions, and various activities associate with organized crime continue to prefer U.S. currency-denominated cash due to its widespread use in the United States as well as its global use due its wide acceptance as a stable store of value and medium of exchange. Virtual currencies, when exchanger and administrators are unregulated, also provide anonymity and pose risks due to the speed they can be transmitted, disintermediation, global reach, and the lack of regulation and supervision in many jurisdictions. The risk of the misuse of cash and virtual currency is mitigated in the United States by the imposition of AML program, suspicious and currency transaction reporting, and customer recordkeeping requirements on financial institutions. In addition, businesses and individuals have cash reporting obligations in certain circumstances

---

61. Matthew Allen, Assistant Director HSI, Testimony before the House Committee on energy and Commerce Subcommittee on Oversight and Investigations, March 21, 2017, available at https://energycommerce.house.gov/hearings/fentanyl-next-wave-opioid-crisis-2/.

62. DOJ, Press Release, Attorney General Sessions Announces New Indictments in International Fentanyl Case, April 27, 2018, available at https://www.justice.gov/opa/speech/attorney-general-sessions-announces-new-indictments-international-fentanyl-case; DOJ, Press Release, Justice Department Announces First Ever Indictments Against Designated Chinese Manufacturers of Deadly Fentanyl and Other Opiate Substances, October 27, 2017, available at https://www.justice.gov/opa/pr/justice-department-announces-first-ever-indictments-against-designated-chinese-manufacturers.

63. Treasury, Press Release, Treasury Sanctions Chinese Fentanyl Trafficker Jian Zhang, April 27, 2018, available at https://home.treasury.gov/news/press-releases/sm0372.

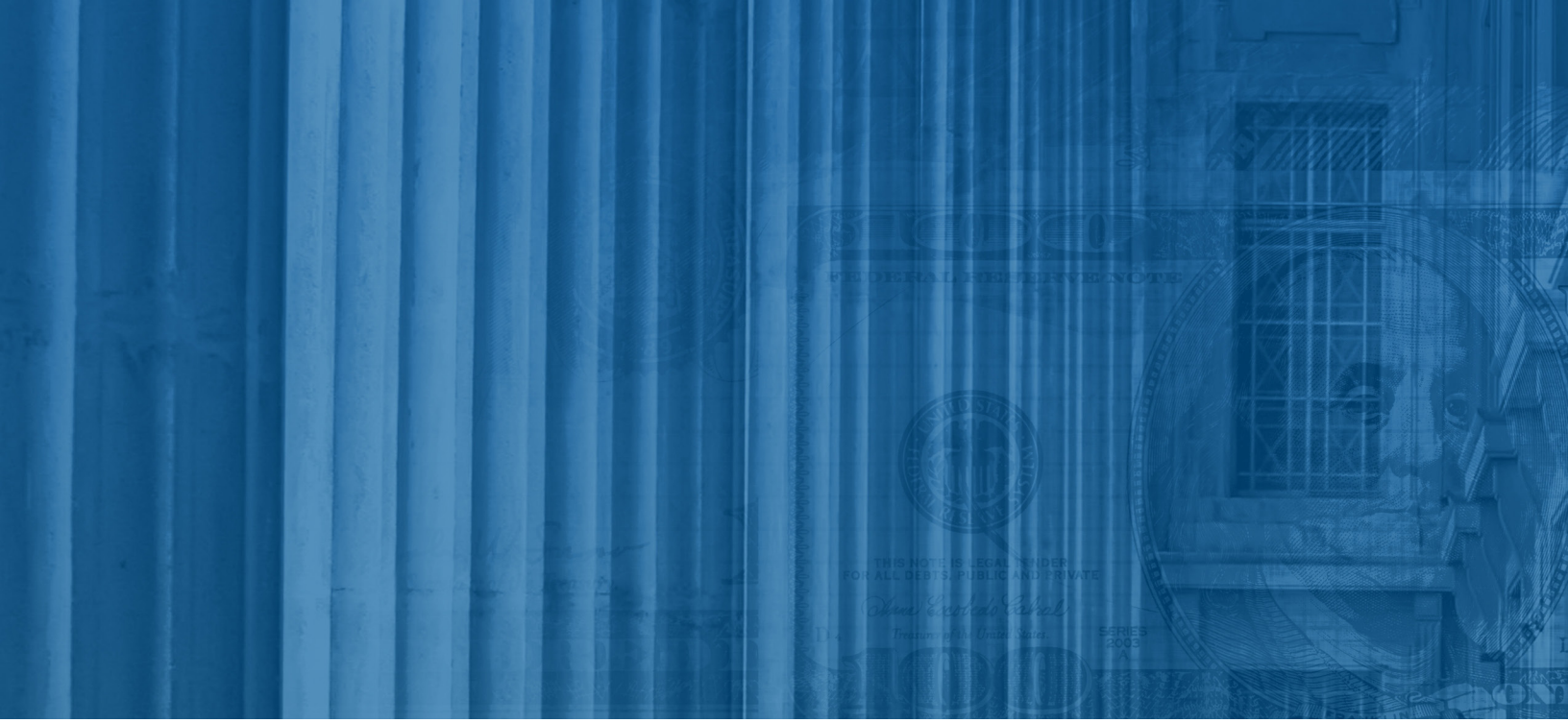
to mitigate the risks of using cash. But these obligations are only effective to the extent they are followed. Criminals seek out complicit merchants, professional, and financial services employees. Individuals who abuse their professional position at financial institutions also are a money laundering risk. These individuals facilitate the opening of accounts, conduct funds transfers, and cash checks while knowingly failing to verify customer identification when required, maintain accurate transaction records, or file required reports.[64] Financial institutions with lax compliance programs also pose a money laundering risk.

Finally, pursuing global money laundering syndicates requires U.S. law enforcement to partner with other countries to trace illicit proceeds, identify relevant parties, collect evidence, seize assets, and apply sanctions to problematic financial networks. A continuing money laundering vulnerability for the United States is that some countries lack the necessary authorities, capabilities, or motivation to help U.S. law enforcement pursue money laundering investigations with a nexus to the United States.

Furthermore, countries with strategic deficiencies or weak AML/CFT regimes continue to pose an illicit finance vulnerability for the United States. Criminals can circumvent weak AML/CFT controls to launder money successfully or to move assets to finance terrorism through the financial system. As part of the Financial Action Task Force (FATF)'s listing and monitoring process to ensure compliance with its international AML/CFT standards, the FATF identifies certain jurisdictions as having strategic deficiencies in their AML/CFT regimes.[65]

64. Title 31 of the U.S. Code, Section 5313, requires a financial institution to file a Currency Transaction Report with FinCEN for each cash transaction or group of related cash transactions in a day that aggregate to more than $10,000. Willful failure to file a CTR is criminalized under Title 31 of the U.S. Code, Section 5322. Financial institutions in the United States are required to file a suspicious activity report to FinCEN under certain circumstances as specified by regulation.

65. FinCEN, Advisory on the FATF-Identified Jurisdictions with AML/CFT Deficiencies, February 9, 2018, available at https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2018-a001#_ftn1.



SECTION 3.
EMERGING ILLICIT FINANCE RISKS:
VIRTUAL CURRENCIES

Treasury is responsible for maintaining the integrity, efficiency, and accessibility of the U.S. financial system to facilitate commerce and the free movement of capital. In pursuit of this objective, Treasury seeks to encourage responsible innovation in the financial sector, domestically and globally, while protecting the financial system from money laundering, terrorist financing, sanctions evasion, cybercrime, fraud and other illicit finance risks—including risks associated with new and emerging payments products and services.

Overview

Virtual currencies, particularly decentralized convertible virtual currencies, such as bitcoin, have emerged as an alternative to traditional payments systems. Sometimes also called cryptocurrency, this type of virtual[66] currency relies on a combination of distributed ledger technology and public/private key cryptography.

There are a large number of virtual currencies available today. Some of these virtual currencies add technical features explicitly designed to obscure or anonymize transactions (referred to as anonymity-enhanced cryptocurrencies or privacy coins), presenting potential AML/CFT risks through businesses that choose to service them. Anonymizing software such as the Tor network used in conjunction with mixers and tumblers[67] can further obscure the source and destination of virtual currency and frustrate law enforcement's efforts to link transactions to people, virtual currency wallets, or IP addresses.[68]

According to the Internal Revenue Service-Criminal Investigations Division (IRS-CI), some bitcoin alternatives, or altcoins, provide more anonymity than bitcoin because they do not post transactions to a decentralized public blockchain ledger. Anonymity-enhanced virtual currencies are being used online to purchase illicit drugs and other illegal goods and services through online marketplaces. Virtual currencies are also being used to facilitate money laundering. Financial Crimes Enforcement Network (FinCEN) analysis indicates that virtual currency transactions include over $1 billion in ransomware extortion funds, and over $1.5 billion has been stolen through hacks of virtual currency exchangers and administrators over the past two years.[69]

---

66. Virtual currency, digital currency, and cryptocurrency are often used interchangeably. Guidance issued by FinCEN refers to virtual currency. See FinCEN, Guidance, Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies, March 18, 2013, available at https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf.

67. Tumbler and mixing services takes virtual currencies like bitcoin from many users, routes them through a complex funding path, and redistributes them so they no longer can be readily traced to a specific source. See FBI, Law Enforcement Bulletin, Virtual Currency: Investigative Challenges and Opportunities, September 8, 2015, available at https://leb.fbi.gov/articles/featured-articles/virtual-currency-investigative-challenges-and-opportunities.

68. Bitcoin and other virtual currencies rely on blockchain technology, a distributed public ledger containing an historical record of every transaction. Third-party services like mixers and tumblers can defeat the blockchain by obscuring the source, destination, and movement of the virtual currency. Some virtual currencies have built-in mixers.

69. Thomas P. Ott, Associate Director, FinCEN Enforcement Division, statement before House Subcommittee on Terrorism and Illicit Finance, June 20, 2018.

FinCEN analysis also estimates that at least $4 billion in virtual currency has moved through darknet marketplaces since 2011.[70]

There have been instances of terrorist groups and their supporters soliciting funds in virtual currencies, such as bitcoin, and using virtual currencies to move funds or purchase goods and services. Lack of regulation and supervision in most of the world exacerbates the illicit finance and sanctions evasion risks that virtual currencies present.

Illicit Use Increasing

The Federal Bureau of Investigation (FBI) has approximately 122 open investigations relating to the use of virtual currencies. These investigations are focused on money laundering, cyber intrusion, business e-mail compromise, securities fraud, initial coin offerings, human trafficking, drug trafficking, and bank fraud.[71] In fiscal year 2018, FBI investigations led to the seizure of virtual currency worth approximately $60 million from approximately 30 different investigations.

Other federal law enforcement agencies also note the increased prevalence of virtual currency investigations and related seizures. For example, Homeland Security Investigations (HSI) recorded one investigation involving virtual currency in fiscal year 2011, but initiated 203 investigations in fiscal year 2017.[72] For fiscal year 2018 as of May, HSI had initiated 144 new virtual currency investigations, an annual rate of more than 216. In fiscal year 2014, HSI seized $151,459 in virtual currency, whereas fiscal year 2018 through the end of April saw $25,442,611 in HSI-seized virtual currency. The following charts have been included to provide a visual example of how one particular agency has seen an increase in seizures and criminal investigations involving virtual currency respectively. These charts confirm the reporting from other law enforcement agencies that the detection of criminal exploitation of virtual currency is on the rise.

Similarly, from FY 2015 to the present, the U.S. Secret Service (USSS) seized more than $28 million in virtual currencies, primarily bitcoin, in the course of its criminal investigations.[73]

Regulation and Supervision

Mitigating the misuse of virtual currencies requires applying the same safeguards as are applied to conventional payment systems, including licensing, supervision, recordkeeping, and transaction

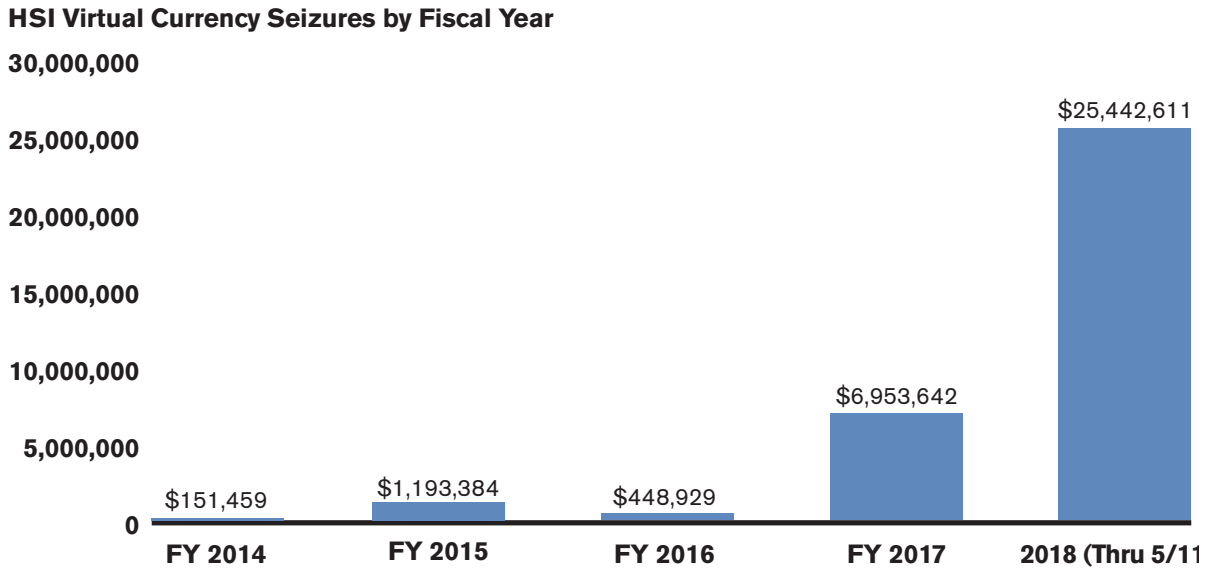
---

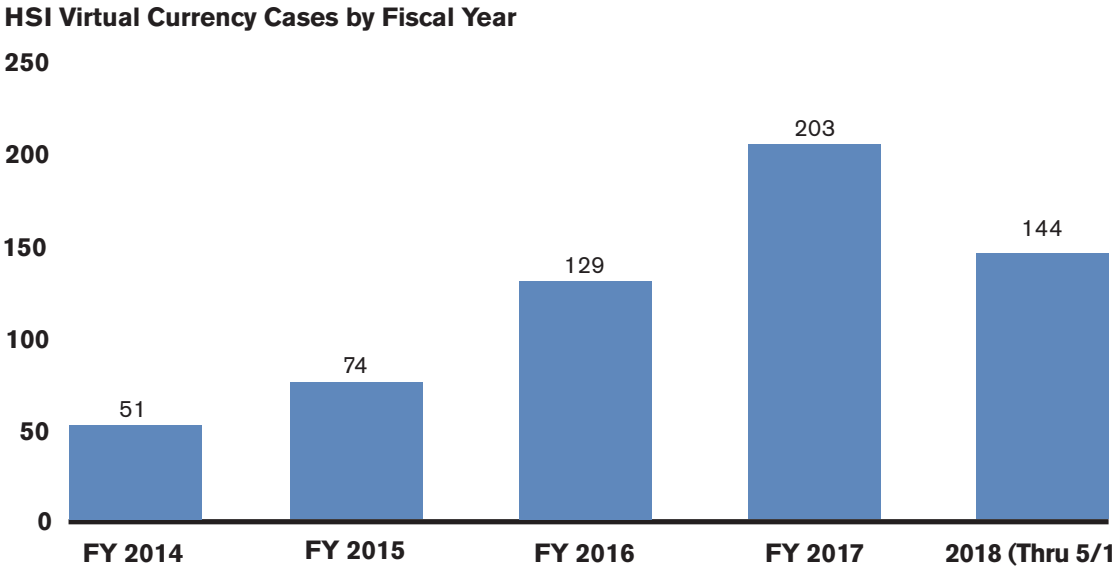
70. Darknet content is not indexed by traditional search engines and requires unique software or authorization to access. See FBI, A Primer on Darknet Marketplaces, November 1, 2016, available at https://www.fbi.gov/news/stories/a-primer-on-darknet-marketplaces and ICE HSI, ICE Investigators Expose Darknet Criminals to the Light, available at https://www.ice.gov/features/darknet.

71. Steven M. D'Antuono, Acting Deputy Assistant Director, Criminal Investigative Division, FBI, statement before the House Subcommittee on Terrorism and Illicit Finance, June 20, 2018.

72. Gregory Nevano, Deputy Assistant Director Illicit Trade, Travel, and Finance Division, HSI, statement before the House Committee on Financial Services Subcommittee on Terrorism and Illicit Finance, June 20, 2018.

73. Robert Novy, Deputy Assistant Director Office of Investigations, Secret Service, statement before the House Subcommittee on Terrorism and Illicit Finance, June 20, 2018.





reporting obligations, as well enforcing the requirement to respond to subpoenas, court orders, and warrants, and to provide other information needed to assist law enforcement in their investigations. These basic AML/CFT measures are not widely applied internationally to virtual currency despite increasing evidence of misuse.

The FATF has been actively monitoring risks in this area, and issued guidance on a risk-based approach to virtual currencies in 2015. Given the urgent need for an effective global, risk-based response to the AML/CFT risks associated with virtual asset financial activities, the FATF has adopted changes to the FATF Recommendations and Glossary that clarify how the Recommendations apply in the case of financial activities involving virtual assets, which includes

virtual currency. These changes add to the Glossary new definitions of "virtual assets" and "virtual asset service providers"—such as exchanges, certain types of wallet providers, and providers of financial services for Initial Coin Offerings.[74] These changes make clear that jurisdictions should ensure that virtual asset service providers are subject to AML/CFT regulations, for example conducting customer due diligence including ongoing monitoring, record-keeping, and reporting of suspicious transactions. They should be licensed or registered and subject to monitoring to ensure compliance. The FATF is working to provide additional clarification to jurisdictions in managing the money laundering and terrorist risks of virtual assets, while creating a sound AML/CFT regulatory environment in which companies are free to innovate. As part of a staged approach, the FATF plans to prepare updated guidance on a risk-based approach to regulating virtual asset service providers, including their supervision and monitoring; and guidance for operational and law enforcement authorities on identifying and investigating illicit activity involving virtual assets.

In its various bilateral engagements with foreign counterparts, the Treasury Department routinely stresses the importance of jurisdictions taking immediate steps to address and mitigate the risks associated with virtual currency and other related digital financial assets. Treasury Department also works with the interagency, to include our federal regulatory partners, to highlight the U.S. approach to regulating, supervising, and taking enforcement actions relating to virtual currency. This includes providing "lessons learned," law enforcement case studies, and regulatory guidance directly to bilateral partners for their consideration in developing their own jurisdictional approach to regulating virtual currency and other related asset activities.

The United States regulates convertible virtual currency exchangers and administrators for centralized virtual currencies as money transmitters under the BSA and its implementing regulations. Like traditional money transmitters, a virtual currency money transmitter is required to register with FinCEN as a money services business and to implement AML programs, recordkeeping, and transaction reporting measures, including SARs. These requirements apply to foreign-located convertible virtual currency money transmitters that have no physical presence in the United States but that do business in whole or substantial part within the United States, as well as to domestic convertible virtual currency money transmitters. In addition, a money transmitter that is a U.S. person (wherever located) must, like all U.S. persons and persons otherwise subject to OFAC jurisdiction, comply with all OFAC sanctions obligations.

The BSA excludes from the definition of MSBs individuals and entities engaged in financial activities that are performed by entities registered with, and regulated or examined by, the Securities and Exchange Commission (SEC) or the Commodity Futures Trading Commission (CFTC) under federal securities and commodities trading laws, respectively. To the extent virtual currency activities, including so-called Initial Coin Offerings or an exchange-traded fund tied to the price of bitcoin or other virtual currencies, are being done by an SEC-registered exchange or broker-dealer, or CFTC-registered futures commission merchant, the individuals or entities engaged in those activities would not be covered for AML/CFT purposes as money transmitters,

74. FATF, Regulation of Virtual Assets, available at http://www.fatf-gafi.org/publications/fatfrecommendations/documents/regulation-virtual-assets.html.

but instead would be covered under the BSA as an SEC-registered exchange or broker-dealer, or a CFTC-regulated futures commission merchant.

In late 2017, the Financial Stability Oversight Council (FSOC), which was established under the Dodd-Frank Wall Street Reform and Consumer Protection Act and is charged with identifying risks to U.S financial stability, promoting market discipline, and responding to emerging threats to the stability of the U.S. financial system, formed a working group to consider issues related to digital assets. The working group, which includes FSOC member agencies with relevant jurisdictions, is examining potential uses and risks associated with digital assets, including digital currencies and their potential use for money laundering or other illicit financing purposes. It is also considering potential steps to mitigate those risks.

In addition to registration, examination and supervision by FinCEN and BSA examiners at the IRS are crucial to mitigating potential illicit finance risks associated with virtual currency. FinCEN and the IRS have examined over 30 percent of all registered virtual currency exchangers and administrators since 2014. Examinations have included a wide array of virtual currency businesses: virtual currency trading platforms, administrators, virtual currency kiosk (or ATM) companies, crypto-precious metals dealers, and individual peer-to-peer exchangers. As a result of examination and supervision, the number of SAR filings from virtual exchangers has risen tremendously over the past few years. When virtual currency money transmitter businesses fail to comply with their AML/CFT obligations, FinCEN has used its civil authorities. For example, in 2017, in partnership with DOJ, FinCEN took enforcement action against BTC-e, an internet-based, foreign-located virtual currency exchanger, for willful violation of AML/CFT laws such as adequate internal controls to mitigate the risks presented by virtual currencies with anonymizing features.[75]

Addressing Law Enforcement Obstacles

In the face of rapidly evolving technology, the U.S. and a few other countries are already regulating virtual currency exchangers and administrators subjecting them to licensing or registration and other controls. However, some service providers remain unlicensed, do not collect adequate customer records, and do not respond to legal process. These intermediaries can be prosecuted in the U.S. for operating as unlicensed money transmitters (18 U.S.C. §1960). While there have been relatively few such prosecutions in recent years, the DOJ is increasingly using this approach as a way to disrupt money laundering networks.

More challenging for law enforcement is attempting to follow the money trail in countries that do not impose AML/CFT requirements on virtual currency exchangers and administrators. Vulnerabilities in foreign jurisdictions enable illicit activity in the United States and other third-party jurisdictions as virtual currency users can often access virtual currency exchange and other services anywhere with an Internet connection. Success cannot come without concerted action in the international community. In the most extreme cases, law enforcement may be unable to identify where virtual currency exchangers, administrators, and digital wallets are located.

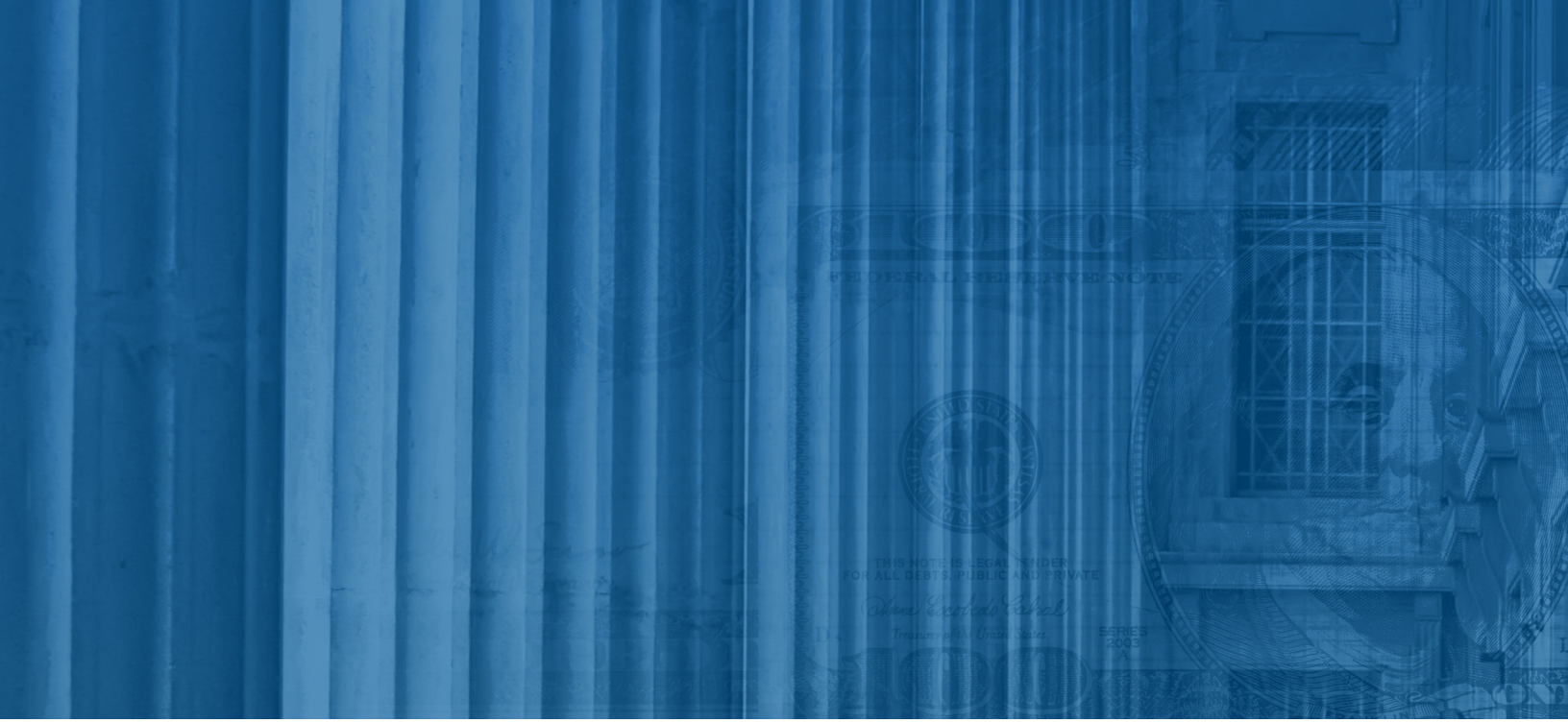
75. More information on the BTC-e case is available in the 2018 NMLRA.

According to a July 2018 FATF Report to G-20 Finance Ministers and Central Bank Governors,[76] in which the FATF summarized the results of its stock take of the different regulatory approaches across jurisdictions, three countries (China, India, and Indonesia) noted they have prohibited the use of virtual currencies or have prohibited financial institutions from dealing in virtual currencies; seven countries (Australia, France, Germany, Italy, Japan, Switzerland, and the United States) noted they apply AML/CFT regulations to virtual currencies, albeit to varying degrees depending on types of entities; two countries (Argentina and South Africa) noted they do not specifically regulate virtual currencies or exchanges but require suspicious transaction reports, including relating to virtual currencies; and 12 jurisdictions (Brazil, Canada, European Union, Mexico, Netherlands, Russia, Saudi Arabia, South Korea, Spain, Turkey, United Kingdom, and the European Union) noted they are in the process of establishing laws or regulations to address the use of virtual currencies. The FATF report reflects members' voluntary inputs and thus is not a comprehensive or definitive assessment of regulation by jurisdiction.

Because this lack of global regulation, supervision, and enforcement significantly increases the AML/CFT risks associated with virtual currency activities, the Department of the Treasury is aggressively pressing, bilaterally and through multilateral fora, for all other jurisdictions to regulate and supervise virtual currency exchangers, hosted wallets, and other virtual currency businesses that act as nodes with the regulated fiat currency system, in compliance with the international AML/CFT standards established by the FATF—the international standard setting body for measures to combat money laundering, terrorist financing, and proliferation financing.

Another challenge is law enforcement's ability to learn, understand, and investigate virtual currency-linked criminal conduct. Each of the federal law enforcement agencies that investigate financial crime are prioritizing training and support for agents to know how to identify, trace and seize virtual currencies, and preserve and exploit related evidence.

76. See FATF, FATF Report to the G20 Finance Ministers and Central Bank Governors, July 2018, available at http://www.fatf-gafi.org/media/fatf/documents/reports/FATF-Report-G20-FM-CBG-July-2018.pdf.



SECTION 4.
ENFORCEMENT EFFORTS AND TARGETED ACTIONS

Counter Terrorist Financing[77]

The October 2018 *National Strategy for Counterterrorism* notes that defeating the terrorist threat to the United States requires multiple lines of effort, including isolating and cutting off terrorists from their financial sources of support. In support of this, the U.S. government employs a range of targeted measures, including targeted sanctions, other financial measures, and law enforcement action, to identify, disrupt, and dismantle the financial networks that support these groups.

Central to this effort is E.O. 13224, which states that "because of the pervasiveness and expansiveness of the financial foundation of foreign terrorists, financial sanctions may be appropriate for those foreign persons that support or otherwise associate with these foreign terrorists." E.O. 13224 provides U.S. authorities an important tool to implement targeted financial sanctions against terrorists and TF facilitators. Designations under E.O. 13224 result in the blocking and freezing of the individual or group's assets that are subject to U.S. jurisdiction. U.S. persons are prohibited from engaging in any transactions with individuals or groups designated under E.O. 13224 except as authorized by Treasury. As of July 2018, over 1,134 individuals and entities are designated as Specially Designated Global Terrorists (SDGTs) under this authority and cut off from the U.S. financial system.

Furthermore, the Secretary of State, in consultation with the Attorney General and the Secretary of the Treasury, has the authority to designate entities as FTOs under Section 219 of the Immigration and Nationality Act if 1) it is a foreign organization; 2) the organization engages in terrorist activity or terrorism or retains the capability and intent to engage in terrorist activity or terrorism; and 3) the terrorist activity or terrorism of the organization threatens the security of U.S. nationals or the national security of the United States. There are 66 designated FTOs as of July 2018, and all are also designated as SDGTs. FTO designations impose financial restrictions similar to those imposed under E.O. 13224, but also carry immigration restrictions, making alien representatives or members of designated groups inadmissible to and in certain circumstances removable from the United States.

The implementation of sanctions programs targeting international terrorist organizations has resulted in the blocking in the United States of approximately $34 million (as of December 31, 2016) in which there exists an interest of an international terrorist organization or other related designated party.[78] Approximately $149 million in assets relating to the three designated state sponsors of terrorism[79] in 2016 has been identified by OFAC as blocked pursuant to economic sanctions imposed by the United States.[80]

However, the imposition of sanctions by the United States and its international partners against terrorists, terrorist organizations, and their support structures is a powerful tool that reaches far

77. See the 2018 NTFRA for other examples of TF enforcement actions.

78. Office of Foreign Assets Control, Department of the Treasury, Terrorist Assets Report, Calendar Year 2016, Twenty-fifth Annual Report to the Congress on Assets in the United States Relating to Terrorist Countries and International Terrorism Program Designees.

79. Iran, Sudan, and Syria.

80. There was a significant reduction in blocked assets between calendar year 2015 and calendar year 2016, primarily because victims of terrorism obtained nearly $2 billion of the blocked assets of terrorist organizations and state sponsors of terrorism during that period as a result of judgments in U.S. courts.

beyond the blocking of terrorist assets. Designating individuals or entities as SDGTs or FTOs notifies the U.S. public and the international community that these parties are either actively engaged in or supporting terrorism, or that they are being used by terrorists and their organizations. Financial sanctions expose and isolate these individuals and organizations, deter would-be donors, and force these groups to expend time and resources to find new sources of revenue and channels for moving these funds. U.S. sanctions are also magnified by the central role of the U.S. dollar in the international financial system, as funds transfers that neither originate from nor are destined for the United States can nevertheless pass through or otherwise touch a U.S. financial institution, a path that is prohibited by the imposition of sanctions and would result in a blocking of funds if pursued.

Beyond the U.S. financial system, these designations help protect the international financial system from terrorist abuse, as banks and other private institutions around the world frequently consult OFAC's Specially Designated Nationals and Blocked Persons (SDN) List and deny listed persons access to their institutions to minimize their own risk. Foreign partners often implement U.S. terrorism designations multilaterally. The U.S. government also proposes certain designations for listing at the relevant UN Security Council sanctions committees.[81] These efforts to "multilateralize" designations and sanctions across the international community are critical to ensuring comprehensive travel bans, asset freezes, and arms embargoes on listed individuals and entities.

A further indicator of the impact of these sanctions is how designation targets react. The United States has seen high-ranking officials within terrorist organizations subject to U.S. sanctions programs struggling to manage the effects of U.S. measures and worrying about additional actions that may be taken against them.

Designations of SDGTs and FTOs enhance the ability of DOJ to prosecute criminal charges relating to financial support and other support provided to terrorists and terrorist organizations. Under E.O. 13224, U.S. persons may not engage in financial transactions with an SDGT unless expressly authorized by statute or by a license issued by OFAC, nor may they engage in a transaction to circumvent the E.O., or make or receive any contribution of funds, goods, or services to or for the benefit of an SDGT. Willful violation of an E.O. or implementing regulations issued pursuant to International Emergency Economic Powers Act (IEEPA) is a criminal offense[82]; consequently, violations of E.O. 13224 are *de facto* TF offenses, and in certain cases DOJ prosecutors can use criminal violations of E.O. 13224 as an alternative to or in conjunction with prosecution under 18 U.S.C. § 2339B. In recent years, DOJ obtained convictions in more than 80 international terrorism and terrorism-related cases, many of which involved provision of material support or resources to an FTO or economic sanctions violations. Similar designation regimes and related criminal prohibitions exist in numerous other countries.

---

81. Specifically, the Security Council Committee Pursuant to Resolutions 1267, 1989, and 2253 (Concerning ISIL (Da'esh), Al-Qaida, and Associated Individuals, Groups, Undertakings and Entities) and the Security Council Committee Pursuant to Resolution 1988 (Concerning the Taliban).

82. See 50 U.S.C. § 1705.

DOJ addresses terrorist financing activity as a fundamental component of DOJ's broader counterterrorism strategy, and there have been several terrorism investigations that benefited from the FBI's close working relationship with major financial institutions. These joint efforts with U.S. financial institutions, where information was sought and obtained using legal process, were coordinated by the Federal Bureau of Investigation-Terrorist Financing Operations Section (FBI-TFOS) and illustrate the financial investigative efforts that are part of all counterterrorism investigations, not just those that focus on possible terrorist financing. In addition to these initiatives, the DOJ utilizes an "all tools" approach, whereby individuals suspected of providing financial or other support to terrorism will be charged with non-terrorism criminal offenses if doing so would disrupt a terrorist support network without jeopardizing ongoing investigative activity.

The FBI Counterterrorism Division's operational priorities are classified. However, the FBI does make public its target figure for terrorism disruptions. The FBI defines a disruption as interrupting or inhibiting a threat actor from engaging in criminal or national security related activity. The FBI set a target of 200 terrorist disruptions for FY 2017 and ended up causing 723 disruptions.[83] Cutting off financing and other forms of support provided to foreign terrorist organizations is one method to disrupt extremist networks.

ISIS leaders and operatives have been aggressively targeted around the world, resulting in the U.S. sanctioning fifteen ISIS branches along with more than 95 ISIS senior leaders, operatives, financial facilitators, recruiters, and affiliated MSBs since 2014. U.S. and UN designations, along with close cooperation between U.S. and Iraqi authorities, have effectively shut down exchange houses that were functioning as key nodes of ISIS's financial facilitation networks, both by exposing their ties to the group and freezing millions of dollars in tainted assets. According to U.S. counterterrorism authorities, ISIS has lost over 97 percent of the territory it once controlled, and its illicit income streams are down.

While the rise of ISIS deprived AQ and its regional affiliates of some supporters and operatives, limited fundraising on behalf of AQ and its regional affiliates continues to occur in the United States. On April 12, 2018, three U.S.-based individuals[84] pleaded guilty to concealing the provision of thousands of dollars to Anwar Al-Awlaki, an SDGT and member of AQAP.[85] As AQ generates almost all of its revenue outside of the U.S., the U.S. government has aggressively utilized financial tools to limit AQ funding streams globally. This includes designating more than 160 individuals affiliated with AQ and other terrorist organizations throughout Afghanistan and Pakistan, more than 70 individuals and entities across the Gulf, and several more in Africa and other countries.

---

83. Department of Justice FY 2017 Annual Performance Report & FY 2019 Annual Performance Plan.

84. Another individual pleaded guilty on July 10, 2017, to one count of conspiracy to provide and conceal material support or resources to terrorists and one count of solicitation to commit a crime of violence. DOJ, Press Release, "Man Pleads Guilty to Conspiring to Provide Material Support to Terrorists and Soliciting the Murder of a Federal Judge," July 10, 2017.

85. Press Release, DOJ, "Three Men Plead Guilty to Concealing Sending Funds to Anwar Al-Awlaki," April 12, 2018, available at https://www.justice.gov/opa/pr/three-men-plead-guilty-concealing-sending-funds-anwar-al-awlaki. Al-Awlaki is confirmed to have died on September 30, 2011, in Yemen.

Hizballah receives support from Iran and uses a far-flung network of companies and brokers to procure weapons and equipment, and clandestinely move funds on behalf of operatives.[86] Hizballah is able to access the international financial system because unlike AQ and ISIS it is not subject to UN sanctions, and many countries have not designated the entirety of Hizballah under their domestic authorities or imposed other restrictions on Hizballah-related financial transactions.

While some foreign governments may take limited action against Hizballah financing, the U.S. government has employed all available tools to disrupt these terrorist networks. With respect to Lebanon, OFAC has sanctioned more than 130 Hizballah-affiliated individuals and entities comprising the group's organizational infrastructure, financial networks, and procurement nodes. FinCEN identified the Lebanese Canadian Bank in 2011 and the Kassem Rmeiti and Halawi Exchanges in 2013 as entities of primary money laundering concern under Section 311 of the USA PATRIOT Act[87] for facilitating money laundering activities for Hizballah. These public findings led the Lebanese government to take action against these institutions and shut down the Lebanese Canadian Bank.

Treasury has also taken action to disrupt Hizballah financial facilitators and procurement networks operating outside of Lebanon. OFAC has designated Hizballah supporters in more than 20 countries, including in the Western Hemisphere, West Africa, and across the Middle East. In FY 2018 alone, Treasury has designated over 25 Hizballah-affiliated individuals and entities—more than any previous year—targeting top Hizballah financiers, Iran's conduits of funding to Hizballah, and included an unprecedented joint designation with our Gulf partners of five members of Hizballah's leadership. For example, in May 2018, OFAC designated Hizballah financier Mohammad Ibrahim Bazzi and five of his companies that funded Hizballah with millions of dollars.

In addition, Treasury is working with its Gulf Cooperation Council (GCC) partners under the auspices of the Terrorist Financing Targeting Center (TFTC) collaboratively to sanction terrorist groups and their financiers. In May 2018, the seven member states of the TFTC designated five senior Hizballah leaders, including Hizballah Secretary General Hassan Nasrallah, and nine other Hizballah financiers and entities.

Furthermore, under E.O. 13224, Treasury designated Hizballah's primary sponsor, the IRGC-QF; the IRGC-QF's commander, Ghasem Soleimani; Bank Saderat, an Iranian institution used to provide tens of millions to Hizballah; and more than 50 other Iran-related persons and entities. Additional designations targeting Iranian terrorist networks have included the then-Governor of the Central Bank of Iran (CBI) (the first designation of a CBI official) and an Iraq-based bank and its chairman for moving millions of dollars on behalf of the IRGC-QF; an extensive currency exchange network in Iran and the United Arab Emirates that procured and transferred millions of dollars in bulk cash to the IRGC-QF; and an Iran- and Germany-based

86. *Id.*

87. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism USA PATRIOT) Act of 2001, Pub. L. 107–56, Oct. 26, 2001.

network that circumvented European export controls and procured advanced equipment and materials to counterfeit Yemeni bank notes potentially worth hundreds of millions of dollars for the IRGC-QF.

These actions targeting Iran's support to Hizballah are one facet of the Administration's effort to exert "maximum pressure" on the Iranian regime until it changes its malign behavior. During this Administration, Treasury's persistent pursuit of the Iranian regime's malign activity has led to the designation of 168 Iran-related persons in 19 tranches. These targeted designations, along with the robust reimposition of nuclear-related sanctions on November 5, 2018, are the toughest sanctions ever imposed on the Iranian regime and are designed to deprive the regime of vital revenue it uses to fund its malign activity around the world. To bolster implementation of Treasury's powerful authorities that provide the ability to target a broad range of activity and sectors of Iran's economy, the President issued E.O. 13846 in August 2018 to not only reimpose relevant provisions of executive orders revoked under the JCPOA, but also to broaden the scope of sanctions in effect prior to the JCPOA.

In addition to the use of our sanctions authorities, Treasury has used the full array of unique financial authorities to carry out this economic pressure campaign. For instance, in October 2018, Treasury issued a comprehensive Iran advisory to alert financial institutions to the risks Iran poses to the international financial system, which will help financial institutions detect and report illicit activity and better understand and avoid exposure to U.S. sanctions. Treasury, in conjunction with the State Department, is also working to bolster international efforts to constrain Iran through diplomatic engagement around the globe. This has included visits to over 30 countries to highlight Iran's illicit business activities, including its use of front and shell companies, counterfeiting currency, and cyberattacks to fund its support for terrorism.

In January 2018, the Attorney General announced the creation of the Hizballah Financing and Narcoterrorism Team (HFNT), a group of experienced international narcotics trafficking, terrorism, organized crime, and money laundering investigators and prosecutors. HFNT prosecutors and investigators are tasked with investigating individuals and networks providing support to Hizballah, and pursuing prosecutions in any appropriate cases. The HFNT will begin by assessing the evidence in existing investigations, including cases stemming from Project Cassandra, a DEA-led law enforcement initiative targeting Hizballah's drug trafficking and related operations.[88]

DEA's Project Cassandra targets a global Hizballah network responsible for the movement of large quantities of cocaine in the United States and Europe. This global network, referred to by DEA as Hizballah's External Security Organization Business Affairs Component (BAC), currently operates under the control of SDGTs Abdallah Safieddine and Adham Tabaja. Members of the BAC have allegedly established business relationships with South American drug cartels responsible for supplying large quantities of cocaine to the European and U.S. drug markets. The

88. DOJ, Press Release, "Attorney General Sessions Announces Hezbollah Financing and Narcoterrorism," January 11, 2018, available at https://www.justice.gov/opa/pr/attorney-general-sessions-announces-hezbollah-financing-and-narcoterrorism-team.

BAC launders a significant volume of drug proceeds as part of a trade based money laundering scheme known as the Black Market Peso Exchange.[89]

Countering Proliferation Financing

The U.S. government wields a variety of tools and authorities to detect and combat PF. Interagency coordination is essential and involves a variety of measures, ranging from global sanctions and other financial authorities utilized to target PF and support networks to domestic actions taken by law enforcement to investigate, prosecute, and pursue the forfeiture of PF-derived proceeds. Financial regulators are also involved in monitoring private sector compliance with U.S. regulations designed to combat various types of illicit finance, a process that involves regular supervisory reviews and occasionally taking enforcement action against institutions that run afoul of these regulations, when appropriate. Coordinated outreach from all of these departments and agencies to the private sector and communication with international partners is also a key component that helps to inform and refine actions taken and provide these stakeholders with necessary information to help better combat PF threats.

Financial and Regulatory Efforts

As part of the broader post-September 11, 2001, national security reform efforts, the U.S. government focused increasingly on the importance of disrupting the finances and funding networks that fueled various national security threats and on the importance of financial intelligence collected and disseminated by U.S. financial institutions. Terrorism and Financial Intelligence (TFI) was established in 2004 to lead the U.S. government's counter-illicit financing efforts, including efforts to combat PF. TFI seeks to mitigate PF risk through both systemic and targeted actions, bringing various capabilities to bear to exploit financial intelligence, impose economic sanctions on PF networks, engage private sector entities and foreign partners, and take regulatory actions to protect the U.S. financial system from abuse.

Targeted actions, usually in the form of targeted financial sanctions administered and enforced by OFAC, are used to identify, disrupt, and prevent weapons of mass destruction (WMD) proliferators from accessing the U.S. financial system. OFAC and the State Department use authorities granted to them through legislation and under various executive orders to designate and identify WMD proliferators and their support networks. Once designated or identified, OFAC regulations require U.S. persons—including financial institutions—to block (freeze) the property, including financial assets, of the targets. E.O. 13382[90] is the principal authority used to target WMD proliferators and their support networks worldwide, but OFAC can also utilize various

89. DEA, Press Release, DEA and European Authorities Uncover Massive Hizballah Drug and Money Laundering Scheme, February 1, 2016, available at https://www.dea.gov/divisions/hq/2016/hq020116.shtml.

90. E.O. 13382 (2005), among other things, blocks the property of persons engaged in proliferation activities and their support networks. The establishment of such an authority was a key recommendation of the 2005 report from the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction (the "Silberman-Robb Commission"), which concluded that Treasury should possess equally robust authorities to target WMD proliferation activity as the Department had for targeting terrorism (E.O. 13224).

authorities granted under specific country sanctions programs, such as those targeting North Korea.[91] As of July 2018, 387 individuals and entities were designated pursuant to E.O. 13382.[92]

FinCEN also has its own targeted authorities it can utilize to protect the U.S. financial system from abuse. Under Section 311 of the USA PATRIOT Act, FinCEN can determine that a foreign jurisdiction, financial institution, class of transaction, or type of account is of "primary money laundering concern" and can impose a variety of regulatory measures that trigger a number of obligations for U.S. financial institutions when dealing with the subject of these actions. These "special measures" range from increased recordkeeping and reporting requirements for transactions associated with the target to a complete prohibition on opening correspondent accounts for the target. Since November 2016, FinCEN has taken action under Section 311 three times. In all three cases, the target has been connected to PF activity (all related to North Korea) and in each case FinCEN proposed a prohibition under the "fifth special measure" on U.S. financial institutions opening or maintaining correspondent banking accounts for the targets, as well as the application of special due diligence to their foreign correspondent accounts that is reasonably designed to guard against their indirect use to process transactions involving these targets.[93]

These actions are complemented by the efforts of FinCEN and the federal functional regulators that evaluate and enforce financial institutions' compliance with the appropriate regulatory requirements. For example, as administrator of the BSA, FinCEN promulgates implementing regulations for the BSA to reduce the potential for abuse by various illicit finance threats, including PF. To develop these regulations, FinCEN and other offices within TFI regularly engage all the appropriate stakeholders to understand these threats. FinCEN works with the federal functional regulators and law enforcement to develop guidance, administrative rulings, and advisories for the financial industry to aid financial institutions in identifying priority threats, such as PF.

For their part, the federal functional regulators regularly examine the financial institutions they supervise for compliance with BSA/AML program requirements and OFAC obligations, as well as the reporting and recordkeeping requirements of the BSA. The functional regulators also have a range of formal and informal enforcement authority to address significant violations that may be identified through their supervisory activities. The combination of a strong AML/CFT framework and effective supervision makes it more difficult for proliferators and their facilitators to access the U.S. financial system.

---

91. For example, at the time of writing, there were six separate Executive Orders targeting North Korea: 13466, 13551, 13570, 13687, 13722, and 13810.

92. See Specially Designated Nationals And Blocked Persons List, available at https://www.treasury.gov/resource-center/sanctions/SDN-List/Pages/default.aspx.

93. See (1) Nov. 2016 Section 311 final rule for the entire jurisdiction of North Korea; (2) Nov. 2017 Section 311 final rule targeting the China-based Bank of Dandong for facilitating millions of dollars of transactions for companies tied to the DPRK weapons programs; and (3) Feb. 2018 Section 311 finding and notice of proposed rulemaking targeting Latvia-based ABLV Bank for institutionalized money laundering practices, including processing transactions for parties connected to UN-designated entities involved in North Korea's procurement or export of ballistic missiles. All available at https://www.fincen.gov/resources/statutes-and-regulations/311-special-measures.

FinCEN also serves as the U.S. government's central repository for suspicious activity reporting on potential proliferation financing activity, which it makes available to state, local, tribal, and federal law enforcement agencies across the country. When necessary, FinCEN also makes use of its regulatory authorities under the BSA to obtain targeted information from financial institutions on proliferation finance-related matters. This information may be used in a variety of efforts to target threats, inform regulatory policy, or engage and educate stakeholders such as financial institutions and foreign partners.

Additionally, U.S. government counter-PF initiatives have benefited from and contributed to long-standing efforts to protect the U.S. financial system against all forms of illicit finance. These laws, rules, regulations, and guidance have aided financial institutions in identifying and mitigating risk, provided valuable information to law enforcement, and created the foundation of financial transparency required to deter, detect, and punish those who would abuse the U.S. financial system to launder the proceeds of crime and move funds for illicit purposes. For example, controls instituted to combat money laundering and terrorist financing have also strengthened the U.S. government's ability to identify, deter, and disrupt PF.

Law Enforcement Efforts

Law enforcement agencies play a critical role in U.S. counter-PF efforts. The DOJ is the principal government entity responsible for overseeing the investigation and prosecution of PF offenses at the federal level. Specifically, the National Security Division's (NSD) CES supervises and coordinates these efforts across the country, ensuring that these cases are given the appropriate amount of attention and resources. CES, in partnership with the U.S. Attorneys' offices and other law enforcement agencies, investigates and dismantles PF networks, which have sought to exploit the U.S. financial system. DOJ's ability to bring federal charges and asset forfeiture claims against PF facilitators and front companies is a critical aspect of the U.S. Government's effort to counter PF activity in the U.S. A public charging document not only serves a criminal deterrent purpose, but can also be shared with private sector stakeholders, which are then able to act based on that information.

These actions would not be possible without the investigative efforts of key federal law enforcement agencies, such as the FBI and Commerce's Bureau of Industry and Security (BIS), which specializes in export control violation cases. In fact, in recognition of the threat facing the U.S. from nation-states' efforts to acquire WMD, the proliferation of advanced weapons technology worldwide, and attempts by terrorist groups to obtain WMD or advanced weapons technology, the FBI combined three counterproliferation-related components into a single jointly managed entity at FBI Headquarters—the Counterproliferation Center (CPC)—to disrupt global proliferation networks.[94] The creation of the CPC has resulted in an expanded counterproliferation mandate and enhanced coordination among various related components, including agents, analysts, and professional staff. The CPC mission is to lead the FBI's efforts to identify, deny,

94. The three components comprising the CPC are (1) the WMD Directorate, which provides scientific expertise; (2) the Counterintelligence Division, which provides operational expertise; and (3) the Directorate of Intelligence, which provides analytical expertise. See https://www.fbi.gov/about/leadership-and-structure/national-security-branch/fbi-counterproliferation-center.

disrupt, and exploit attempts to obtain or divert embargoed, export-controlled, or otherwise sensitive technologies or activities related to WMD, missile delivery systems, space or conventional weapons systems, or dual-use components. In order to accomplish its mission, the CPC works to identify, penetrate, mitigate, and disrupt proliferation networks that are engaged in efforts to acquire and utilize WMD and critical controlled U.S. technologies and, in doing so, often works to identify and understand the financing tactics these networks employ.

Similarly, BIS works to advance U.S. national security objectives by ensuring an effective export control system. In addition to managing the export control regulatory framework, BIS's Export Enforcement (EE) division works to mitigate the risk of sensitive exports reaching hostile entities or those that engage in onward proliferation through the use of both preventative and investigative methods. These methods include applying law enforcement and export control expertise to prevent and deter exports of the most sensitive items to illicit end-users and to embargoed destinations. BIS's Export Enforcement BIS's Export Enforcement works closely with other federal law enforcement agencies, including the FBI and the DHS, to conduct investigations or preventative actions, as well as with DOJ to investigate and potentially bring criminal charges.[95] BIS lends key expertise regarding controlled goods and technology and works with other agencies to track efforts by PF networks to finance illicit procurement.

Countering Money Laundering

The DOJ charged, on average, 2,257 defendants with money laundering (18 U.S.C. §§ 1956 or 1957) each year between FY 2015 and FY 2017 (see Figures 1 through 12 for additional prosecution statistics). This is slightly below figures from FYs 2012–2014, during which an average of 2,509 defendants were charged each year with money laundering.

Since 2010, there has been a steady decrease in the gross amount of bulk cash seizures throughout the United States reported to Bulk Cash Smuggling Center (BCSC). The decrease in seizures could indicate that TCOs are using other, more discreet, methods of moving illicit money such as TBML, or it could indicate that law enforcement is targeting other money laundering-related activities away from the borders. Nonetheless, in FY 2016, Homeland Security Investigations (HSI) arrested 575 individuals and seized more than $66.3 million associated with bulk cash smuggling.[96]

There have been a number of large-scale, precedent-setting prosecutions combating illicit finance in recent years.

Drug Money Laundering

The first nationwide undercover operation to target vendors of illicit goods on the Darknet began in 2017, and led to 90 active investigations around the country and the arrest and impending prosecution of more than 35 Darknet vendors, some of whom have been charged with money

95. See BIS, *Enforcement*, available at https://www.bis.doc.gov/index.php/enforcement.

96. See ICE, *Bulk Cash Smuggling Center*, available at https://www.ice.gov/bulk-cash-smuggling-center.

laundering involving the exchange of drug distribution proceeds in the form of bitcoin for U.S. currency. The effort involved the participation of HSI, UUSSS, the U.S. Postal Inspection Service and DEA, as well as prosecutors from DOJ's Money Laundering and Asset Recovery Section (MLARS) and 40 U.S. Attorney's Offices. As alleged, more than 50 Darknet vendor accounts were identified and attributed to the real individuals selling illicit goods on Darknet market sites such as Silk Road, AlphaBay, Hansa, Dream, and others. Law enforcement, including HSI's New York Field Division, federal prosecutors, and MLARS coordinated to investigate 65 targets identified by an undercover operation in more than 50 federal districts.[97]

The United States has also utilized OFAC sanctions programs to apply economic sanctions against significant narcotics traffickers under the Kingpin Act (21 U.S.C. §§ 1901–1908 and 8 U.S.C. § 1182) and against significant transnational criminal organizations (TCOs) under E.O. 13581, thereby freezing their U.S. assets, including financial accounts and real properties, and denying their access to the U.S. financial system. To date, OFAC has designated 12 TCOs and more than 200 targets related to those TCOs. Since 2000, OFAC has worked with the interagency to investigate and identify 118 significant foreign narcotics traffickers ("drug kingpins") for sanctions, and designated more than 2,000 companies and individuals around the world under dozens of sanctions investigations related to those drug kingpins. More than 950 (almost half) of the foreign persons targeted under the Kingpin Act are Mexican drug cartels and their networks.

Consumer Fraud

DOJ also initiated a series of groundbreaking, multi-district prosecutions targeting an international fraud and money laundering network that victimized tens of thousands of individuals in the United States through fraudulent schemes that resulted in hundreds of millions of dollars in losses.[98] Charges were filed against 56 individuals and five Indian companies. Since October 2016, 24 defendants have been convicted of conspiracy charges involving wire fraud, money laundering, and identity fraud, as well as two related convictions for naturalization fraud and passport fraud. Thirty-two additional defendants are located in India and the United States is pursuing their arrests.

As alleged, the scheme involved a network of call centers in India that used information obtained from data brokers and other sources to identify potential victims who were told by callers impersonating officials from the IRS or U.S. Citizenship and Immigration Services that they faced arrest, imprisonment, fines, or deportation if they did not pay taxes or penalties to the government. If the victims agreed to pay, the call centers would then immediately turn to a network of U.S.-based co-conspirators to liquidate and launder the extorted funds as quickly as possible through wire transfers or by purchasing prepaid debit cards that were registered using

97. See DOJ, Press Release, "First Nationwide Undercover Operation Targeting Darknet Vendors Results in Arrests of More Than 35 Individuals Selling Illicit Goods and the Seizure of Weapons, Drugs and More Than $23.6 Million," available at https://www.justice.gov/opa/pr/first-nationwide-undercover-operation-targeting-darknet-vendors-results-arrests-more-35.

98. See *United States v. HGlobal et al.* (Victim Impact Statement), available at https://www.justice.gov/usao-sdtx/victim-witness-program/us-v-hglobal.

stolen identity information. The wire transfers also involved the use of fraudulent identification information.

The case had a significant impact in reducing fraud in the United States, with the Treasury Inspector General reporting that in the months following the October 2016 arrests, the average number of reported scam calls dropped from as much as 45,000 calls and 300 new victims a week to 2,500 calls and 20 victims a week.[99]

In June 2018 federal authorities announced[100] the culmination of a large-scale, multinational investigation into business e-mail compromise schemes, also known as cyber-enabled financial fraud. The investigation, which involved participation from DHS, DOJ, Treasury, and the U.S. Postal Inspection Service, resulted in 74 arrests, including 42 in the United States, 29 in Nigeria, and one in Canada, Mauritius, and Poland each. Authorities seized almost $2.4 million. Local authorities, participating with federal law enforcement, charged 15 alleged money mules for their role in defrauding victims. See the 2018 NMLRA for more information on money mules and for other examples of enforcement actions.

Health Care Fraud

The largest health care fraud enforcement action to date occurred in June 2018 with 601 defendants charged, including 165 doctors, nurses and other licensed medical professionals, for their alleged participation in health care fraud and money laundering schemes involving more than $2 billion in false billings. Of those charged, more than 162 defendants, including 76 doctors, were also charged for their roles in prescribing and distributing opioids and other dangerous narcotics.[101] In FY 2017, DOJ opened 967 new criminal health care fraud investigations, filed criminal charges in 439 cases involving 720 defendants, and secured convictions against 639 defendants for health care fraud-related crimes.[102]

Transnational Criminal Organizations

On February 9, 2017, President Donald J. Trump issued E.O. 13773, which directed the federal government to "ensure that Federal law enforcement agencies give a high priority and devote sufficient resources to efforts to identify, interdict, disrupt, and dismantle transnational criminal organizations[.]" It directs federal agencies to make combating TCOs a priority line of effort, develop new strategies to counter TCOs, and increase information sharing and international

---

99. See DOJ, *Criminal Division*: *Performance Budget FY 2019 Congressional Submission*, available at https://www.justice.gov/jmd/page/file/1034256/download.

100. See DOJ, Press Release, "74 Arrested in Coordinated International Enforcement Operation Targeting Hundreds of Individuals in Business Email Compromise Schemes," June 11, 2018, available at https://www.justice.gov/opa/pr/74-arrested-coordinated-international-enforcement-operation-targeting-hundreds-individuals.

101. See DOJ, Press Release, "National Health Care Fraud Takedown Results in Charges against Over 412 Individuals Responsible for $1.3 Billion in Fraud Losses," July 13, 2017, available at https://www.justice.gov/opa/pr/national-health-care-fraud-takedown-results-charges-against-over-412-individuals-responsible.

102. See DOJ, Press Release, "Department of Justice and Health and Human Services Return $2.6 Billion in Taxpayer Savings from Efforts to Fight Healthcare Fraud," April 6, 2018, available at https://www.justice.gov/opa/pr/department-justice-and-health-and-human-services-return-26-billion-taxpayer-savings-efforts.

partnership efforts. The Attorney General also established an interagency Transnational Organized Crime Task Force in October 2018 and has designated the following criminal groups as top transnational organized crime threats: MS-1; Cartel de Jalisco Nueva Generación (CJNG); Sinaloa Cartel; Clan del Golfo, and Lebanese Hezbollah.

In response to Eurasian organized crime, notably, on December 2017 OFAC designated the Thieves-in-Law, along with 10 individuals and two entities, pursuant to E.O. 13581, which targets significant groups and their supporters.[103] In 2017, DOJ settled a money laundering and civil forfeiture action associated with a $230 million tax refund fraud scheme committed by Russian organized crime against the Russian treasury. In a complex series of transactions, the $230 million was laundered through bank accounts in Russia and other countries, with a portion of the funds used to buy real estate in Manhattan.[104] The company accused of laundering the fraud proceeds agreed to pay $5.9 million.

On August 6, 2018, the Secretary of the Treasury submitted its first unclassified report to congress describing interagency efforts in the United States to combat illicit finance related to the Russian Federation.[105] In addition to other illicit finance issues, the report addresses Russia's links to Transnational Organized Crime and those linkages to the U.S. and global economy. The report also highlights how Russian malign actions have exploited lax controls in Latvia's financial sector and noted the action taken by FinCEN in February 2018, pursuant to Section 311 of the USA PATRIOT Act to issue a notice of proposed rulemaking against ABLV Bank, a Latvian bank it found had facilitated large-scale illicit activity connected to Azerbaijan, Russia, and Ukraine. This action identified a key access point being exploited by illicit Russian actors to access the international banking system.[106]

---

103. Treasury, Press Release, "Treasury Targets the "Thieves-in-Law" Eurasian Transnational Criminal Organization," December 22, 2017, available at *https://home.treasury.gov/news/press-releases/sm0244*.

104. DOJ, Press Release, May 12, 2017, available at https://www.justice.gov/usao-sdny/pr/acting-manhattan-us-attorney-announces-59-million-settlement-civil-money-laundering-and.

105. Report to Congress Pursuant to Section 243 of the Countering America's Adversaries Through Sanctions Act of 2017 Regarding Interagency Efforts in the United States to Combat Illicit Finance Relating to the Russian Federation, August 6, 2018, available at https://home.treasury.gov/sites/default/files/2018-08/U_CAATSA_243_Report_FINAL.pdf.

106. Federal Register, February 16, 2018, available at https://www.fincen.gov/sites/default/files/federal_register_notices/2018-02-16/2018-03214.pdf.

STATISTICS ON MONEY LAUNDERING AND RELATED PROSECUTIONS

Figure 1

Defendants Charged with Money Laundering (18 U.S.C. § 1956)

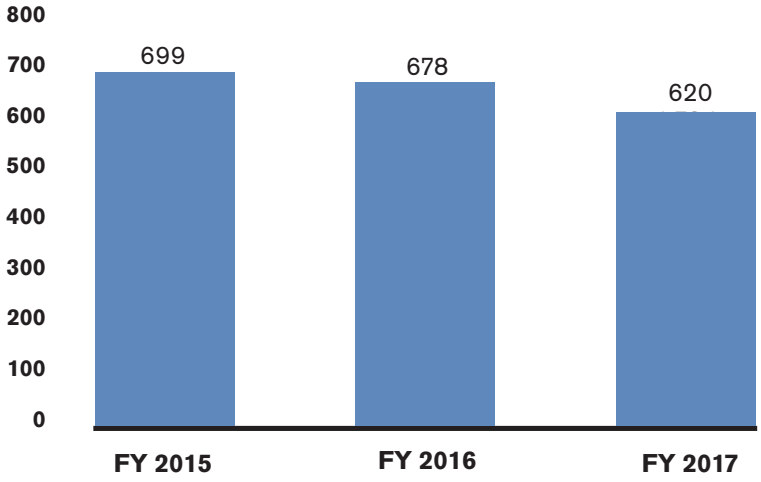
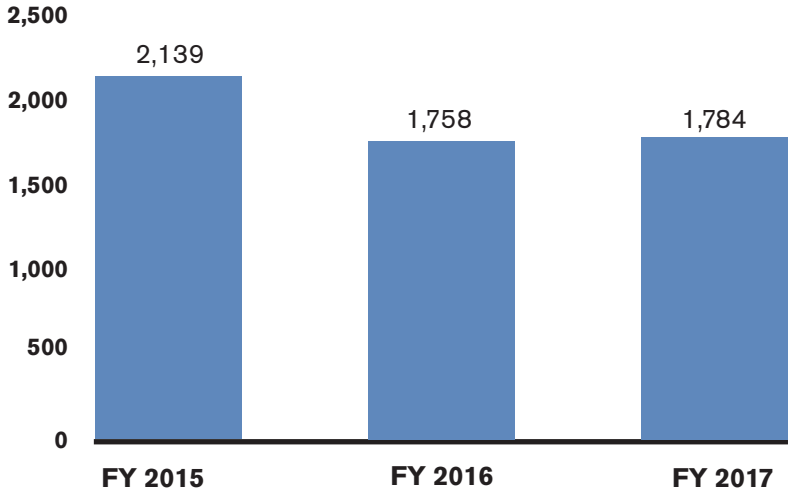


Figure 2

Defendants Charged with Money Laundering (18 U.S.C. § 1956)



Possible charges under 18 U.S.C. § 1956 include:

- § 1956(a)(1)(A)(i): intent to promote the carrying on of specified unlawful activity;
- § 1956(a)(1)(A)(ii): intent to engage in tax evasion or tax fraud;
- § 1956(a)(1)(B)(i): knowledge that the transaction was designed to conceal or disguise the nature, location, source, ownership or control of proceeds of the specified unlawful activity; or
- § 1956(a)(1)(B)(ii): knowledge that the transaction was designed to avoid a transaction reporting requirement.

Figure 3

Cases Charging Money Laundering Conspiracy (18 U.S.C. § 1956(h))

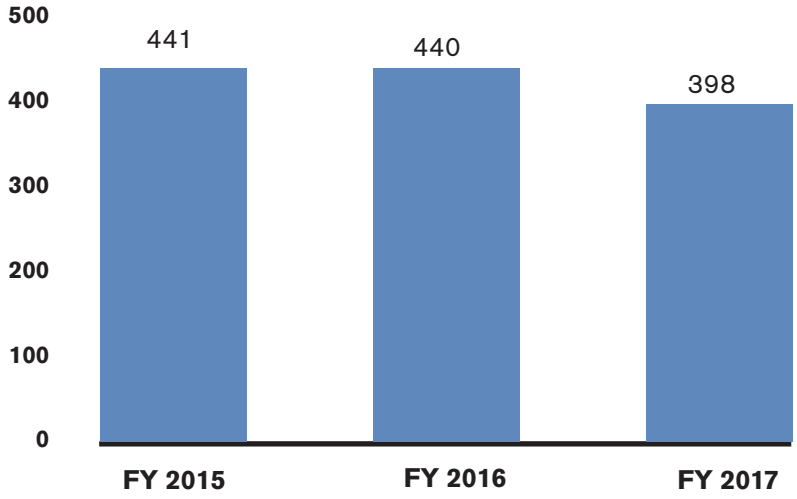


Figure 4

Defendants Charged with Money Laundering Conspiracy (18 U.S.C. § 1956 (h))

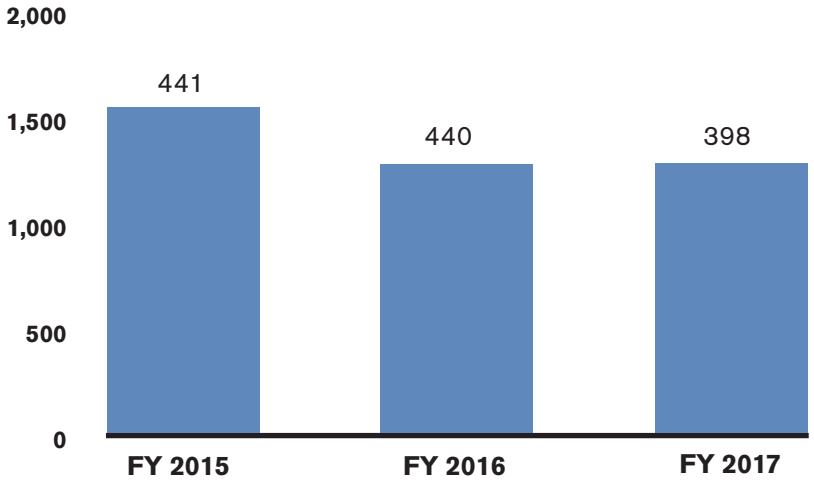


Figure 5

Cases Charging Money Laundering (18 U.S.C. § 1957)

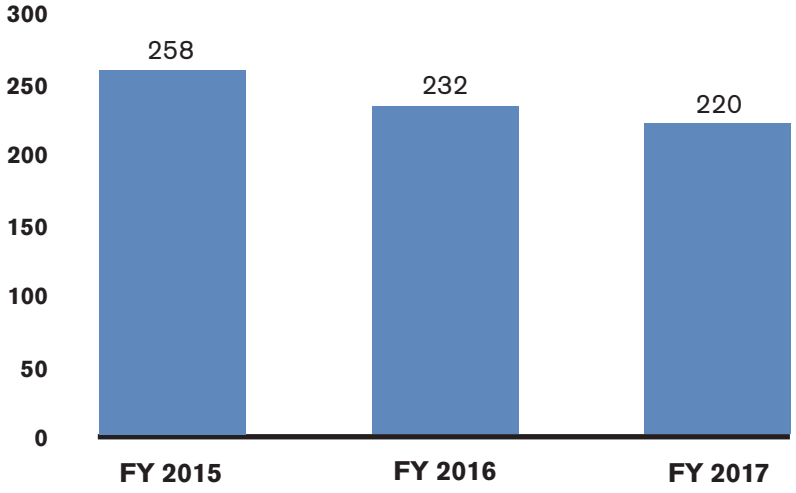


Figure 6

Prosecutions under 18 U.S.C. § 1957 arise when the defendant knowingly conducts a *monetary* transaction in criminally derived property in an amount greater than $10,000, which is in fact proceeds of a specified unlawful activity.

Defendants Charged with Money Laundering (18 U.S.C. § 1957)

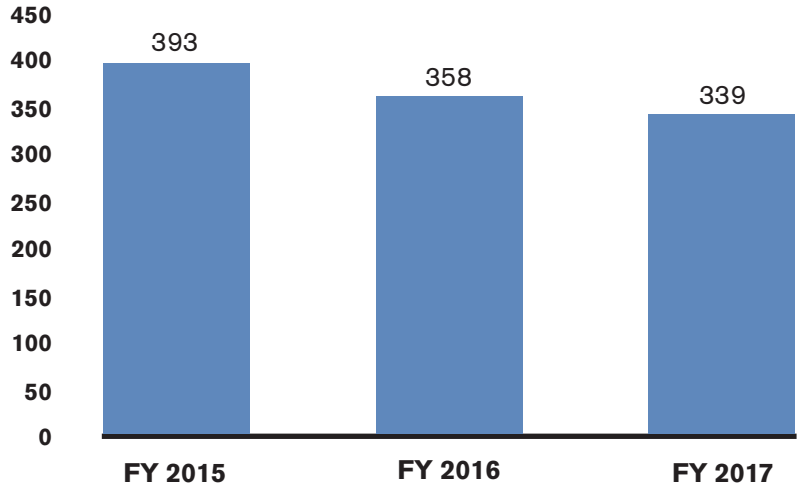


Figure 7

Cases Charging Operating an Unlicensed Money Transmitting Business
(18 U.S.C. § 1960)

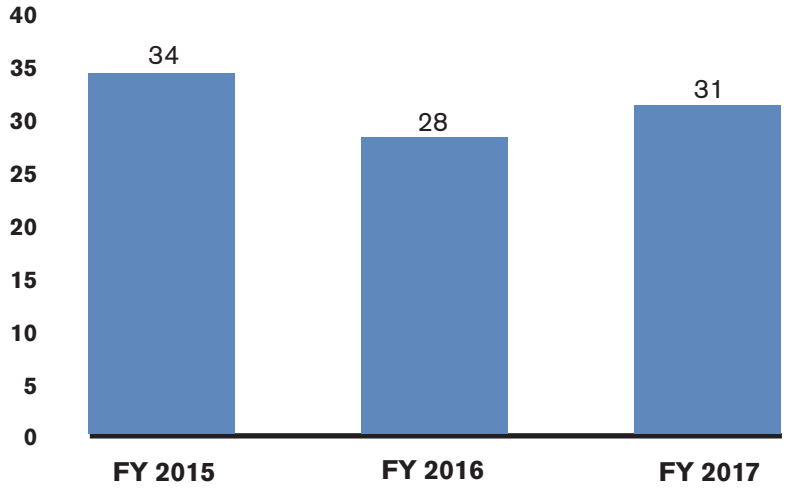


Figure 8

Defendants Charged with Operating an Unlicensed Money Transmitting Business
(18 U.S.C. § 1960)

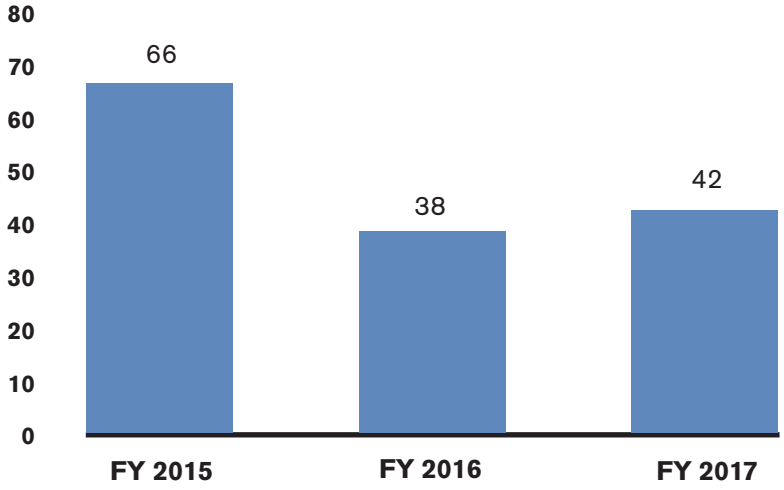


Figure 9

Cases Charging Bulk Cash Smuggling (31 U.S.C. § 5332)

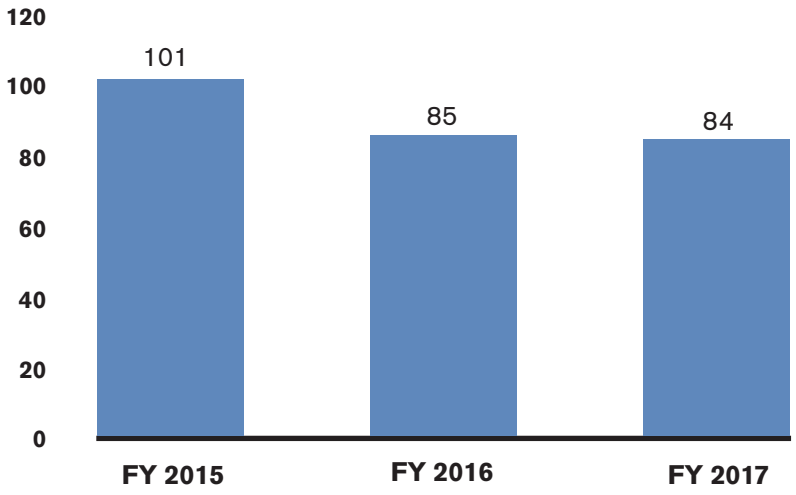


Figure 10

Defendants Charged with Bulk Cash Smuggling (31 U.S.C. § 5332)

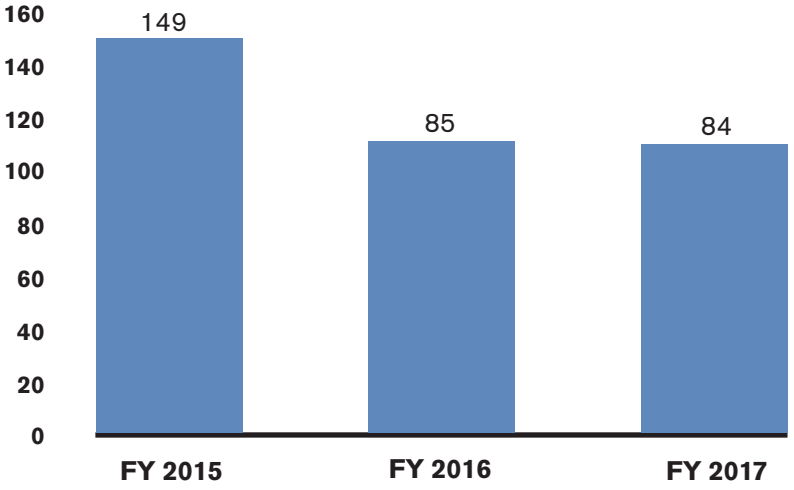


Figure 11

Cases Charging Structuring (31 U.S.C. § 5324)

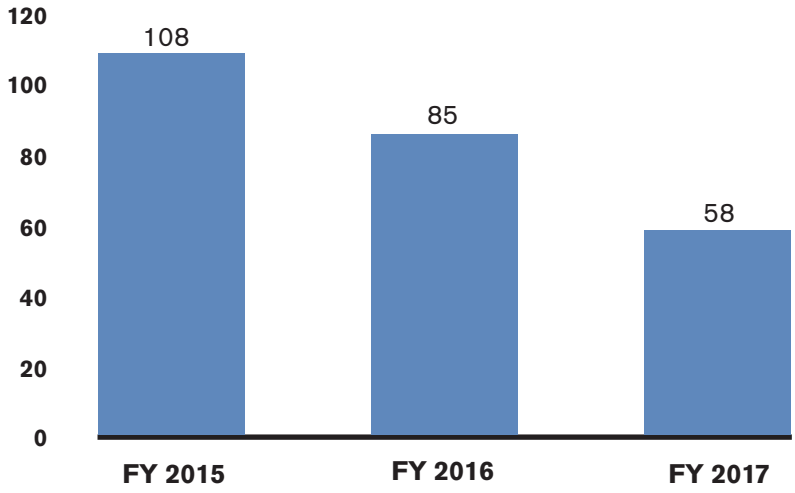
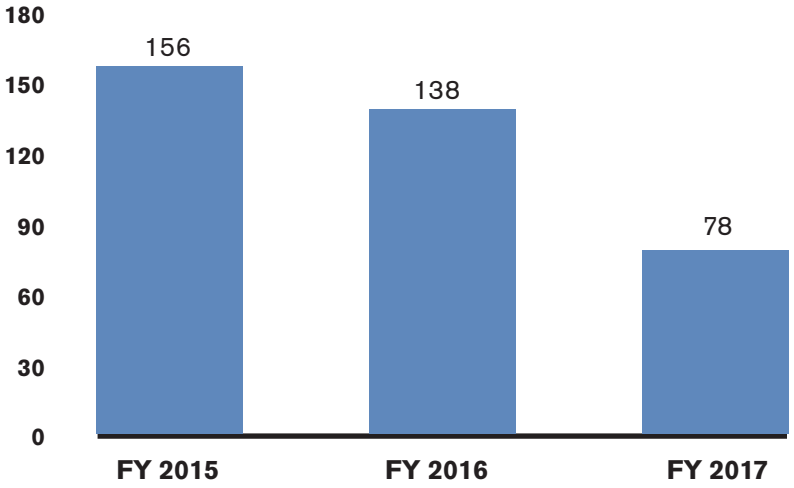
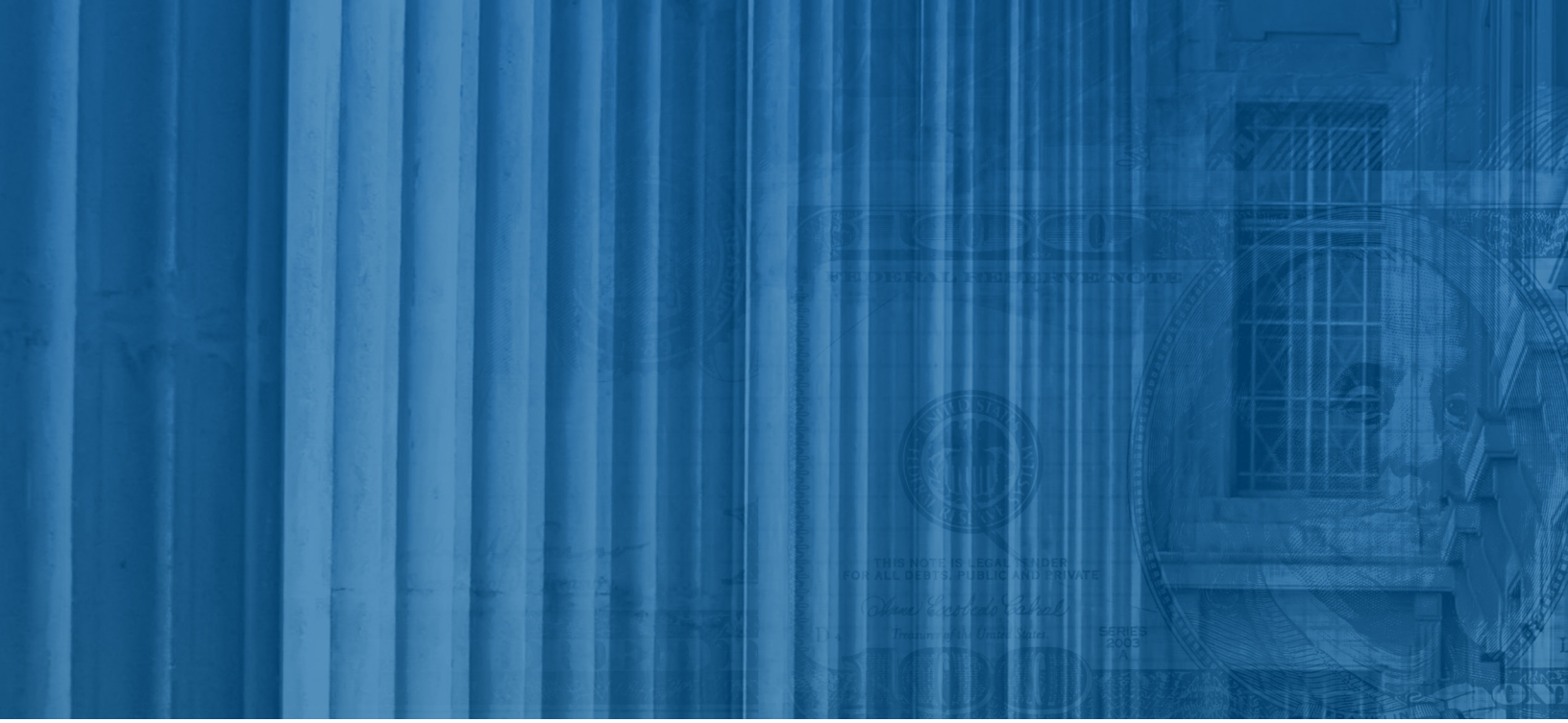


Figure 12

Defendants Charged with Structuring (31 U.S.C. § 5324)





SECTION 5.
INTERAGENCY COORDINATION AND INTERGOVERNMENTAL COOPERATION

Interagency Coordination

As noted previously, TFI's core mission focuses on countering illicit finance by utilizing Treasury's unique expertise, access to financial intelligence, and authorities, including financial sanctions and regulatory enforcement actions, to disrupt and disable terrorists, criminals, WMD proliferators, and other national security threats to the United States and to protect the U.S. and international financial systems from misuse. TFI utilizes its specialized expertise to play a key coordinating role among various US departments and agencies to implement U.S. policy in this area. This coordination occurs within the context of overall policy direction articulated by the Administration, principally through the National Security Council (NSC).

In addition to the day-to-day coordination and cooperation among U.S. departments and agencies, the USG has established a number of formal coordinating mechanisms intended to draw expertise and authorities from across the USG to address specific national security threats. Elements of these mechanisms focus on and help to address illicit finance threats in the areas of TF, PF, and ML and are described briefly as follows.

Counter Terrorism Financing Coordination

Following the September 11, 2001, terrorist attacks, the U.S. government embarked on a sustained effort to prevent terrorism, both at home and abroad, and disrupting terrorist financing has been integral to that effort. U.S. authorities improved their ability to investigate and prosecute terrorist financers by reorganizing law enforcement to more effectively target terrorist financiers, better utilizing existing legal tools and authorities to improve identification of sources of TF, enacting new legal authorities, and strengthening interagency cooperation to identify terrorists and counter TF.

The **Terrorist Financing Operations Section** (TFOS) was established within the FBI in March 2002 to identify and disrupt all TF activities.[107] FBI-TFOS is specifically charged with centralizing the FBI's investigative efforts on TF facilitators and ensuring financial investigative techniques are used to enhance FBI Counter Terrorism investigations. As part of these efforts, TFOS regularly exploits BSA data, including SARs, Currency Transaction Reports (CTRs), and other information provided by financial institutions, both to identify new targets for investigations and to bolster current investigations.

The **National Joint Terrorism Task Force** (NJTTF) was established in 2002 to manage and improve information sharing among the 104 local FBI-led JTTFs. The task forces are based in 104 cities nationwide, including at least one in each of the FBI's 56 field offices. The JTTFs include approximately 4,000 members nationwide with participation from more than 500 state and local agencies and 55 federal agencies.

107. See Office of the Inspector General, Department of Justice, "Audit of the Federal Bureau of Investigation's and the National Security Division's Efforts to Coordinate and Address Terrorist Financing," Audit Report 13–17, March 2013.

The **Counter-Narcoterrorism Operations Center** (CNTOC) is contained within the DEA-led Special Operations Division, which is a multi-agency operational coordination center. The CNTOC coordinates all DEA investigations and intelligence related to narcoterrorism and money laundering linked to terrorist organizations. FBI-TFOS has agents embedded within the CNTOC.

The **National Counter Terrorism Center** (NCTC) integrates and analyzes all intelligence pertaining to terrorism possessed or acquired by the U.S. government (except purely domestic terrorism); serves as the central and shared knowledge bank on terrorism information; provides all-source intelligence support to government-wide counterterrorism activities; and establishes the information technology systems between the NCTC and other agencies to enable integration, dissemination, and use of terrorism information. NCTC is the principal advisor to the Director of National Intelligence (DNI) on intelligence operations and analysis relating to counterterrorism.

Counter Proliferation Financing Coordination

The U.S. Government controls exports of sensitive equipment, software, and technology as a means to protect our national security, and seeks to prevent proliferation of weapons and technologies, including weapons of mass destruction, to problem end-users and supporters of international terrorism. A number of federal departments and agencies play central roles in coordinating interagency cooperation to combat proliferation and proliferation financing.

The **Counterproliferation Center** (CPC) at the FBI combined three counterproliferation-related components into a single, jointly-managed entity at FBI Headquarters to disrupt global proliferation networks. The creation of the CPC has resulted in enhanced coordination among various related components within FBI. The Center also plays a key role in interfacing with other USG departments with a counterproliferation mission.

Counter-Proliferation Task Forces (CPTF) exist in certain U.S. Attorney's offices to enhance cooperation among all agencies involved in export control, forge relationships with affected industries, and facilitate information sharing to prevent illegal foreign acquisition of U.S. technology.

The **Counterintelligence and Export Control Section** (CES) is part of DOJ NSD and supervises and coordinates PF-related prosecutorial efforts across the country, ensuring that these cases are given the appropriate amount of attention and resources.

The **Office of Export Enforcement**, which is located within the Bureau of Industry and Security (BIS) at the Department of Commerce (Commerce), has direct access to FinCEN's BSA data, works cooperatively with the export community, and conducts investigations to support criminal and administrative sanctions. BIS is also responsible for developing lists that financial institutions can use to identify transactions that may involve WMD proliferation financing, including the *Denied Persons List, Entity List,* and *Unverified List*.

The **Export Enforcement Coordination Center** (E2C2) was established by E.O. 13558. E2C2 is led by HSI on behalf of DHS. The Center serves as the enforcement de-confliction hub for all U.S. agencies with a role in export enforcement. E2C2 maximizes information sharing, consistent with national security and applicable laws. This helps partner agencies detect, prevent, disrupt, investigate, and prosecute violations of U.S. export control laws.

The **National Counter-Proliferation Center** (NCPC) is part of the Office of the Director of National Intelligence (ODNI) and works with all U.S. intelligence agencies to identify and address key intelligence gaps. NCPC works to promote strengthened intelligence community efforts to understand and help address the financial aspect of proliferation.

The **Counter-Proliferation Investigations Program** (CPI) at DHS is housed within HSI, which is responsible for overseeing a broad range of investigative activities related to export violations, including the enforcement of U.S. laws related to the export and illicit transshipment of military items and controlled dual-use goods, as well as violations related to sanctioned or embargoed countries such as Iran. The CPI priority programs address trafficking in WMD materials, sensitive dual-use commodities, and technologies sought by proliferant countries and terrorist groups.

The **National Export Enforcement Coordination Network** (NEECN) was created in 2007 within the CPI program to coordinate and de-conflict intelligence community and U.S. federal law enforcement efforts to combat foreign adversaries from obtaining single-use munitions and dual-use technology, including WMD components.

Anti-Money Laundering Coordination

The **High Intensity Drug Trafficking Areas** (HIDTA) program is a grant program that has been administered and funded by the Office of National Drug Control Policy (ONDCP). The HIDTA program assists federal, state, local, and tribal law enforcement operating in areas determined to be critical drug trafficking regions of the United States. HIDTA funds more than 800 distinct law enforcement initiatives developed to identify and disrupt/dismantle drug trafficking organizations and money laundering organizations; reduce drug-related crime and violence; and identify and respond to emerging drug trends. The initiatives are collocated in 29 regional HIDTA programs across the United States and each initiative is linked electronically to the HIDTA Investigative Support Center. The FY 2019 President's Budget proposes to transfer the HIDTA Program from the ONDCP to DEA for the purpose of facilitating coordination of the program with other drug enforcement assets.

OCDETF coordinates law enforcement task forces combining federal, state, and local agencies focused on dismantling high-priority drug trafficking, money laundering, violent, and/or transnational criminal organizations. The OCDETF Fusion Center collects and analyzes drug and related financial investigative information and intelligence from a variety of sources to support OCDETF's coordinated, multi-jurisdictional investigations.

The **National Bulk Cash Smuggling Center** (BCSC), led by HSI, collects and analyzes cash seizure data from federal, state, and local law enforcement agencies operating throughout the

United States. BCSC provides tactical intelligence and expertise to support the investigation of bulk cash smuggling.

The **El Paso Intelligence Center** (EPIC), operated by DEA, collects and analyzes cash seizure data from interdictions along the southwestern U.S. border. The EPIC Bulk Currency Unit (EBCU) is a joint collaboration between HSI and DEA that facilitates sharing bulk cash interdiction and seizure information in support of bulk currency investigations. The EBCU provides uniformity in bulk currency accounting practices and ensures that EPIC's National Seizure System receives comprehensive reporting of bulk currency seizure data.

The **El Dorado Task Force** (EDTF) is comprised of analysts, law enforcement agents, and prosecutors from approximately 32 federal, state, and local law enforcement agencies working together to target financial crime and money laundering in the New York and New Jersey metropolitan area. El Dorado is funded by the New York/New Jersey HIDTA and led by HSI. El Dorado currently has 13 teams of investigators coordinating on a number of active investigations.

The **Health Care Fraud and Abuse Control Program** (HCFAC) was created by Congress though the Health Insurance Portability and Accountability Act of 1996 to coordinate federal, state, and local law enforcement activities with respect to combating health care fraud and abuse, and associated money laundering. HCFAC operates under the joint direction of the Attorney General and the Secretary of the Department of Health and Human Services.

SAR Review Teams exist in all 94 federal judicial districts; most are led by IRS-CI with all federal law enforcement agencies with authority to investigate and/or prosecute financial crimes participating. The teams meet monthly to review proactively all SARs received from financial institutions in that judicial district. The SARs may be assigned to a particular law enforcement agency to investigate, based on that agency's expertise, or may be investigated jointly.

Regulatory And Joint Regulatory/Law Enforcement Coordination

Treasury and the Federal Banking Agencies Working Group on BSA/AML: Treasury and the Federal Banking Agencies are working closely to identify ways to enhance the effectiveness and efficiency of the BSA/AML regulations, supervision and examinations, while meeting the requirements of the statute and regulations and supporting law enforcement. The agencies are committed to strengthening the U.S. AML/CFT regime in ways that support efforts by financial institutions to devote their resources towards addressing the areas of highest risk for illicit finance activities. This includes encouraging banks to innovate with new technologies, improving information-sharing between financial institutions, and fostering increased collaboration between the government and the private sector, including through better communication of risks, to further the objectives of the BSA.

The **Bank Secrecy Act Advisory Group** (BSAAG) is chaired by FinCEN and is the main AML information conduit and policy coordination mechanism among regulators, law enforcement,

and industry. Congress directed the Secretary of the Treasury in 1992 to establish the BSAAG. The BSAAG serves as a forum for these various stakeholders to communicate about how SARs, CTRs, and other BSA reports are used by law enforcement and how the record keeping and reporting requirements can be improved to enhance their utility while minimizing costs to financial institutions. The BSAAG meets twice annually. The BSAAG is currently focusing on improving the effectiveness and efficiency of the regulatory and supervisory regime. For example, under the auspices of BSAAG, officials from FinCEN and elsewhere at the Treasury Department, industry, law enforcement, and federal regulators, are discussing ways to aims to identify areas to improve the collection and use of financial intelligence to better combat key national security threats.

The **Federal Financial Institutions Examination Council (FFIEC) BSA/AML Working Group** is composed of representatives from the federal banking agencies and the Conference of State Bank Supervisors who work to coordinate BSA/AML policy matters and training, and to improve communications among the agencies. The BSA/AML working group builds on existing activities and works to strengthen the ongoing initiatives of other formal and informal interagency groups that oversee various BSA/AML issues. This working group collaborates with FinCEN in planning and executing its monthly meetings, and also invites other agencies, such as the SEC, Commodity Futures Trading Commission (CFTC), TFFC, IRS, and OFAC, to ensure broader coordination of BSA/AML and sanctions efforts.

Intergovernmental Cooperation

In addition to employing all relevant domestic tools of government to combat illicit finance, the United States also promotes transparency and accountability in the international financial system, working bilaterally and multilaterally to build capacity and accountability.

The Financial Action Task Force

Multilateral engagement is key to promoting a level playing field around the world and encouraging other jurisdictions to improve and maintain robust AML/CFT regimes. Treasury's TFFC leads the U.S. interagency delegation to the FATF, the global standard-setting body for legal, regulatory, and operational measures against money laundering, terrorist financing, and proliferation financing.[108] The FATF has 37 member countries and maintains a global network that encompasses almost every other country in the world. TFFC has consistently played a leadership role within the FATF, with the Assistant Secretary for Terrorist Financing currently serving as the FATF's President.[109]

In addition to setting global AML/CFT standards, the FATF reviews illicit finance trends, develops best practices and guidance for implementing AML/CFT measures, and, through a peer review process, monitors members' progress in complying with the FATF standards. TFFC

108. See *Financial Action Task Force*, available at http://www.fatf-gafi.org/home/.

109. The objectives of the U.S. presidency to the FATF can be found at http://www.fatf-gafi.org/media/fatf/content/images/Objectives-FATF-XXX-(2018-2019).pdf.

is active in the FATF's public identification and monitoring process where the FATF identifies jurisdictions with strategic deficiencies in their AML/CFT regimes and develops an action plan with the country to address these deficiencies. Through this process, the FATF continues to focus on the severe risks emanating from Iran and DPRK, with DPRK subject to countermeasures, the FATF's most severe warning.

In addition to the FATF, TFFC leads the U.S. delegation to the eight regional FATF Style Regional Bodies (FSRBs). TFFC also works closely with the G7 and the G20, pushing the member countries to lead by example on important issues and to implement global standards effectively.

Basel Committee on Banking Supervision AML/CFT Expert Group

The Basel Committee on Banking Supervision AML/CFT Expert Group (AMLEG) works to develop AML/CFT policy development through coordinated effort and cooperation with international banking supervisors, and publishes decisions in the form of standards, guidelines, and sound practices. AMLEG works with a range of bodies, including the FATF, which are also hosted by the Bank for International Settlements.

Financial Stability Board Correspondent Banking Coordination Group

The Financial Stability Board (FSB) was established to coordinate at the international level the work of national financial authorities and international standard-setting bodies, and to develop and promote the implementation of effective regulatory, supervisory, and other financial sector policies in the interest of financial stability. It brings together national authorities responsible for financial stability in 24 countries and jurisdictions, international financial institutions, sector-specific international groupings of regulators and supervisors, and committees of central bank experts. Through its six Regional Consultative Groups, the FSB conducts outreach with and receives input from an additional approximately 65 jurisdictions. The Correspondent Banking Coordination Group was established to coordinate and maintain impetus in the implementation of the action plan devised by the FSB to assess and address the decline in correspondent banking.

The Egmont Group

The Egmont Group is an organization of representatives of 155 Financial Intelligence Units (FIUs). The Egmont Group provides a platform for the secure exchange of expertise and financial intelligence to combat money laundering and terrorist financing. FinCEN continues its work in the Egmont Group to promote effective information sharing and networking. FinCEN sponsors new FIUs for membership in the Group, and has played a key role on projects relating to cross-border, enterprise-wide suspicious transaction information sharing within the financial sector, compiling best practices in FIU security, and advising counterparts on FIU issues relating to FATF recommendations and mutual evaluations.

International Criminal Police Organization

International Criminal Police Organization (INTERPOL) Washington, the United States National Central Bureau, is the statutorily designated representative of the Attorney General to INTERPOL. As such, it is the official U.S. Point of Contact in INTERPOL's worldwide, police-to-police communications and criminal intelligence network. INTERPOL Washington is co-managed by the DOJ and DHS pursuant to a Memorandum of Understanding. INTERPOL Washington includes analysts and agents detailed from DOJ, DHS, and Treasury, including FBI, DEA, Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF), U.S. Marshals Service, HSI, U.S. Customs and Border Protection (CBP), USSS, and IRS-CI, among others.

Terrorist Financing Targeting Center

On May 21, 2017, the United States and the six Gulf Cooperation Council (GCC) countries[110] signed a historic agreement announcing a joint commitment to establish the Terrorist Financing Targeting Center (TFTC). The TFTC is a new TFI-led effort to leverage the expertise and deep experience of TFI's components in the region to strengthen multinational collaboration on CFT. By co-locating key TFI personnel with foreign counterparts, the TFTC will enhance information sharing and institutionalize capacity-building to target terrorist financing networks that pose national security threats to the United States and the GCC countries, and deepen existing cooperation by coordinating disruptive action, including sanctions designations. The TFTC is also consistent with the objective identified in the October 2018 *National Strategy for Counterterrorism* for our foreign partners to take a greater role in preventing and countering terrorism.

The TFTC's efforts support the administration's priorities to fight terrorism in new and innovative ways through a multilateral initiative that will dramatically increase the ability to curb terrorist financing. The TFTC has already resulted in greater regional cooperation as evidenced by the joint designations by the seven participating members of TFTC on October 25, 2017, May 16, 2018, and October 23, 2018 that targeted terrorist leaders, financiers, and facilitators. The most recent designations on October 23 targeted nine individuals associated with the Taliban, including those facilitating Iranian support to bolster the terrorist group. The TFTC will continue to disrupt the finances and operations of terrorist organizations by identifying, tracking, and sharing information regarding terrorist financing networks; coordinating joint disruptive actions; and offering support to countries in the region that need assistance building capacity to counter terrorist finance threats.

Counter-ISIS Finance Group (CIFG)

Treasury's TFFC co-chairs the Coalition's Counter-ISIS Finance Group (CIFG), a working group of the D-ISIS Coalition, along with Saudi Arabia and Italy, which convenes 50 members and observers to share information and coordinate multilateral actions that target ISIS's global financial networks.

110. Bahrain, Kuwait, Oman, Qatar, Saudi Arabia, and the United Arab Emirates.

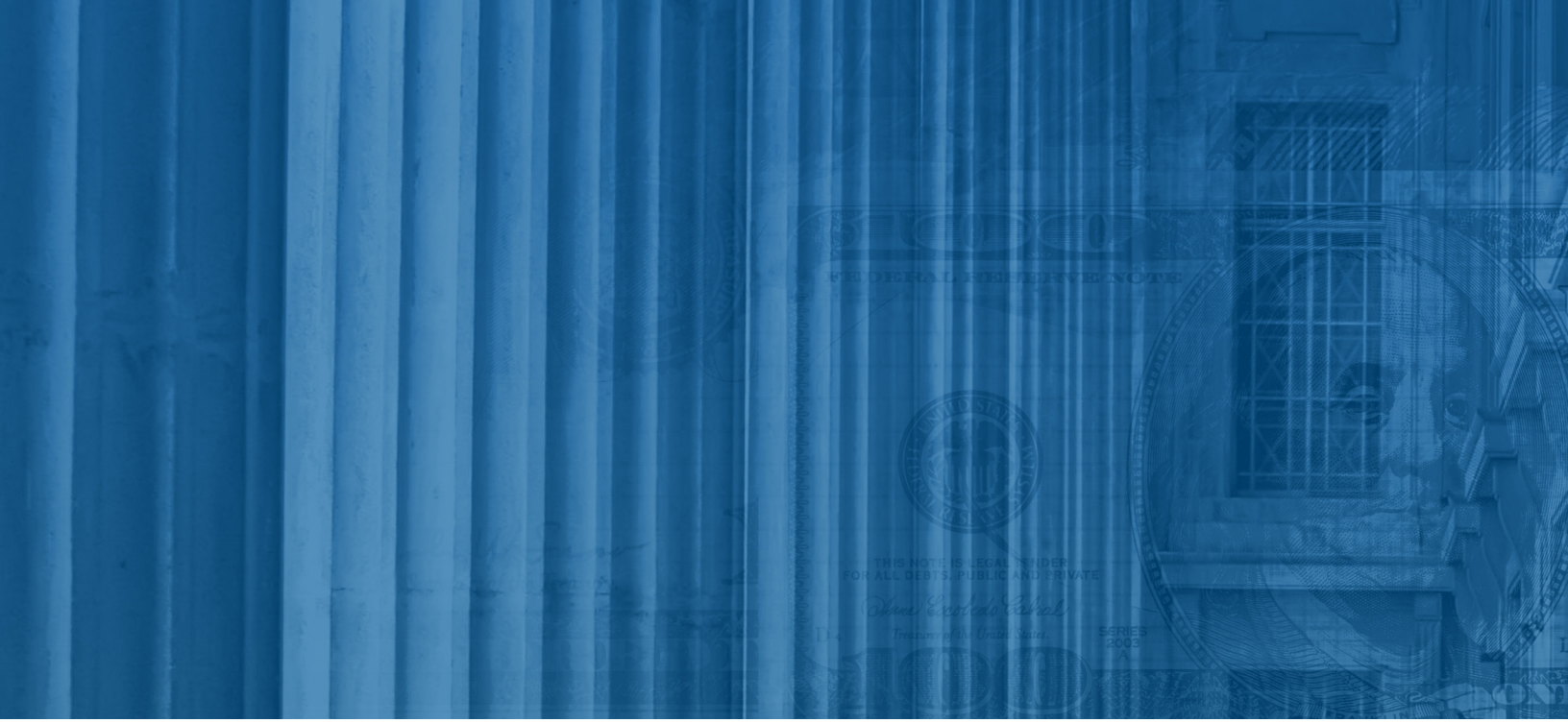
The CIFG focuses on identifying and disrupting ISIS's ability to generate revenue and access the regional and international financial systems. The CIFG has facilitated unprecedented multilateral information sharing on ISIS's global financial activity, deepened the Coalition's understanding of the effect of finances on ISIS's operations, and member states have co-sponsored the designation of ISIS financiers and their money transfer companies to the relevant UN sanctions committee list. In addition, the CIFG has helped to coordinate the provision of AML/CFT technical assistance to the Government of Iraq to support its efforts to protect the Iraqi financial system from terrorist abuse. As ISIS adapts in response to its territorial losses in Iraq and Syria, the CIFG will adapt with it, focusing on ISIS financing of its branches and leveraging its collaboration with like-minded multilateral organizations and encouraging members to take more concrete actions against ISIS financing.

Five Eyes Law Enforcement Group

International collaboration and de-confliction is enhanced through the Five Eyes Law Enforcement Group (FELEG), Money Laundering Working Group (MLWG). The mission of the FELEG/MLWG is to collaborate, inspire, and innovate to prevent, disrupt, and dismantle the money laundering activities and capabilities of international crime groups and networks impacting adversely on FELEG jurisdictions. The FELEG/MLWG is currently led by FBI and is comprised of the following member countries and agencies: United States, FBI, DEA, HSI, with IRS-CI participation; Canada, Royal Canadian Mounted Police; United Kingdom, National Crime Agency; Australia, Australian Federal Police, Australian Criminal Intelligence Commission; and New Zealand Police.

Law Enforcement Coordination Group

In order to build international awareness about Hizballah, and increase international cooperation against the group, Treasury, in close coordination with State and DOJ, established the Law Enforcement Coordination Group (LECG). The LECG has more than 25 member countries and has met six times. The LECG brings together national and regional law enforcement bodies to combat Hizballah's travel, trade, and procurement activities. The last meeting was co-hosted by Interpol and Europol in Quito, Ecuador, and attended by more than a dozen Central and South American countries. The meeting focused on combating Hizballah's travel, trade-based money laundering, and procurement activities. It also identified how investigative, enforcement, and regulatory authorities can be used to identify Hizballah-related illicit activity



SECTION 6.
INFORMATION SHARING AND GUIDANCE

The BSA, with its recordkeeping and reporting requirements, fosters a public-private partnership in order to bring as much relevant information as possible to the attention of law enforcement to combat illicit finance. That process works most effectively when the private sector works together to share information, which is possible under Section 314(b) of the USA PATRIOT Act.

Section 314(B)

The number of financial institutions taking advantage of the opportunity to share information for the purpose of better understanding and reporting suspicious activity to FinCEN has been increasing in recent years, and the number of SARs filed referencing shared information has been increasing as well.[111] Section 314(b) of the USA PATRIOT Act provides financial institutions with the ability to share information with one another under a safe harbor that offers protections from liability in order to improve identification and reporting of potential money laundering or terrorist activities. TFI strongly encourages information sharing through Section 314(b), which is a voluntary program. Currently, financial institutions subject to an AML program requirement under FinCEN regulations, and any association of such financial institutions, are eligible to share information under Section 314(b).

Outreach And Guidance

An acknowledged challenge for reporting entities is that many transactions associated with the financing of terrorism or proliferation are often hard to distinguish from otherwise ordinary, legitimate transactions. Most SARs indicating a suspicion of terrorist financing were not prompted by the reporting entity's initial detection of suspicious activity, but because the reporting entity was alerted to the names of certain individuals or entities by law enforcement or media reports.

FinCEN runs a number of programs to ensure that all of its public and private partners are effectively networking, coordinating, and sharing financial intelligence, including the following:

- *BSAAG*: As previously discussed in greater detail, FinCEN operates this congressionally established forum for industry, regulators, and law enforcement to communicate at a strategic level about how law enforcement agencies use FinCEN reports, and how recordkeeping and reporting requirements can be improved.
- *314 Information Sharing Program*: FinCEN facilitates information exchange among financial institutions and among FinCEN, financial institutions, and law enforcement. Law enforcement also shares ML/TF trends and emerging risk information with private sector representatives through the BSAAG. FinCEN uses the forum to discuss and help shape eventual public advisories.
- *Data Access, Training, and Inspection Program*: FinCEN provides more than 10,000 authorized law enforcement and regulatory users with direct access to the financial

111. FinCEN, *314(b) References in Suspicious Activity Reports (SARs) Suggest Increased Information Sharing among Financial Institutions*, available at https://www.fincen.gov/sites/default/files/shared/314bInfographic.pdf.

reporting collected by FinCEN, trains users how to utilize and safeguard the information properly, and inspects agency compliance in securing the information.

- *Regulatory Helpline*: FinCEN operates a helpline for financial institutions and individual filers needing guidance or clarification on their BSA reporting and recordkeeping requirements, or needing immediately to report suspicious activity.
- *Advisories*: FinCEN runs an Advisory Program to share information and provide feedback to financial institutions, alerting them to significant AML/CFT issues or providing more information of specific ML/TF risks. While the majority of FinCEN advisories are public, FinCEN also issues Secure Advisories that grant it the ability to provide more targeted, detailed, and sensitive information while protecting such information.
- *Foreign FIU Program:* FinCEN maintains relationships with more than 140 foreign FIUs, exchanging financial intelligence using the Egmont Group process, entering into multilateral operational engagements, providing training and mentoring, and serving as a leader in the operation of the Egmont Group.
- *Regulatory Exchange Program*: FinCEN operates a program to exchange AML/CFT compliance information with federal, state, and foreign regulators with whom it has memorandums of understanding.

FinCEN Exchange

Providing financial institutions with key government-provided information allows financial institutions to focus on specific illicit finance and national security threats under their existing BSA compliance obligations and, when appropriate, to file SARs. In turn, this increased reporting assists FinCEN and law enforcement in detecting, preventing, and prosecuting terrorism, organized crime, money laundering, and other financial crimes. After a two-year pilot program, on December 4, 2017, FinCEN publicly launched FinCEN Exchange, an operational public-private information sharing program. As part of this program, since 2015, FinCEN has convened over a dozen briefings with various law enforcement agencies across the country, involving more than 40 financial institutions. Information provided by financial institutions through SARs after the briefings have helped FinCEN map out and target weapons proliferators, sophisticated global money laundering operations, human trafficking and smuggling rings, and corruption and trade-based money laundering networks, among others.

Participants in these briefings have provided positive feedback and the private sector has expressed a strong interest in participating in the program. They find the information invaluable for channeling their resources toward high-priority targets. As such, the FinCEN Exchange team is committed to cultivating partnerships and actively developing additional events to include different types of financial institutions and key local, state, federal, or tribal enforcement agencies. As part of this effort, the FinCEN Exchange team is soliciting, accepting, and reviewing feedback as it develops the program and topic-focused events. Additionally, the team is coordinating with other information-sharing partnerships, such as the United Kingdom's Joint Money Laundering Intelligence Taskforce.

Public-Private Sector Dialogues

Treasury's TFI regularly engages public and private sector practitioners and leaders, both domestic and international, across the full spectrum of money laundering and terrorist financing issues. For example, TFI convenes multilateral and bilateral public-private sector dialogues with key jurisdictions and regions to discuss mutual AML/CFT issues of concern. These dialogues, which usually include representatives from central banks, ministries of finance, banking regulators and supervisors, and financial institutions, have fostered frank discussions on difficult topics, helped the parties learn from one another, dispel misunderstandings, clarify issues, and overcome challenges. These open and collaborative dialogues help participant countries develop more effective AML/CFT frameworks.

Guidance from Other Agencies

Federal law enforcement agencies publish a variety of relevant data and information on current ML/TF risks. In addition to news releases regarding individual investigations, agencies publish periodic reports[112] with ML/TF/WMD PF risk information as appropriate.

HSI's Cornerstone Initiative involves ongoing outreach to businesses and industries across the country to share information on criminal typologies and ML methods. Cornerstone also publishes a quarterly newsletter[113] with typologies, case examples, and tips for the private sector.

The Domestic Security Alliance Council (DSAC) is a security and intelligence-sharing initiative among the FBI, DHS, and the private sector, including the largest U.S. banks. Created in 2005, DSAC enables an effective two-way flow of vetted information between the FBI and participating members to help prevent, detect, and investigate threats impacting American businesses.

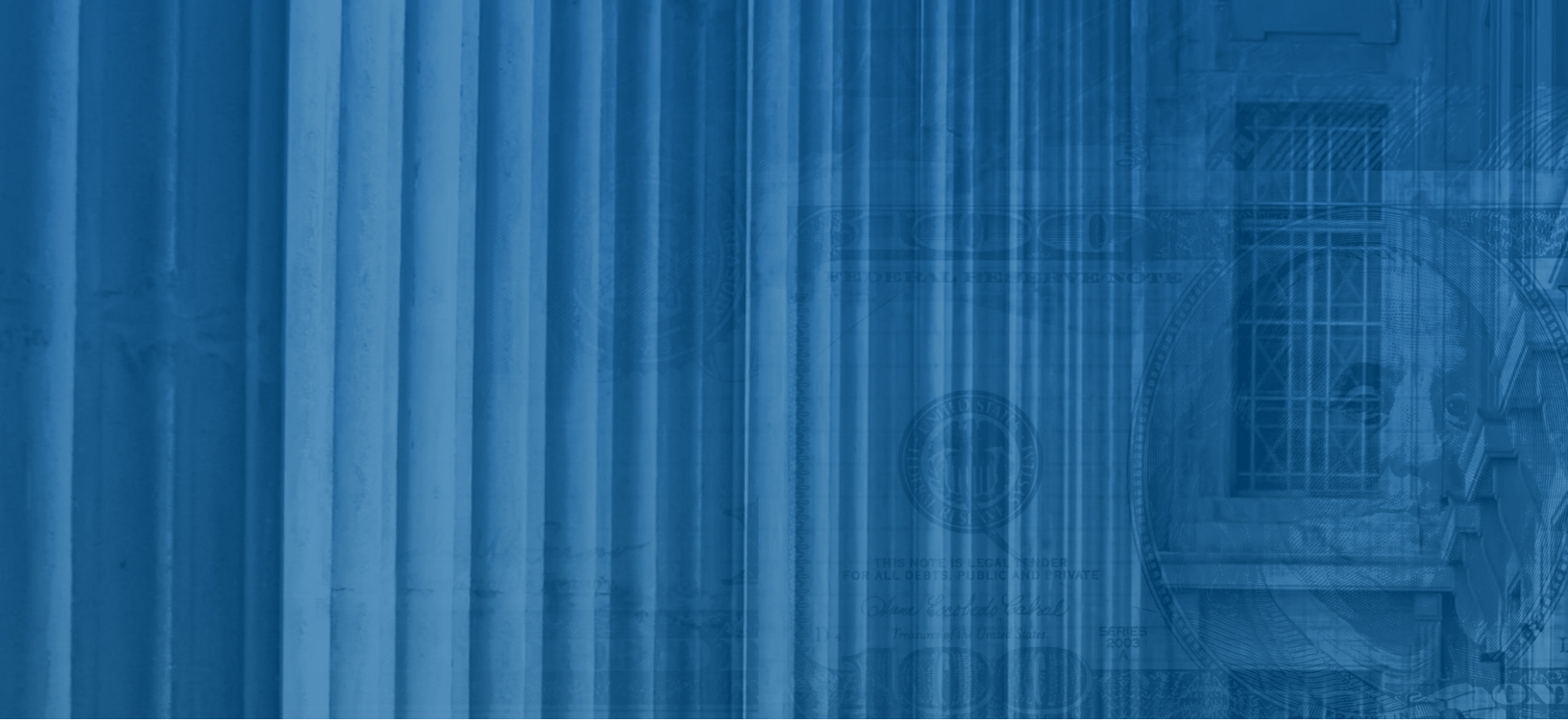
The FBI chairs an annual meeting with FinCEN at the Federal Reserve Bank of New York for international banks with a presence in the United States to share typologies, case examples, and guidance. The FBI also provides a classified briefing twice a year to selected personnel from the 20 largest financial institutions in the United States to share information on TF trends.

The federal functional regulators – the federal banking agencies, SEC, and CFTC - and self-regulatory organizations (SROs) also publish guidance on ML/TF risks for the financial institutions they supervise.

---

112. See the DEA Money Laundering Report, HSI United States of America–Mexico Bi-National Criminal Proceeds Study, annual reports (e.g., IRS-CI's annual report), and strategic plans.

113. U.S. Immigration and Customs Enforcement, Cornerstone Reports, available at http://www.ice.gov/cornerstone#tab1.



SECTION 7.
TECHNOLOGY ENHANCEMENTS

Technology-based innovation in the financial sector has great potential for enhancing the effectiveness of Bank Secrecy Act (BSA) regulations, sanctions authorities, and other tools and authorities for protecting the financial system against illicit finance abuse. Financial institutions are exploring the use of technology-based solutions to improve regulatory compliance, including AML/CFT compliance, while potentially lowering compliance costs. The development of responsible financial technology (FinTech) and Regulatory Technology (RegTech) solutions can potentially promote efficiency, competition, consumer choice, financial inclusion, as well as protecting the integrity of the financial system. The section below focuses on the use of digital identity products and services for customer identification and advanced AML/CFT transaction monitoring solutions to potentially improve the effectiveness of the AML/CFT regime.

Digital Identity

Trustworthy customer identification is a critical foundational element of the U.S. AML/CFT regime. Innovative digital identity products and services that meet appropriate standards for trustworthiness, cybersecurity, and privacy could improve customer identification and verification for onboarding and for authorizing account access, especially with respect to online financial services. Digital identity solutions can also potentially facilitate ongoing due diligence on the customer relationship and support transaction monitoring and identifying and reporting suspicious transactions. In addition to strengthening AML/CFT safeguards, digital identity solutions could improve general risk management and antifraud efforts, all while potentially generating cost savings and efficiencies for financial services firms.

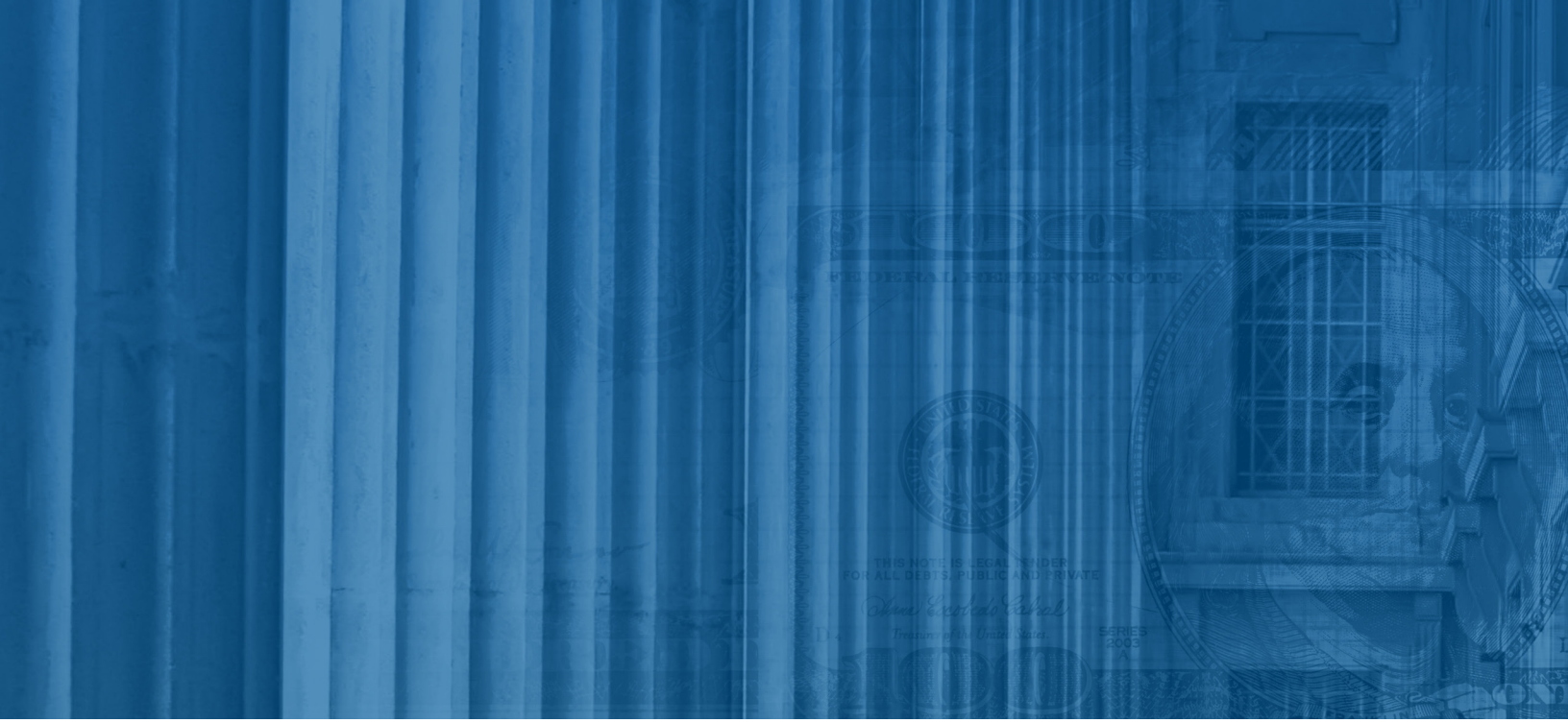
New and emerging technologies (including low-cost, more reliable biometrics, advanced chip sets; and smart phone mobile technology) could support the creation of digital identity products and services that could potentially support trustworthy digital customer identification and verification by financial institutions.

Transaction Monitoring and Reporting Solutions

Financial institutions are exploring the development and use of next generation AML/CFT RegTech compliance solutions that rely on a combination of big data sets, advanced algorithms, and machine learning to improve their ability to monitor transactions and identity and report suspicious activity. They are also looking to share information on suspicious activities in order to enable them to identify and report financial conduct that would not otherwise be visible or concerning to a single institution. Treasury recognizes that artificial intelligence and machine learning applications can potentially improve the ability of financial institutions to monitor transactions and detect patterns, trends and anomalies across big data sets, helping to identify potentially illicit activity and strengthening AML/CFT compliance, with potential cost savings. A key part of our efforts includes engaging extensively with financial institutions and technology businesses to understand both evolving technology, products and services and existing compliance methods and business models. Treasury is also engaging with international counterparts and with the federal functional regulators to learn from each other about the use of innovation labs, tech sprints, and other mechanisms to support the development and adoption of AML/CFT RegTech solutions.

Efforts to Build a Trustworthy Digital Identity Ecosystem

Developing trustworthy interoperable digital identity products and services for both the public and the private sectors requires partnership with financial institutions. Treasury, in conjunction with its domestic partners, is considering several actions to support adoption of effective digital identity solutions for AML/CFT compliance. Domestically this includes Treasury engagement with private sector stakeholders to identify if there are obstacles or challenges to the use of digital identity products and services. Treasury is also working with other federal agencies to understand their current efforts to improve identity systems for government services and encourage the use of innovative digital identity products and services that promote user convenience, while combating identity-based fraud. Internationally, Treasury is also leading efforts at the FATF to issue guidance, supporting the use of trustworthy digital identity products and services for customer identification/verification for onboarding and authenticating customer identity for authorizing account access.



APPENDIX 1:
GOALS, OBJECTIVES, AND PRIORITIES

The President's National Security Strategy (NSS)[114] identifies countering WMD proliferation, defeating terrorists, and dismantling transnational criminal organizations among the administration's top priorities. For each, the NSS and the subsidiary strategies developed to address each of these priorities emphasize the importance of dismantling the networks of support, which include financiers and money launderers. For example, one of the five lines of effort in the October 2018 *National Strategy for Counterterrorism*[115] is focused on isolating terrorists from their sources of support, with a specific priority action on countering terrorist financing. Executive Order (E.O.) 13773 of February 9, 2017, on Enforcing Federal Law with Respect to Transnational Criminal Organizations and Preventing International Trafficking[116] further elaborates the national strategy to combat TCOs and associated money laundering networks and professionals.

The goals, objectives, and priorities of the administration specific to combating illicit finance are articulated in the relevant federal agencies, bureaus, and departments' strategic plans and performance goals prepared in compliance with the Government Performance and Results Modernization Act (GPRA), which requires agencies to publish and keep updated their strategic and performance plans. Many agencies of government are charged directly or indirectly with combating illicit finance as a function of their authorities to combat terrorism, WMD proliferation, or financial crime, in the case of law enforcement; or, in the case of the financial regulators, as part of the effort to maintain the safety and soundness of the U.S. financial system.

The operational goals, objectives, and priorities, as described in the following paragraphs, among the relevant federal agencies engaged in combating illicit finance are consistent with the priorities identified in the NSS and those E.O.s regarding TCOs.

DEPARTMENT OF THE TREASURY

FYs 2018–2022 Strategic Plan[117]

Through its national security mission and statutory authority, Terrorism and Financial Intelligence (TFI) has broad tools to address activity that threatens national security and to protect the U.S. and international financial systems from abuse. Strategic objectives include (1) identifying, disrupting, and dismantling priority threats to the U.S. and international financial systems; and (2) identifying and reducing vulnerabilities in the U.S. and international financial systems to prevent abuse by illicit actors.

---

114. The White House, *National Security Strategy*, December 2017.

115. The White House, *National Strategy for Counterterrorism*, October 2018, available at https://www.whitehouse.gov/wp-content/uploads/2018/10/NSCT.pdf.

116. Presidential Executive Order on Enforcing Federal Law with Respect to Transnational Criminal Organizations and Preventing International Trafficking, available at https://www.whitehouse.gov/presidential-actions/presidential-executive-order-enforcing-federal-law-respect-transnational-criminal-organizations-preventing-international-trafficking/.

117. Treasury, Strategic Plan 2018–2022, available at https://www.treasury.gov/about/budget-performance/strategic-plan/Documents/2018-2022_Treasury_Strategic_Plan_web.pdf.

TFI deploys Treasury's powerful economic tools and authorities in a calibrated, strategic way to ensure maximum effect against rogue regimes, proliferators of weapons of mass destruction, terrorist groups, and transnational criminal organizations, among others. Treasury works bilaterally and multilaterally with international counterparts to ensure that these authorities, including those granted under the International Emergency Economic Powers Act (IEEPA) and the USA PATRIOT Act, are used strategically to target rogue regimes, criminal networks, and terrorist organizations, while considering the potential impact on the economies of the United States and its allies. TFI components include the following:

- **The Office of Terrorist Financing and Financial Crimes** (TFFC) is the policy and outreach office for TFI and works across all elements of the national security community and with the private sector and foreign governments to identify and address the threats presented by all forms of illicit finance to the international financial system. It leads the U.S. delegations to the Financial Action Task Force (FATF), the international anti-money laundering and countering the financing of terrorism (AML/CFT) standard-setting body, and to the nine FATF-style regional bodies, which oversee compliance with the FATF standards regionally.
- **The Office of Intelligence and Analysis** (OIA) is responsible for TFI's intelligence functions, integrating the Treasury Department into the larger intelligence community, and providing intelligence support to both Treasury leadership and the intelligence community.
- **The Office of Foreign Assets Control** (OFAC) administers and enforces economic and trade sanctions. OFAC works closely with U.S. law enforcement, intelligence, military and diplomatic agencies to investigate and designate foreign actors to OFAC's SDN List.
- **The Financial Crimes Enforcement Network** (FinCEN) is one of Treasury's bureaus and is the U.S. financial intelligence unit. FinCEN is responsible for administering the Bank Secrecy Act (BSA) and other regulatory functions. FinCEN supports law enforcement investigative efforts and fosters interagency and global cooperation against domestic and international financial crimes. It also provides U.S. policy makers with strategic analyses of domestic and worldwide trends and patterns.

TFI works to identify, assess, and understand the key illicit finance risks that the United States faces and to develop and implement strategies to address them domestically and globally. To accomplish this, Treasury works closely with federal financial regulatory and law enforcement agencies, the Department of State, the intelligence community, counterparts in other countries, the global standard setter for AML/CFT, the FATF, and the private sector.

All components of TFI work together to integrate their roles and authorities and maximize the collective impact on illicit finance threats and risks. TFI has a wide range of efforts underway to maintain outreach and partnership with domestic and international partners. In July 2018, TFFC, as the lead component for Treasury's FATF delegation, assumed the presidency of the FATF, prioritizing efforts to (1) address the money laundering and other illicit financing risks associated with virtual currencies and related assets, (2) take further action to strengthen international CFT efforts, and (3) enhance its work on countering WMD proliferation

financing. Moreover, in October 2018, the FATF, under the U.S. presidency, clarified how the FATF standards apply to virtual asset service providers, which include virtual currency exchangers and administrators, and how countries under the FATF standards must license or register and regulate them for AML/CFT, and monitor them for compliance with their AML/CFT obligations. In addition, TFFC leads the U.S. national risk assessment processes for money laundering and terrorist financing, as well as the first-ever proliferation finance risk assessment conducted in conjunction with this strategy.

FinCEN also plays a key role in maintaining ongoing dialogue between the U.S. government and the financial sector through vehicles such as the Bank Secrecy Act Advisory Group (BSAAG), regular issuances of advisories and public guidance statements, and FinCEN Exchange. Treasury launched the FinCEN Exchange to provide financial institutions with additional information about priority issues on a more regular basis. This will allow these financial institutions to focus on specific illicit finance and national security threats. As part of this program, FinCEN convenes regular briefings with law enforcement and financial institutions to exchange information on priority illicit finance threats, including targeted information and broader typologies. This program enables financial institutions to better identify risks and focus on high priority issues, and allows FinCEN and law enforcement to receive critical information to help them disrupt money laundering and other financial crimes. Moreover, FinCEN regularly releases advisories and guidance to financial institutions, such as a recent advisory on Iranian illicit finance.

Beyond outreach, TFI can employ a number of statutory and executive authorities to target threat actors who pose a risk to the financial system. Key to employing these measures and closing loopholes in the international financial system is access to information about the financial activities and vulnerabilities of illicit finance networks. Treasury benefits from being the only finance ministry in the world with an in-house intelligence shop, OIA. OIA produces all-source assessments and other material to identify threats and vulnerabilities in licit and illicit networks that may be addressed by Treasury-led action. OFAC administers a wide range of sanctioning authority to impose targeted financial sanctions on threats to the U.S. or international financial system. For instance, in FY 2018, OFAC conducted over 25 Hizballah-related sanction designations, and saw more designations in calendar year 2018 by the Departments of State and Treasury than in any single year. Furthermore, in September 2018, Treasury sanctioned a company with ties to the Assad regime in Syria that facilitated the trading of fuel between Assad's government and ISIS. The designations (or sanctioning) disrupted this specific illicit supply chain and eliminated access to the international financial system. FinCEN also has tools under the BSA and USA PATRIORT Act in this regard. To protect the international banking system, FinCEN named Latvia-based ABLV Bank as a primary money laundering concern under Section 311 USA PATRIOT Act. This closed a key access point exploited by illicit Russian actors to access the international banking system. As another example, FinCEN can also impose Geographic Targeting Orders under the USA PATRIORT Act, such as the recent Geographical Targeting Order (GTO) renewals on certain real estate qualifications. In addition, FinCEN has the authority to take civil enforcement actions. During FY 2018, FinCEN resolved three civil enforcement actions against financial institutions that violate the BSA, which resulted in the assessment of civil money penalties against two depository institutions and one casino.

TFI also works in close partnership with law enforcement, including IRS-CI to enforce laws against terrorist financing and money laundering, including the BSA, and works with federal and state regulators to ensure compliance with the BSA, as well as the BSA section of the IRS-Small Business/Self-Employed Division, which examines for BSA compliance those entities subject to the BSA that do not have a federal functional regulator. It is important to highlight TFI's partnership with law enforcement colleagues in particular, as a key objective of the U.S. AML/CFT regime is to generate the financial intelligence that is vital to the successful investigation and prosecution of financial crimes.

In addition to these efforts to safeguard the U.S. financial system, Treasury and its interagency partners are working to identify ways to improve the effectiveness of the AML/CFT safeguards in place. As described in section five of the Strategy, the Treasury and the Federal Banking Agencies Working Group on BSA/AML is exploring ways to modernizing the regulatory regime in ways that support efforts by financial institutions to devote their resources toward addressing the areas of highest risk for illicit finance activities. This includes encouraging banks to innovate with new technologies and approaches to enhance BSA/AML effectiveness and fostering increased collaboration between the government and the private sector, such as through better communication of risks, to further the objectives of the BSA. There are also efforts already under way within the BSAAG, which is chaired by FinCEN and is comprised of members from financial institutions, trade groups, and law enforcement, to obtain feedback on opportunities to improve the BSA framework. Treasury is also conducting outreach with financial institutions and businesses in the FinTech and RegTech sector in order to understand and assess the potential of technological innovations coming to market.

One of the goals in Treasury's 2018–2022 Strategic Plan is *Enhance national security*. The objectives, strategies, and performance measures to enhance national security are as follows.

- **Objective 1–Strategic threat disruption:** Identify, disrupt, and dismantle priority threats to the U.S. and international financial systems.

The desired outcomes are

- identify, disrupt, and successfully isolate threats from the U.S. and global financial system;
- deny revenue sources to terrorist financiers, money launderers, weapons proliferators, drug kingpins, and human rights abusers; and
- proactively implement U.S. policy toward regimes such as Iran, North Korea, Venezuela, and Russia, and terrorist organizations such as ISIS, Hizballah, and Al-Qaida (AQ).

Strategy (TFI): *Disrupt the capability of priority targets to raise, use, and move funds through strategic application of Treasury's tools and authorities*

Measures and indicators of success

- Implementation of administration and congressional policies
- Priority threats disrupted

Strategy (TFI): *Identify threats to the financial system from terrorists, proliferators, rogue regimes, and criminal actors through the exploitation and analysis of BSA data, other financial information, and all-source intelligence research and analysis*

Measures and indicators of success

- Threats identified
- Creation of analytic products

Strategy (TFI and International Affairs): *Expand current and facilitate new threat information-sharing and collaboration with domestic and international partners*

Measures and indicators of success

- Information shared
- Collaboration events

Strategy (TFI): *Maximize and integrate Treasury's economic tools and authorities across TFI components against illicit actors*

Measure and indicator of success

- Use of tools and authorities

Strategy (TFI): *Coordinate analysis of all available information sources, including intelligence analysis, BSA data, and other financial information obtained through Treasury administrative authorities or from foreign partners*

Measure and indicator of success

- Internal coordination activities

■ **Objective 2–AML/CFT Framework:** Identify and reduce vulnerabilities in the U.S. and international financial system to prevent abuse by illicit actors.

The desired outcomes are

- prevent terrorists and other illicit actors from using the U.S. and international financial systems through strengthened U.S. and global AML/CFT frameworks, and
- enhance transparency in the international financial system.

Through its national security mission and AML/CFT regulatory authorities, TFI has the responsibility to protect the U.S. financial system. The interconnectedness of the international financial system means that both threats and vulnerabilities are inherently global in nature and that illicit activity occurring outside the U.S. financial system can directly undermine the integrity of the U.S. system.

Deploying Treasury tools in coordination with other U.S. government agencies, and partnering with the private sector and foreign governments are necessary to encourage, incentivize, and compel action to bolster the integrity of the international financial system and ensure that illicit actors—including proliferators, terrorist support networks, destabilizing regimes, and transnational criminal organizations—are unable to use the financial system in support of their objectives.

Strategy (TFI and Economic Policy): *Proactively identify vulnerabilities within the financial system and address them through a risk-based approach that integrates oversight measures, regulations, targeted enforcement actions, and compliance.*

Measures and indicators of success

- Vulnerabilities addressed
- Risk-based approach implemented

Strategy (TFI): *Exchange information between and among governments, law enforcement, and financial institutions to address risks to the U.S. and global financial systems*

Measures and indicators of success

- Information exchanged
- Number of partners
- Information leading to action

Strategy *(TFI): Encourage international partners to adopt, implement, and enforce international AML/CFT standards*

Measure and indicator of success

- Number of partners adopting standards

Strategy (TFI): *Modernize, streamline, and simplify the regulatory framework to more effectively and efficiently address national security priorities*

Measures and indicators of success

- Regulatory changes
- Guidance produced

Strategy (TFI): *Modernize systems and analytical capabilities to better collect, assess, disseminate, and act upon financial data and intelligence*

Measures and indicators of success

- System modernization
- Increased analytic production and dissemination

Strategy (TFI): *Conduct law enforcement and private sector outreach and take enforcement actions, as appropriate, against noncompliant entities to encourage robust compliance controls for private actors to effectively implement sanctions-related policies and procedures*

Measures and indicators of success

- Outreach events
- Enforcement actions

IRS-Criminal Investigation (IRS-CI)

IRS FYs 2018–2022 Strategic Plan[118]

Included in the IRS FY 2018–FY 2022 Strategic Plan is the goal: *Protect the Integrity of the Tax System by Encouraging Compliance through Administering and Enforcing the Tax Code*. IRS criminal tax investigations often parallel and support money laundering and terrorist financing investigations. The objectives and supporting activities for this goal are to

- investigate criminal violations of the tax code to enforce accountability and maximize deterrence.
- Share data and coordinate on cases within and across relevant business units.
- Expand the Cyber Crimes Unit in response to the ongoing threat of virtual financial crimes.
- Raise public awareness of the outcomes of IRS criminal investigations.

Due to limited staffing, the IRS lowered its FY 2018 target to 3,000 completed investigations and 2,900 for FY 2019. The IRS expects to achieve its target of 1,900 convictions for FY 2018 and 1,800 for FY 2019. In FY 2017, IRS-CI[119] completed 3,089 criminal investigations. The

118. See IRS, *Strategic Plan: FY 2018–2022*, available at https://www.irs.gov/pub/irs-pdf/p3744.pdf.

119. See IRS, *FY 2019 Congressional Budget Justification and Annual Performance Report and Plan* at 41, available at https://www.treasury.gov/about/budget-performance/CJ19/05.%20IRS%20FY%202019%20CJ.pdf.

number of completions decreased 17 percent from FY 2016. IRS-CI has experienced a steady decrease in the number of special agents available to work cases due to attrition and limited hiring. Consequently, completed tax cases involving legal source income, illegal source income, and money laundering associated with narcotics decreased (22.5 percent, 13.2 percent, and 12.3 percent, respectively) in FY 2017 compared to the same period in FY 2016.

DEPARTMENT OF JUSTICE (DOJ)

FYs 2018–2022 Strategic Plan[120]

The Attorney General has designated the following four strategic goals for the DOJ's FYs 2018–2022 Strategic Plan:

- Strategic Goal 1, Enhance National Security and Counter the Threat of Terrorism
- Strategic Goal 2, Secure the Borders and Enhance Immigration Enforcement and Adjudication
- Strategic Goal 3, Reduce Violent Crime and Promote Public Safety
- Strategic Goal 4, Promote Rule of Law, Integrity, and Good Government

The underlying objectives and strategies supporting Strategic Goals 1 and 3 include combating illicit finance as part of the effort to counter the threat of terrorism and combatting drug trafficking and other forms of financial crime. Portions of the relevant objectives and strategies are highlighted as follows.

Strategic Goal 1

Objective 1.1:[121] Disrupt and defeat terrorist operations.

DOJ's top priority is combating terrorism, whether via deterrence, disruption, or prosecution. Within DOJ, the National Security Division (NSD), U.S. Attorneys' Offices, and the FBI have the primary responsibility for defeating terrorism and other threats to national security. They carry out this mission through FBI investigations and criminal prosecutions. Success involves collaborating with the Intelligence Community and law enforcement partners to neutralize terrorist cells and operatives at home, dismantle extremist networks worldwide, and cut off financing and other support provided by terrorist sympathizers.

Strategies to Achieve Objective 1.1

Strategy 1: *Identify, disrupt, and prosecute terrorist suspects for plots and acts that threaten our national security.*

120. See DOJ, *Strategic Plan for 2018–2022*, available at https://www.justice.gov/jmd/page/file/1071066/download.

121. These specific objective numbers have been extracted from the DOJ Strategic Plan.

DOJ will protect the United States by disrupting the terrorists' sources of financial, weaponry, and material support, as well as by prosecuting those who engage in plots or acts that threaten our national security.

Key Performance Indicators

- Number of counterterrorism (CT) disruptions through investigations
- Number of incidents reported to the United States Bomb Data Center via the Bomb and Arson Tracking System
- Percentage of CT defendants whose cases were favorably resolved
- Number of activities conducted with the goal of building the capacity of foreign law enforcement, prosecutors, and judicial systems to disrupt and dismantle terrorist actions and organizations

Strategic Goal 3

Objective 3.2: Disrupt and dismantle drug trafficking organizations to curb opioid and other illicit drug use in our nation.

DOJ will leverage the collective talent and expertise of its law enforcement components to target, investigate, and prosecute domestic and international drug trafficking organizations (DTOs). Through the formation of prosecutor-led, multi-agency task forces, DOJ will continue to mount a comprehensive, multilevel attack on drug trafficking and money laundering organizations that pose the greatest threat to the Nation. DOJ will focus on all elements of DTOs, including international sources of supply, money launderers, international and domestic transportation organizations, and regional and local distribution networks.

Strategies to Achieve Objective 3.2

Strategy 1: *Identify and disrupt organized crime and drug networks.*

To address the safety and security threats posed by organized crime and drug networks, DOJ will target the most significant and violent offenders.

Strategy 2: *Enforce drug trafficking laws including opioid-related health care fraud to reduce opioid addictions and deaths.*

DOJ will enforce drug trafficking laws against those who traffic in illicit opioids and will work to ensure compliance with the Controlled Substances Act to reduce opioid use, addiction, and deaths in the United States. DOJ will also pursue opioid prosecutions through the Medicare Fraud Strike Force, and against physicians, pharmacists, and drug companies, where appropriate.

Key Performance Indicators

- Number of disruptions and dismantlements of DTOs linked to Consolidated Priority Target Organizations (CPOTs)[122]
- Number of disruptions and dismantlements of Priority Target Organizations (PTOs) not linked to CPOTs
- Number of Scheduled Diversion Investigations completed
- Number of CPOT-linked investigations with one or more defendants convicted

National Security Division

Among the areas of focus that NSD has identified that will guide its operations in the coming years,[123] the following implicitly include combatting the financing of terrorism and proliferation:

Prevent, disrupt, and defeat terrorist operations before they occur by integrating intelligence and law enforcement efforts to achieve a coordinated all tools response to terrorist threats.

Prosecute those involved in terrorist acts, adapting investigations to address changing terrorism threats, including homegrown violent extremism and cyber-enabled terrorism.

Protect national assets from nation-state and terrorist threats, including through investigating, prosecuting, and disrupting espionage activity, proliferation, and foreign investment threats; and strengthening partnerships with potential targets of intelligence intrusions.

Criminal Division

DOJ's Criminal Division houses the Money Laundering and Asset Recovery Section (MLARS) along with numerous other sections whose missions include prosecuting money laundering predicate crimes and related money laundering offenses (see statistics on money laundering and related prosecutions in the enforcement section). MLARS has jurisdiction over complex, sensitive, international, and multi-district cases, including those pertaining to public corruption, foreign corruption, corporate fraud, procurement fraud, computer crime, intellectual property crime, international organized crime, gang crime, narcotics offenses, money laundering offenses, child sexual exploitation, and human rights violations. Among the Criminal Division's stated priorities is ensuring the stability and security of domestic and global markets, as well as the integrity of government programs, by reducing fraud, money laundering, and other economic crimes by both corporations and individuals.[124]

---

122. The Attorney General's CPOT List is a multi-agency target list of the command and control elements of the most prolific international drug trafficking and money laundering organizations affecting the United States.
123. See National Security Division FY 2019 Budget Request At A Glance, available at https://www.justice.gov/jmd/page/file/1033231/download.
124. See Department of Justice Criminal Division FY 2019 Budget Request At A Glance, available at https://www.justice.gov/jmd/page/file/1033246/download.

Organized Crime Drug Enforcement Task Forces[125] (OCDETF)

The OCDETF Program is the centerpiece of DOJ's long-term intra- and inter-agency drug enforcement strategy. OCDETF is also an integral part of the President's Executive Order on Enforcing Federal Law with Respect to Transnational Criminal Organizations and Preventing International Trafficking. OCDETF resources and coordinates law enforcement task forces combining federal, state, and local agencies focused on dismantling high-priority drug trafficking money laundering, violent, and transnational criminal organizations.

OCDETF manages the annual formulation of the Attorney General's CPOT list. OCDETF also requires its participants to identify major Regional Priority Organization Targets (RPOTs). The CPOT and RPOT lists are important management tools for the OCDETF Program. These lists enable the OCDETF Regions and districts to focus enforcement efforts on specific targets that are believed to be primarily responsible for the national and regional drug supply, and to coordinate related nationwide investigations against the CPOT and RPOT organizations. It is through the disruption and dismantlement of these major drug trafficking and money laundering organizations that OCDETF will have its greatest impact on the overall drug supply.

The FY 2018 CPOT list began with 54 targets and currently contains 49 targets. These targets are the leaders of the most significant DTOs around the world that impact the supply of illegal drugs in the United States. The RPOT Lists identify those organizations whose drug trafficking and money laundering activities have a significant impact in a particular OCDETF Region.

More than 99 percent of OCDETF's active cases include a financial investigation component. This figure represents an all-time high and demonstrates that OCDETF participants are complying with OCDETF mandates to pursue financial investigations as an integral part of each investigation. As a result of OCDETF's continuing focus on the importance of financial investigations, a significant percentage of investigations result in the seizure and restraint of assets, and in charges calling for the forfeiture of the proceeds and instrumentalities of crime. During the last four fiscal years, FYs 2014–2017, OCDETF investigations have been responsible for the seizure of approximately $1.4 billion in assets.

In FY 2017, 12 percent of all OCDETF defendants were charged with financial crimes. Additionally, 9 percent of OCDETF defendants were convicted of a financial charge. Additionally, 30 percent of investigations with indictments that were closed in FY 2017 were reported as resulting in convictions for financial crimes. Furthermore, 8 percent of OCDETF investigations initiated in FY 2017 targeted a primary money laundering organization.

Participating agencies have seized or forfeited a substantial amount of the estimated illegal proceeds but the numbers are decreasing. Due to the increasing complexity of investigations and ever-evolving technological advances, OCDETF's investigative agents and prosecutors strive to find expertise sufficient to investigate and dismantle the financial infrastructure of these criminal organizations fully, despite continued emphasis on targeting money launderers and facilitators.

125. See FY 2019 Interagency Crime and Drug Enforcement Congressional Submission, available at https://www.justice.gov/jmd/page/file/1034356/download.

Federal Bureau of Investigation

FBI mission priorities that involve combating illicit finance include the following:

- Protect the United States from terrorist attack
- Protect the United States against cyber-based attacks and high-technology crimes
- Combat public corruption at all levels
- Combat domestic and transnational criminal organizations and enterprises
- Combat major white collar crime

The FBI's Money Laundering, Forfeiture, and Bank Fraud Unit manages the ML threat associated with facilitation by targeting professional gatekeepers/controllers providing laundering services for a fee.[126] Money laundering facilitators move money often without concern or knowledge of the underlying crime. Money laundering facilitators encompass complicit third parties, who knowingly launder illicit proceeds through the U.S. financial system on behalf of their clients; complicit financial institutions (banks, broker dealers, casinos, hedge funds, MSBs); or trade-based money laundering (TBML) operations manipulating value systems to move money. Individuals and groups engaged in this activity employ methods such as real estate investing, establishing money mule networks, exploiting financial institutions, stock or commodities market manipulation, TBML, shell, shelf and front company formations, as well as the exploitation of virtual currency and emerging payment systems.

In 2015, FBI designated money laundering as a priority focus for its 56 field offices. The FBI initiated more than 250 cases targeting money laundering facilitation in two years. Investigations into multinational money laundering organizations, necessitating the effective support of many countries' law enforcement agencies can be difficult and time consuming, with individual investigations potentially lasting more than a year. However, the potential impact of prosecuting professional money launderers or professional laundering networks can be worth the expenditure of resources because they broadly facilitate and promote the ongoing criminal activity of TCOs and other criminals and help them avoid legal consequences.

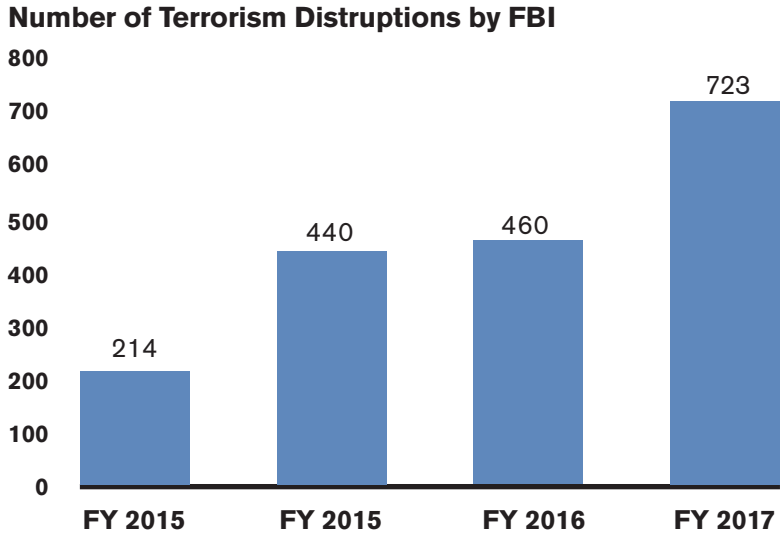
The FBI CT Division's operational priorities are classified. However, the DOJ does report goals and accomplishments in several relevant categories for the FBI. The number of terrorism disruptions the FBI achieved in FY 2017 exceeded the target of 200 and has been climbing each year (see Figure 1). The FBI also exceeded its FY 2017 goal of 150 non-CPOT gang/criminal enterprise dismantlement with 178. The FBI has exceeded its target in this area in four of the five previous fiscal years. Instrumental to the FBI's continued success in combating gangs/criminal enterprises has been its working partnerships with federal, state, and local law enforcement counterparts.

126. See FBI, "Combating the Growing Money Laundering Threat," October 24, 2016, available at https://www.fbi.gov/news/stories/combating-the-growing-money-laundering-threat.

The DOJ Strategic Plan for FY 2018–2022[127] includes specific long-term outcome goals, covering the plan's strategic goals. For the FBI, the plan's goals include the following:

- Conduct 250 CT disruptions effected through investigations
- Dismantle a cumulative total of 175 non-CPOT gangs/criminal enterprises
- Disrupt and dismantle 295 DTOs linked to CPOTs annually (with DEA and OCDETF)
- Dismantle a cumulative total of 1,925 criminal enterprises engaging in white-collar crimes

Figure 1. "Disruption" is defined as interrupting or inhibiting a threat actor from engaging in criminal or national security-related activity. A disruption is the result of direct actions and may include, but is not limited to, the arrest, seizure of assets, or impairing the operational capabilities of key threat actors.



Drug Enforcement Administration

DEA focuses on the disruption and dismantling of drug trafficking and money laundering organizations believed to be primarily responsible for the nation's illicit drug supply. This includes the CPOTs identified by DOJ, plus other Priority Target Organizations (PTOs) identified by DEA. The most significant DTOs operating in the United States today are Mexican TCOs, which are DEA's priority targets. DEA also places a high priority on preventing drug proceeds from ending

127. See DOJ, *Strategic Plan for 2018-2022*, available at https://www.justice.gov/jmd/page/file/1071066/download.

up in the hands of terrorist organizations.[128] In early 2018, a DOJ task force was stood up to combat this threat as it relates to Hizballah.[129]

DEA's performance goals most relevant to combating illicit finance concern dismantling or disrupting Consolidated Priority Organization Target (CPOTs).

Performance Measure: CPOT-linked DTOs dismantled and disrupted (OCDETF, DEA, FBI)

	FY 2012	FY 2013	FY 2014	FY 2015	FY 2016	FY 2017
Target (dismantled)	145	145	145	150	188	188
Actual (dismantled)	171	219	208	194	185	*
Target (disrupted)	340	340	340	350	233	233
Actual (disrupted)	446	500	431	422	268	*

During the fiscal year, the number of CPOT-linked drug trafficking organizations dismantled/disrupted was impacted due to the cyclical nature of investigations, sequestration, and the overall impact of declining resources, so that complete data is not available for FY 2017. As previously noted, the FYs 2018–2022 target is to disrupt and dismantle 295 DTOs linked to CPOTs annually (with FBI and OCDETF).

Investigation and prosecution of drug trafficking organizations linked to the FY 2017 dismantled CPOT targets have led to more than $21 million in seizures, $16.6 million in forfeitures, and $1.5 million in money judgments. Furthermore, dismantlement of these organizations includes the disruption and/or dismantlement of their money launderers and financial infrastructure. These organizations are also responsible for multiple forms of organized criminal activity in addition to drug trafficking, such as violence, terrorism, corruption, human smuggling, trafficking in persons, weapons trafficking, complex financial crimes, and other illegal activities.

128. See Drug Enforcement Administration FY 2019 Budget Request At A Glance, available at https://www.justice.gov/jmd/page/file/1033151/download.

129. See DOJ, Press Release, "Attorney General Sessions Announces Hezbollah Financing and Narcoterrorism Team," January 11, 2018, available at, https://www.justice.gov/opa/pr/attorney-general-sessions-announces-hezbollah-financing-and-narcoterrorism-team.

DEPARTMENT OF HOMELAND SECURITY

Immigration and Customs Enforcement FYs 2016–2020 Strategic Plan[130]

Immigration and Customs Enforcement (ICE) has identified the following three goals in the FYs 2016–2020 Strategic Plan:

- Goal 1: *Counter terrorism and protect the borders.*
- Goal 2: *Protect the borders through efficient immigration enforcement.*
- Goal 3: *Operate an efficient, effective agency.*

The underlying objectives supporting Goal 1 include combating illicit finance as a core element of achieving the goal and are highlighted below.

Goal 1

Objective B[131]*: Counter Terrorist Entry into the United States and Support Terrorism Investigations.*

ICE will focus on preventing terrorist organizations' efforts to move weapons, money, and people across international borders. ICE will support terrorism investigations through partnerships with the FBI Joint Terrorism Task Forces (JTTFs), the National Targeting Center, the National Counterterrorism Center (NCTC), and other government organizations. ICE will also undermine terrorist capabilities by thwarting state-sponsored or terrorists' attempts to obtain nuclear materials, conventional or advanced weaponry, and sensitive technology. ICE will work with DHS and other affected agencies to pursue completion of the U.S. government-wide export control reform initiative. ICE's strategy will include the prosecution of criminal networks as well as the identification, seizure, and forfeiture of funds used to support weapons smuggling operations and proceeds derived from this criminal activity.

Objective E: *Fight Financial Crime and Attack the Illicit Proceeds of Crime.*

Through ICE's unique combination of border search authority and access to BSA reports and trade data, ICE will conduct long-term, multilateral financial investigations. ICE will target transnational criminal organizations and identify emerging money laundering methods, such as virtual currencies. ICE will also support, through its investigative efforts, the actions of other agencies, such as administrative actions, to include OFAC designations and USA PATRIOT Act Section 311 actions, as well as FinCEN advisories and other financial tools; and coordination with the Office of the Comptroller of the Currency (OCC). Additionally, ICE will continue to partner and forge relationships with the financial and private industry to identify and eliminate vulnerabilities in the U.S. and international financial system. ICE will partner with UCBP and international counterparts to expand the Trade Transparency Unit, allowing ICE to exchange

130. See *U.S. Immigration and Enforcement Strategic Plan 2016–2020*, available at https://www.dhs.gov/publication/ois-strategic-plan.

131. The specific objective lettering have been extracted directly from the ICE Strategic Plan.

trade data and identify financial irregularities and international trade anomalies indicative of trade-based money laundering, customs fraud, contraband smuggling and other financial crimes that allow transnational criminal organizations to move and launder illicit proceeds disguised as legitimate trade.

Objective H: *Protect the Homeland through Counter-Proliferation Investigations (CPIs).*

ICE is designated as the primary federal law enforcement agency charged with investigating violations of U.S. export laws and as the executive agent for the U.S. Export Enforcement Coordination Center as designated under E.O. 13558. ICE will leverage its leadership position within the interagency to enhance and coordinate a government response to export enforcement violations while prioritizing its CPI efforts in targeting the trafficking and illegal export of conventional military equipment, firearms, controlled dual-use technology and materials used to manufacture weapons of mass destruction, including chemical, biological, radiological, and nuclear materials. ICE seeks to prevent illicit procurement networks, both real and virtual, terrorist groups, hostile nations, foreign adversaries and transnational criminal organizations from illegally obtaining these controlled technologies.

Homeland Security Investigations:[132] HSI is the investigative arm of ICE and is responsible for investigating a wide range of domestic and international activities arising from the illegal movement of people and goods into, within, and out of the United States.

Performance Measure: Percent of significant HSI cases that result in a disruption or dismantlement

Description: This measure reports on the percent of significant transnational criminal investigations that resulted in a disruption (i.e., impeding the normal and effective operation of the targeted organization) or dismantlement (i.e., destroying the organization's leadership, financial base, and network to the degree that the organization is incapable of operating and/or reconstituting itself). HSI investigations cover a broad range of areas, including national security threats, financial and smuggling violations (including illegal arms exports), financial crimes, commercial fraud, human trafficking, narcotics smuggling, child pornography/exploitation, and immigration fraud.

132. See ICE, *Fiscal Year 2019 Congressional Justification* at pp. 6–7, available at https://www.dhs.gov/sites/default/files/publications/U.S.%20Immigration%20and%20Customs%20Enforcement.pdf.

Fiscal Year:	FY 2017	FY 2018	FY 2019
Target:	15.8%	15.8%	15.9%
Result:	22.9%	TBD	TBD

Performance Measure: Percent of significant drug investigations that resulted in a disruption or dismantlement

Description: This measure will report on the percent of transnational drug investigations resulting in the disruption or dismantlement of high-threat transnational drug trafficking organizations/individuals. "Transnational drug trafficking organization" is defined by DOJ as those organizations on approved CPOT or RPOT lists or those who are earning, laundering, or moving more than $10 million a year in drug proceeds. To impact the result of this measure, ICE established international partnerships to link global customs and law enforcement agencies.

Fiscal Year:	FY 2017	FY 2018	FY 2019
Target:	15.1%	15.2%	15.2%
Result:	19.0%	TBD	TBD

Performance Measure: Percent of significant illicit trade, travel, and finance investigations (all of which are nondrug related) that result in a disruption or dismantlement

Description: This measure reports on the percent of significant nondrug related trade, travel, and finance investigations that resulted in a disruption or dismantlement. These investigations include human smuggling, nondrug financial investigations equal to or more than $5 million, commercial fraud that poses an immediate threat to public health and safety, and large-scale identity and benefit fraud.

Fiscal Year:	FY 2017	FY 2018	FY 2019
Target:	17.3%	17.4%	17.4%
Result:	22.9%	TBD	TBD

Performance Measure: Percent of significant national security and counter proliferation investigations that result in a disruption or dismantlement

Description: This measure reports on the percent of significant national security and counter proliferation investigations that resulted in a disruption or dismantlement. Significant national security investigations include JTTF investigations and investigations of individuals that have been designated as national security threats by the wider intelligence community and/or Treasury.

Fiscal Year:	FY 2017	FY 2018	FY 2019
Target:	9.2%	9.3%	9.3%
Result:	14.8%	TBD	TBD

U.S. Customs and Border Protection (CBP)

DHS Annual Performance Report FYs 2017–2019[133]

CBP's priority mission is securing the U.S. border and keeping terrorists and their weapons out of the United States. It also is responsible for securing and facilitating trade and travel while enforcing hundreds of U.S. regulations, including immigration and drug laws. In FY 2017, there were 11 strategic performance measures used to assess CBP's efforts. In FY 2017, 64 percent of the measures met their target and 56 percent maintained or improved actual results compared to FY 2016.

Prior Results					FY 2017		Performance Plan	
FY 2012	FY 2013	FY 2014	FY 2015	FY 2016	Target	Result	FY 2018	FY 2019
CBP								
Amount of smuggled outbound currency seized at the ports of entry (in millions) (CBP)								
$31.9	$36.9	$37.7	$37.6	$28.9	$30.0	$39.0	$30.0	$30.0
Percent of inbound cargo identified by CBP as potentially high-risk that is assessed or scanned prior to departure or at arrival at a U.S. port of entry (CBP)								
98%	98%	99.22%	99.76%	99.28%	100%	99.50%	100%	100%

U.S. Secret Service (USSS)

DHS Annual Performance Report FYs 2017–2019[134]

The USSS, in addition to its protective mission, has a role in investigating financial crime to safeguard the U.S. currency and payment systems. In FY 2017, there were 11 strategic performance measures used to assess USSS' efforts. Here are the current performance targets most relevant to combating illicit finance.

133. See *DHS Annual Performance Report Fiscal Years 2017–2019*, available at https://www.dhs.gov/sites/default/files/publications/DHS%20FY%202017-2019%20APR_0.pdf.

134. *Id.*

Prior Results					FY 2017		Performance Plan	
FY 2012	FY 2013	FY 2014	FY 2015	FY 2016	Target	Result	FY 2018	FY 2019
USSS								
Amount of dollar loss prevented by cyber investigations (in millions) (USSS)								
–	$1,119	$384	$589	$558	$600	$3,145[1]	$650	$700
Financial crimes loss prevented through a criminal investigation (in billions) (USSS)								
$2.75	$4.20	$3.04	$1.47	$2.42	$1.90	$3.55	$2.10	$2.30
Number of cyber mitigation responses (USSS)								
–	–	–	–	157	250	253	390	400
Number of financial accounts recovered (in millions) (USSS)								
–	3.90	0.29	0.93	0.51	0.40	27.18	0.50	0.50
Percent of currency identified as counterfeit (USSS)								
0.0085%	0.0072%	0.0068%	0.0058%	0.0057%	<0.0088%	0.0093%[3]	<0.0088%	<0.0088%
100%	100%	100%	99.7%	100%	100%	100%	100%	100%
Terabytes of data forensically analyzed for criminal investigations (USSS)								
–	4,002	4,902	6,052	3,334	7,000	5,019[4]	5,000[5]	5,100

DEPARTMENT OF STATE

The FYs 2018–2022 State and U.S. Agency for International Development Joint Strategic Plan[135]

The Department of State (State) and U.S. Agency for International Development (USAID) Joint Strategic Plan outlines a strategic vision for foreign policy and development in support of the Administration's strategic priorities and commitments to the American people. Key priorities in the Joint Strategic Plan include combating terrorism and transnational organized crime, and devising, implementing, and monitoring economic and energy sector sanctions. State houses several bureaus and offices that are responsible for carrying out these priorities and overseeing other issues related to countering illicit finance. These include the following:

- Bureau of Economic and Business Affairs (EB)
- Bureau of International Narcotics and Law Enforcement Affairs (INL)
- Bureau of International Security and Nonproliferation (ISN)
- Bureau of Counterterrorism (CT)

The CT Bureau leads State efforts to increase pressure on terrorist groups and individuals through the designation of FTOs, Specially Designated Global Terrorists (SDGTs), and State

135. See Department of State, *FY 2018–2022 State and U.S. Agency for International Development Joint Strategic Plan*, available at https://www.state.gov/documents/organization/277156.pdf.

Sponsors of Terrorism. CT develops and ensures that counterterrorism finance policies are integrated into broader diplomatic efforts, strategies, and programs. Finally, CT develops, manages, and monitors technical assistance programming to build the capacity of foreign partners—including Central Banks, financial intelligence units, as well as formal and informal financial sector partners—to detect, deter, and dismantle terrorist financial networks.

Within the Joint Strategic Plan, Goal 1 and its strategic objectives are the elements of the Plan that implicitly align with the Administration's efforts to combat illicit finance.

Goal 1: Protect America's Security at Home and Abroad

Strategic Objective 1.1: *Counter the Proliferation of WMD and Their Delivery Systems.*

State will pursue diplomatic solutions to proliferation challenges, and rally international support for sanctions against proliferant nations. The threat posed by North Korea's unlawful nuclear and ballistic missile programs requires immediate international attention and State will continue to lead efforts to impose and enforce sanctions on principal sectors of the North Korean economy, or on entities and individuals supporting North Korea's proliferation programs.

Strategic Objective 1.2: ***Defeat ISIS, AQ and other transnational terrorist organizations, and counter state-sponsored, regional, and local terrorist groups that threaten U.S. national security interests.***

State will play a key role in implementing the President's plan to defeat ISIS, through leadership of the Global Coalition to Defeat ISIS. It will work bilaterally and regionally with national and local government partners as well as multilaterally through institutions such as the United Nations (UN), G7, and Global Counterterrorism Forum to promote international norms and good practices, and sustain transregional cooperation to prevent and counter terrorism.

Strategic Objective 1.3: *Counter instability, transnational crime, and violence that threaten U.S. interests by strengthening citizen-responsive governance, security, democracy, human rights, and the rule of law.*

Law enforcement capacity building programs are the bedrock on which State strengthens partnerships to counter TCOs. Globally, State will work with partners to cut financial lifelines for global terror and organized crime organizations, including those involved with human and wildlife trafficking.

Strategic Objective 1.4: *Increase capacity and strengthen resilience of our partners and allies to deter aggression, coercion, and malign influence by state and nonstate actors.*

State will maintain a strong diplomatic presence built on enduring security partnerships to collectively deter aggression and assist allies in sustaining favorable regional strategic balances. Specifically, State will seek to increase cooperation with allies and partners to counter Iranian threats and destabilizing behavior; through sanctions, it will constrain Iran's ballistic missile program and degrade its support for terrorism and militancy.

Strategic Objective 1.5: *Strengthen U.S. border security and protect U.S. citizens abroad.*

State helps protect U.S. national borders through sharing of information within and between foreign governments and by expanding foreign government capacity to identify and interdict suspicious travelers, cargo, and materiel. State's diplomatic engagement on counterterrorism and homeland security protects U.S. citizens and deters terrorist and criminal travel by increasing information sharing on terrorists, risk-based border management, and threat-based security and border screening. To achieve this objective, State negotiates information sharing arrangements with foreign partners and helps build the capacity of foreign government law enforcement and border security agencies.

DEPARTMENT OF DEFENSE (DOD)

DOD has dedicated counter-threat finance (CTF) teams at each of its geographic combatant commands, as well as at U.S. Special Operations Command, U.S. Transportation Command, the National Guard Bureau, and intelligence components. The DOD-CTF teams analyze financial intelligence, integrate intelligence and operations, and coordinate and execute DOD-CTF activities—within DOD and with and in support of U.S. interagency partners.[136] DOD funds this activity largely through its counterdrug appropriation, and conducts this activity under its counterdrug, countertransnational organized crime, and counterterrorism authorities.

DOD-CTF work begins with other U.S. Government partners, to stand up threat finance cells in Iraq, and later in Afghanistan, in order to identify and disrupt terrorist and insurgent support networks. Outside the war zone, DOD-CTF provides support to the diplomatic and law enforcement communities by enhancing their efforts to find and seize illicit funds, prosecute threat financiers, and disrupt complex criminal revenue-generating and laundering activities. For example, DOD-CTF analysts support Treasury's efforts to develop designations against individuals and organizations engaged in illicit finance, and the State's efforts to develop and monitor U.S. and international sanctions against terrorists and transnational criminals. In sum, DOD-CTF analysts excel in helping to identify vulnerabilities and to create a comprehensive analysis for U.S. government partners to target an adversary's financial infrastructure.

In recent years, DOD has undertaken an initiative designed to give DOD-CTF within DOD a solid and lasting institutional foundation, including the recertification of DOD's Directive

136. Statement of Theresa Whelan, Acting Assistant Secretary of Defense (Special Operations and Low-Intensity Conflict) Office of the Secretary of Defense, before the Subcommittee on Emerging Threats and Capabilities of the House Armed Services Committee and the Subcommittee on Terrorism, Nonproliferation, and Trade of the House Foreign Affairs Committee, June 9, 2016.

on Counter-Threat Finance Policy through 2020. This Directive "establishes DOD policy and assigns DOD responsibilities for countering financing used to engage in terrorism, illicit trafficking networks, and related activities that support an adversary's ability to negatively affect U.S. interests." The Directive also states that it is DOD policy to "work with other U.S. government departments and agencies and with partner nations to deny, disrupt, or defeat and degrade adversaries' ability to use global licit and illicit financial networks to negatively affect U.S. interests."

U.S. Special Operations Command serves as DOD's lead component for synchronizing DOD CTF activities that transcend Geographic Combatant Commands' areas of responsibility. The Combatant Commands and other DOD components coordinate their DOD-CTF activities closely with one another. This integration is essential given the fluidity of money and resources and the transnational nature of threat networks.

To advance future DOD-CTF missions and help sustain DOD-CTF capabilities, DOD captures and shares lessons learned from DOD-CTF activities. For example, DOD has gathered and disseminated lessons learned on building threat finance cells based on the experiences in Iraq and Afghanistan.

DOD sustains its DOD-CTF capability across its planning, programming, budgeting, and execution process. The Deputy Assistant Secretary of Defense for Counternarcotics and Global Threats provides policy guidance, conducts annual program reviews, prepares budgets to support DOD-CTF programs across DOD's Future Years Defense Program, and executes DOD-CTF programs funded by the DOD Drug Interdiction and Counterdrug Activities appropriation. DOD uses this process to prioritize DOD-CTF resources in order to focus on the targets that pose the greatest threat to U.S. national security.

SUPERVISORY AUTHORITIES

The federal banking agencies[137] (FBAs) are the supervisory authorities responsible for regulation, supervision, examination, and enforcement of federal banking laws. They include the Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation (FDIC), OCC, and National Credit Union Administration (NCUA).

As stated in its Annual Report, the Board of Governors of the Federal System recognizes its role in deterring illicit finance by examining institutions under its primary supervision for compliance with applicable AML laws and regulations and conducts such examinations in accordance with the Federal Financial Institutions Examination Council's (FFIEC's) *Bank Secrecy Act/Anti-Money Laundering Examination Manual*.[138]

---

137. Under the BSA Regulations, the term "bank" includes each agent, agency, branch or office within the U.S. of commercial banks, savings and loan associations, thrift institutions, credit unions, and foreign banks. See 31 C.F.R. 1010.100(d). Bank is used, therefore, generically to refer to these financial institutions.

138. For additional information, see the 104th Annual Report–2017, https://www.federalreserve.gov/publications/files/2017-annual-report.pdf.

Each of the FBAs maintains a strategic plan. Those sections of the strategic plans of the FDIC and the OCC that explicitly reference examining for BSA or OFAC compliance are presented in the following paragraphs.

FDIC

The FDIC[139] and state bank regulatory agencies[140] conduct BSA/AML examinations for insured state nonmember institutions.[141] During each safety-and-soundness examination, the FDIC evaluates the institution's compliance with the BSA and its implementing regulations[142] as well the FDIC's own BSA compliance program[143] and suspicious activity reporting[144] requirements. The focus of a BSA/AML examination is to assess whether the institution has established and maintains a BSA compliance program that is commensurate with the institution's money laundering and terrorist financing risks.

FDIC: 2018 Annual Performance Plan[145]

The FDIC's 2018 Annual Performance Plan identifies five strategic goals:

- **Strategic goal 1:** *Insured depositors are protected from loss without recourse to taxpayer funding.*
- **Strategic goal 2:** *FDIC-insured institutions are safe and sound.*
- **Strategic goal 3:** *Consumers' rights are protected, and FDIC-supervised institutions invest in their communities.*
- **Strategic goal 4:** *Large and complex financial institutions are resolvable in an orderly manner under bankruptcy.*
- **Strategic goal 5:** *Resolutions are orderly, and receiverships are managed effectively.*

---

139. The Bank Secrecy Act: A Supervisory Update, https://www.fdic.gov/regulations/examinations/supervisory/insights/sisum17/si-summer-2017-article02.pdf.
140. The majority of state bank regulatory agencies examine for BSA/AML compliance. The FDIC conducts BSA/AML examinations for those states that do not conduct BSA/AML examinations, which averages to less than 20 BSA/AML examinations annually on behalf of state counterparts.
141. Insured state nonmember institutions are state-chartered institutions that are not members of the Federal Reserve System. The Federal Reserve conducts BSA/AML examinations for state-chartered banks that are members of the Federal Reserve System. Federally insured credit unions are examined for BSA/AML compliance by the National Credit Union Administration.
142. 31 C.F.R. Chapter X.
143. 12 C.F.R. § 326.8.
144. 12 C.F.R. § 353.
145. See FDIC, *2018 Annual Performance Plan*, available at https://www.fdic.gov/about/strategic/performance/2018annualplan.pdf.

Each goal has a set of strategic objectives, annual performance goals, indicators and targets, and means and strategies. Strategic goal 2 is directly aligned with combating illicit finance. That goal and relevant performance target information are presented as follows.

Strategic goal 2: FDIC-insured institutions are safe and sound.

Annual Performance Goal 2.1–2.2

Assist in protecting the infrastructure of the U.S. banking system against TF, money laundering, and other financial crimes.

Indicator and Target

1. Percentage of required examinations conducted in accordance with statutory requirements and FDIC policy

- Conduct all BSA examinations within the timeframes prescribed by statute and FDIC policy.

Means and Strategies

Operational Processes (initiatives and strategies): The FDIC conducts BSA/AML examinations and OFAC reviews to assess the BSA/AML and OFAC compliance programs of FDIC-supervised financial institutions. These examinations and reviews cover sound risk management, compliance with recordkeeping and reporting requirements, the ability of the institution to identify and report suspicious activities, and compliance with trade and economic sanctions.

BSA/AML examinations and OFAC reviews are performed as a part of all risk management examinations of FDIC supervised insured depository institutions. The FDIC also completes BSA/AML examinations and OFAC reviews for states that do not conduct these examinations.

The FDIC follows a risk-based approach to BSA/AML examinations and OFAC reviews, which allows examiners to focus resources on those areas with the greatest potential risk. Guidance is provided to risk management staff through written memoranda, participation in the FFIEC BSA/AML Examination Workshop, and attendance at the FFIEC Advanced BSA/AML Specialists Conference.

Human Resources (staffing and training): There are 326 FDIC examiners who are designated as BSA/AML subject matter experts. Staffing and training needs are reviewed regularly to ensure the staff resources supporting the BSA/AML examination program are adequate and that employees possess the skills and knowledge to effectively and successfully assess compliance with BSA/AML requirements and detect any emerging risks. In 2017, the FDIC strengthened its BSA/AML staffing resources by establishing senior BSA/AML examiner positions in each region. In 2018, the FDIC is developing a formal on-the-job training program to develop higher-level proficiencies in the BSA/AML and OFAC examination specialty area.

2017 Performance Results

The FDIC successfully met the performance target for this annual performance goal in 2017. This annual performance goal and its associated performance indicator and target are unchanged for 2018.

OCC

The OCC examines national banks and federal savings associations and federal branches and agencies of foreign banks in the United States for BSA/AML compliance as well as for OFAC compliance. OCC-regulated institutions are subject to comprehensive, ongoing supervision designed to enable examiners to identify problems and obtain corrective action. Such supervision permits most bank problems to be resolved through the supervisory process without formal enforcement action.

OCC Strategic Plan, FYs 2015–2019[146]

The OCC's Strategic Plan, FYs 2015–2019 identifies three strategic goals:

- **Goal 1:** *A vibrant and diverse system of national banks and federal savings associations that supports a robust U.S. economy*
- **Goal 2:** *"One OCC" focused on collaboration, innovation, coordination, and process efficiency*
- **Goal 3:** *The OCC is firmly positioned to continue to operate independently and effectively into the future.*

Each goal has a set of strategic objectives, and strategies. Goal 1 is aligned with combating illicit finance. The goal, strategic objective, and strategies are presented as follows.

Goal 1: *A vibrant and diverse system of national banks and federal savings associations that supports a robust U.S. economy*

Strategic Objective 1.1: Provide high-quality, effective, and efficient supervision that is both proactive and risk-based to promote a safe and sound system for the delivery of banking services.

Strategies:

- Enhance capabilities, methods, and practices to effectively oversee and supervise regulated entities and their affiliates and service providers.
- Strengthen the agency's systemic and individual risk identification.
- Support efforts by community banks to address their strategic challenges.

146. See OCC, *The OCC's Strategic Plan Fiscal Years 2015–2019*, available at https://www.occ.gov/publications/publications-by-type/other-publications-reports/occ-strategic-plan-2015-2019.pdf.

- Supervise and regulate commensurate with the size and complexity of the institution.

Strategic Objective 1.3: Provide a coordinated supervisory, regulatory, and legal framework that encourages regulated entities to innovate and adapt in response to a changing environment.

Strategies:

- Support innovation in national bank and federal savings association business models that meet the changing needs of consumers, communities, and businesses.
- Enhance flexibility of the federal savings association charter to promote its long-term value.
- Ensure regulated entities understand and are properly prepared to identify and mitigate operational risks including cyber threats and BSA compliance challenges.

Strategic Objective 1.4: Collaborate with other regulators both domestically and internationally to better identify systemic risk and support efficient financial systems.

Strategies:

- Collaborate with other U.S. financial regulatory agencies to develop consistent supervisory strategies for larger, more complex institutions and encourage knowledge sharing.
- Improve coordination and cooperation with non-U.S. financial supervisors.
- Actively participate in the assessment of resolution and recovery strategies for domestic and global systemically important banks and require appropriate legal entity simplification.

The OCC's Executive Committee members have a process for measuring their individual organization's performance. Also, in March 2016, the OCC established the Compliance and Community Affairs department, led by a Senior Deputy Comptroller who is a member of the agency's Executive Committee and Committee on Bank Supervision. Compliance and Community Affairs focuses on enhancing the agency's ability to comprehensively identify and address compliance risk, issue timely guidance and procedures, and communicate effectively about emerging compliance issues. These changes were designed to strengthen the OCC's ability to provide effective supervision in the area of BSA/AML, as well as consumer compliance, community reinvestment and fair lending.

Other Supervisory Bodies

The **SEC** examines for and enforces compliance with federal securities laws by the financial institutions it regulates, including compliance with BSA requirements where applicable. In addition, broker-dealers must become members of self-regulatory organizations (SROs) that are subject to SEC oversight. The Financial Industry Regulatory Authority (FINRA) is the largest of the SROs.

The SEC's Office of Compliance Inspections and Examinations (OCIE) publishes examination priorities annually. For 2018, OCIE's examination priorities provided that "we will continue to focus a portion of our resources on examining whether the entities we regulate are appropriately adapting their AML programs to address their obligations."

Each January FINRA publishes its Annual Regulatory and Examination Priorities Letter[147] identifying the topics that FINRA will focus on over the coming year. For 2018, the letter noted:

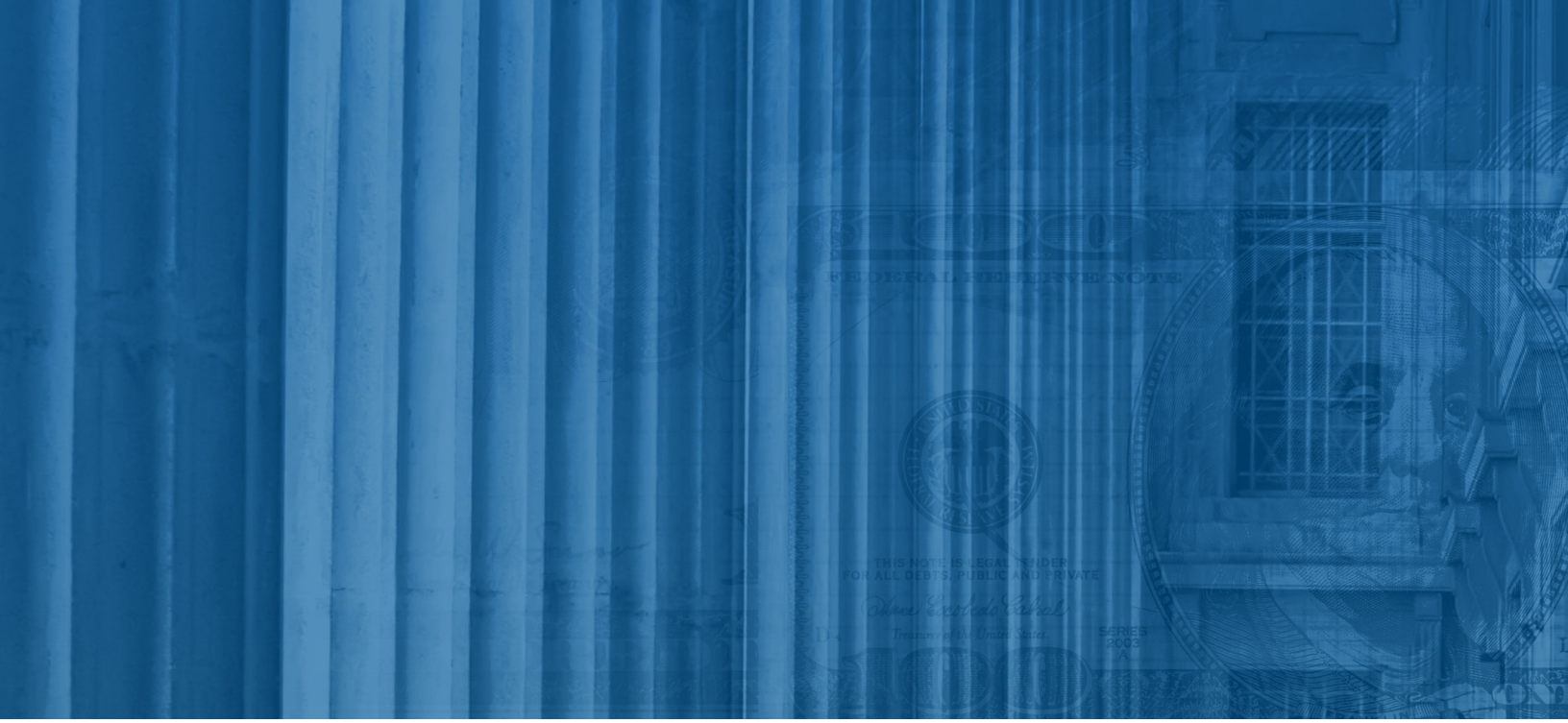
> *FINRA will assess the adequacy of firms' anti-money laundering (AML) programs. FINRA continues to identify concerns related to, for example, the adequacy of (1) firms' policies and procedures to detect and report suspicious transactions; (2) resources for AML monitoring; and (3) independent testing required under FINRA Rule 3310(c). Firms should review the Examination Findings Report to understand FINRA's areas of concern and observations on effective practices related to AML. In addition to those concerns, firms should be attentive to the potential use of their foreign affiliates to conduct high-risk transactions through accounts at member firms, including in microcap and dual-currency securities. FINRA has observed situations where firms do not monitor, or may monitor less closely, accounts opened for an affiliate. Firms should also confirm that their AML surveillance programs cover accounts used in connection with securities-backed lines of credit (SBLOCs) and aggregate activity across accounts when they use multiple accounts to receive and disburse funds in connection with an SBLOC.*

The CFTC oversees the nation's swaps, futures, and options markets. The CFTC also oversees the operations of the futures and swaps industry SROs, which include the National Futures Association (NFA) and the CME Group.

The CFTC Strategic Plan for FYs 2014–2018 includes four goals, which implicitly include deterring illicit finance:

- Goal 1: Market integrity and transparency
- Goal 2: Financial integrity and avoidance of systemic risk
- Goal 3: Comprehensive enforcement
- Goal 4: Domestic and international cooperation and coordination

147. See FINRA, *2018 Annual Regulatory and Examination Priorities Letter*, January 2018, available at, http://www.finra.org/sites/default/files/2018-regulatory-and-examination-priorities-letter.pdf.



APPENDIX 2:
ILLICIT FINANCE FUNDING ALLOCATIONS FOR SELECT PROGRAMS

The chart on Illicit Finance Funding Allocations for Select Programs extrapolates from the President's Annual Budgets and agency justifications submitted to Congress, to reach a rough approximation of what is spent by certain agencies combating illicit finance. Given that many departments and agencies do not separately track budget data related to illicit finance, there are challenges with identifying illicit finance-related funding for most programs. Other challenges are due to the nature of various budget presentations, operational realities and uncertainties. Therefore, the chart only provides figures where they could be reasonably estimated and should not be considered authoritative. As such, the actual scope of work and funds expended on combatting illicit finance are in fact almost certainly greater than what is presented. The absence of a particular agency does not mean that agency has no role in combatting illicit finance. For example, a number of supervisory agencies, such as the Board of Governors of the Federal Reserve System, do not separately track budget data related to combatting illicit finance and are therefore not included on this chart. However, supervisory agencies play a critical role in helping to ensure that U.S. financial institutions maintain effective Bank Secrecy Act/Anti-Money Laundering programs, and this contribution is not reflected in the chart if that agency was not able to provide an estimate for counter-illicit budgetary allocations.

The budget of the Treasury Department's Office of Terrorism and Financial Intelligence is allocated to countering illicit finance. For other offices of the federal government, resources allocated to combating illicit finance reflect only a portion of the agency or department budget as they also do not separately track budget data related to illicit finance. In these cases (e.g., the Federal Bureau of Investigation and the U.S. Attorney's Offices), the figures cited are overly inclusive, as it was not possible to distinguish the precise amount spent on combatting illicit finance from the broader overarching missions of those departments or agencies. Where possible, the notes explain the source or nature of the figures cited. In those examples where no footnotes are cited, the figures were provided directly by the agencies, which used their own internal mechanism to develop an applicable figure.

Information not readily or easily discernible is needed for greater precision, given that some budget allocations not included are based on addressing broader threats and may not capture activities specifically designed to combat illicit financing as such.

Illicit Finance Funding Allocations for Select Programs			
	FY 2017 (millions)	FY 2018 (millions)	FY 20191 (millions)
Department of the Treasury[2]			
Terrorism and Financial Intelligence[3]	$238	$257	$277
IRS-Criminal Investigations[4]	$595	$577	$579
Department of Justice[5]			
Criminal Division[6]	$41	$41	$44
National Security Division	$96	$95	$101
Federal Bureau of Investigation FBI(salaries and expenses)[7]	$4,661	$4,598	$4,684
Drug Enforcement Administration DEA (salaries and expenses)	$21	$21	$21
U.S. Attorney Offices[8]	$2,074		
Organized Crime and Drug Enforcement Task Forces (OCDETF)[9]	$522		
Department of Homeland Security			
ICE-Homeland Security Investigations	$299[10]		
Secret Service	$768[11]	$588	$628
Department of Health and Human Services			
Center for Medicare and Medicaid Services Health Care Fraud and Abuse Control [12]	$725	$745	$770
Office of the Comptroller of the Currency (OCC)[13]	$38	$40	$42
Federal Deposit Insurance Corporation (FDIC)		$8.6	
National Credit Union Administration (NCUA)[14]	$8	$8	$8
Commodity Futures Trading Commission (CFTC)	$0.39	$0.41	$0.42
Department of Defense	$32	$32	$30
Department of State			
Counterterrorism Financing	$12	$12	TBD
Bureau of International Security and Nonproliferation	$17	$18	$14
Department of Commerce			
Bureau of Industry and Security[15] Export Enforcement	$50	$51	$49

Endnotes

1 These are proposed budget figures which have been requested but have not yet been approved.

2 Department of the Treasury Internal Revenue Service, Congressional Budget Justification and Annual Performance Report and Plan–FY 2019, available at https://www.treasury.gov/about/budget-performance/CJ19/FY%202019%20CJ.pdf.

3 This includes budget figures from FinCEN, which is part of TFI these include (in millions) $115 for FY 2017, $115 for FY 2018 and $277 for FY 2019.

4 A small portion of this budget allocation funds the investigation of money-laundering violations associated with narcotics organizations. Most of the allocation funds the enforcement of criminal statutes relating to violations of internal revenue laws.

5 Amounts reflect allocations for DOJ Strategic Goal 1: Enhance National Security and Counter the Threat of Terrorism. The DOJ has four draft strategic goals for the Department of Justice's FY 2018–2022 Strategic Plan (https://www.justice.gov/jmd/page/file/1033266/download).

6 Only a portion of this budgeted amount is directly applicable to combating illicit finance since the Criminal Division prosecutes a wide range of criminal offences.

7 Only a portion of this budgeted amount is directly applicable to combating illicit finance since the FBI investigates a wide range of criminal offences.

8 Only a portion of this budget allocation is devoted to the staff in 56 U.S. attorney offices, which prosecute the majority of money laundering cases nationally (https://www.justice.gov/jmd/file/822056/download).

9 The Interagency Crime and Drug Enforcement appropriation separately funds the OCDETF Program. A small portion of this budget allocation is devoted to attacking the financial infrastructure of drug organizations (https://www.justice.gov/jmd/file/822091/download).

10 Department of Homeland Security, U.S. Immigration and Customs Enforcement, Operations and Support, FY 2019 Congressional Justification. Annual budget figures for ICE-HSI domestic investigations are presented on page 54. The chart on page 72 showing expenditures in FY 2017 per investigative area within domestic investigations shows that financial investigations were 16% of the total. This percentage was applied to the budgeted figure for domestic investigations for FY 18 and FY 19 to reach an estimate of the budgeted figure for financial investigations.

11 Department of Homeland Security, U.S. Secret Service, Operations and Support, FY 2019 Congressional Justification, page 65.

12 Center for Medicare and Medicaid Services (CMS) Health Care Fraud and Abuse Control (HCFAC) addresses a broad range of improper payments including healthcare fraud and associated money laundering, but also ordinary mistakes and inefficiencies so the budget figures cited cover more than illicit finance.

13 OCC funds are, by statute, not appropriated. 12 USC 481. The Comptroller has sole authority to determine how OCC funds are obligated and its expenses incurred and paid, pursuant to 12 USC 16. The OCC Budget is formulated and approved by the Comptroller in accordance with OCC policies and procedures. The Comptroller is responsible for determining how to meet the responsibilities of the OCC. 12 U.S.C. 1, 481 and 482.

14 The actual (2017) and budgeted figures (2018 and 2019) for the NCUA include resources to review compliance with the BSA during credit union examinations; manage security, threat and emergency management programs; and maintain contacts and communications with the intelligence community. Combatting illicit finance is a subset of the objectives of the functions estimated here.

15 U.S. Department of Commerce, Bureau of Industry and Security, Fiscal Year 2019, Presidential Submission, available at http://www.osec.doc.gov/bmi/budget/FY19CBJ/BIS_FY19_President's_Budget_FINAL.pdf.

List of Acronyms

AML	Anti-Money Laundering
ANF	Al-Nusrah Front
AQ	Al-Qaida
AQAP	Al-Qaida in the Arabian Peninsula
ATF	Bureau of Alcohol, Tobacco, Firearms and Explosives (U.S. Department of Justice)
BAC	Business Affairs Component
BCSC	Bulk Cash Smuggling Center (U.S. Department of Homeland Security)
BIS	Bureau of Industry and Security (U.S. Department of Commerce)
BSA	Bank Secrecy Act
BSAAG	Bank Secrecy Act Advisory Group
CAATSA	Countering America's Adversaries Through Sanctions Act
CBP	U.S. Customs and Border Protection
CES	Counterintelligence and Export Control Section (U.S. Department of Justice)
CFTC	Commodity Futures Trading Commission
CIFG	Counter-ISIS Finance Group
CJNG	Cartel Jalisco Nueva Generación
CMS	Center for Medicare and Medicaid Services
CNTOC	Counter-Narcoterrorism Operations Center
CPC	Counterproliferation Center (Federal Bureau of Investigation)
CPI	Counter-Proliferation Investigations Program (U.S. Department of Homeland Security)
CPOT	Consolidated Priority Target Organization
CPTF	Counter-Proliferation Task Force (U.S. Department of Justice)
CDOD-CTF	Department of Defense - Counter-Threat Finance
CTR	Currency Transaction Report

DEA	Drug Enforcement Administration (U.S. Department of Justice)
DHS	Department of Homeland Security
DOD	Department of Defense
DOJ	Department of Justice
DPRK	Democratic People's Republic of Korea
DSAC	Domestic Security Alliance Council
DTO	Drug Trafficking Organization
E.O.	Executive Order
E2C2	Export Enforcement Coordination Center (U.S. Department of Homeland Security)
EB	Bureau of Economic and Business Affairs (U.S. Department of State)
EBCU	El Paso Intelligence Center Bulk Currency Unit
EDTF	El Dorado Task Force
EPIC	El Paso Intelligence Center
FATF	Financial Action Task Force
FBA	federal banking agencies
FBI	Federal Bureau of Investigation
FCPA	Foreign Corrupt Practices Act
FDIC	Federal Deposit Insurance Corporation
FELEG/MLWG	Five Eyes Law Enforcement Group/Money Laundering Working Group
FFIEC	Federal Financial Institutions Examination Council
FinCEN	Financial Crimes Enforcement Network (U.S. Department of the Treasury)
FINRA	Financial Industry Regulatory Authority
FinTech	Financial Technology
FIU	Financial Intelligence Unit

FRB	Board of Governors of the Federal Reserve System (or "Federal Reserve Board")
FSB	Financial Stability Board
FSOC	Financial Stability Oversight Council
FSRB	FATF-Style Regional Bodies
FTO	Foreign Terrorist Organization
GCC	Gulf Cooperation Council
GPRA	Government Performance and Results Modernization Act
HCFAC	Health Care Fraud and Abuse Control Program
HFNT	Hizballah Financing and Narcoterrorism Team
HIDTA	High Intensity Drug Trafficking Area
HSI	Homeland Security Investigations (U.S. Department of Homeland Security)
ICE	U.S. Immigration and Customs Enforcement (U.S. Department of Homeland Security)
IEEPA	International Emergency Economic Powers Act
INL	Bureau of International Narcotics and Law Enforcement Affairs (U.S. Department of State)
INTERPOL	International Criminal Police Organization
IRGC-QF	Islamic Revolutionary Guard Corps-Qods Force
IRS-CI	Internal Revenue Service-Criminal Investigations
ISIS	Islamic State of Iraq and Syria
ISN	Bureau of International Security and Nonproliferation (U.S. Department of State)
JCPOA	Joint Comprehensive Plan of Action
JTTF	Joint Terrorism Task Force (U.S. Department of Justice)
LECG	Law Enforcement Coordination Group

MLARS	Money Laundering and Asset Recovery Section
MSB	Money Services Business
NCPC	National Counterproliferation Center (Office of the Director of National Intelligence)
NCTC	National Counterterrorism Center (Office of the Director of National Intelligence)
NCUA	National Credit Union Administration
NDTA	National Drug Threat Assessment
NEECN	National Export Enforcement Coordination Network
NFA	National Futures Association
NJTTF	National Joint Terrorism Task Force (U.S. Department of Justice)
NMLRA	National Money Laundering Risk Assessment
NPFRA	National Proliferation Financing Risk Assessment
NPT	Treaty on the Non-Proliferation of Nuclear Weapons
NSD	National Security Division (U.S. Department of Justice)
NSS	National Security Strategy
NTFRA	National Terrorist Financing Risk Assessment
OCC	Office of the Comptroller of the Currency
OCDETF	Organized Crime Drug Enforcement Task Forces (U.S. Department of Justice)
OCIE	Office of Compliance Inspections and Examinations (Securities and Exchange Commission)
ODNI	Office of the Director of National Intelligence
OFAC	Office of Foreign Assets Control (U.S. Department of the Treasury)
OIA	Office of Intelligence and Analysis (U.S. Department of the Treasury)
OIS	Office of Immigration Statistics (U.S. Department of Homeland Security)

ONDCP	Office of National Drug Control Policy (Executive Office of the President)
PF	Proliferation Financing
RegTech	Regulatory Technology
RPOT	Regional Priority Organization Targets
SARs	Suspicious Activity Reports
SDGT	Specially Designated Global Terrorist
SDN	Specially Designated Nationals and Blocked Persons
SEC	Securities and Exchange Commission
SRO	Self-Regulatory Organization
TBML	Trade-Based Money Laundering
TCO	Transnational Criminal Organization
TEOAF	Treasury Executive Office for Asset Forfeiture
TF	Terroristic Financing
TFFC	Terrorist Financing and Financial Crimes (U.S. Department of the Treasury)
TFI	Terrorism and Financial Intelligence (U.S. Department of the Treasury)
TFOS	Terrorist Financing Operations Section (Federal Bureau of Investigation)
TFTC	Terrorist Financing Targeting Center
UN	United Nations
USAID	U.S. Agency for International Development
USSS	U.S. Secret Service
WMD	weapons of mass destruction