FinCEN ADVISORY

FIN-2025-A002 **June 6, 2025**

FinCEN Advisory on the Iranian Regime's Illicit Oil Smuggling Activities, Shadow Banking Networks, and Weapons Procurement Efforts

Introduction

Suspicious Activity Report (SAR) Filing Request:
FinCEN requests that financial institutions reference this Advisory in SAR field 2 ("Filing Institution Note to FinCEN") and the narrative by including the key term "**IRAN-2025-A002**."

The U.S. Department of the Treasury's (Treasury) Financial Crimes Enforcement Network (FinCEN) is issuing this Advisory to assist U.S. financial institutions in identifying and reporting potential sanctions evasion and other suspicious activity related to the Islamic Republic of Iran (Iran). On February 4, 2025, President Trump issued National Security Presidential Memorandum (NSPM-2) announcing a maximum pressure campaign against Iran with the goals of denying Iran nuclear weapons and intercontinental ballistic missiles (ICBMs); countering its development of other weapons capabilities; neutralizing Iran's network and campaign of regional aggression; and disrupting, degrading, and denying Iran, including the Islamic Revolutionary Guard Corps (IRGC),[1] and its terrorist proxies, access to the resources that sustain their destabilizing activities.[2]

To support the implementation of NSPM-2, Treasury's Office of Foreign Assets Control (OFAC) has issued several rounds of designations targeting Iranian oil exports (including illicit use of oil smuggling vessels), which are a significant revenue stream for the regime and its terrorist proxies, and Iranian weapons proliferators.[3] This Advisory supports the U.S. maximum pressure campaign against Iran and replaces FinCEN's 2018 Advisory on the Iranian Regime's Illicit Activities.[4] As such, it provides updated red flags and information on current trends and typologies for Iranian sanctions evasion and other illicit activity, including oil smuggling, "shadow banking" networks, and weapons procurement. It is being issued concurrent with OFAC's June 6 sanctions action, the first such action targeting an Iranian "shadow banking" network since the issuance of NSPM-2.[5]

This Advisory is also consistent with FinCEN's National Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) Priorities, which include terrorist financing and proliferation financing, as well as Treasury's 2024 National Terrorist Financing Risk Assessment and 2024 National Proliferation Financing Risk Assessment.[6]

The information contained in this Advisory is derived from FinCEN's analysis of Bank Secrecy Act (BSA) data, open-source reporting, and information provided by law enforcement partners.

Overview of the Iranian Threat

As noted in NSPM-2, Iran has been a destabilizing influence in the region and around the world since it established a fundamentalist Shi'a Islamic Republic in 1979.[7] Of particular concern are Iran's nuclear program, its asymmetric military capabilities, and its role as the world's leading state sponsor of terror.[8] Furthermore, the U.S. government has repeatedly condemned the Iranian government's lethal plotting against U.S. government officials, Israel, and Iranian dissidents, as well as its human rights violations at home and abroad, including the detention of U.S. citizens and the regime's women's rights abuses.[9] These activities present a credible threat to the United States, its allies and partners, and its interests.

Iran has also sponsored a network of terrorist partners and proxies in neighboring countries, sometimes referred to as the "Axis of Resistance,"[10] which the regime uses to advance its geopolitical interests in the region and around the world through violence and terrorism. These terrorist organizations include Hamas,[11] Lebanese Hizballah (Hizballah),[12] Ansarallah (more commonly known as the Houthis), Palestinian Islamic Jihad (PIJ), and multiple Iran-aligned militia groups in Iraq and Syria.[13] As a result of its financial and material support for Hamas, Iran bears responsibility for the horrific Hamas massacres committed on October 7, 2023 in Israel as well as for the direct ballistic and cruise missile attacks carried out by the regime against Israel since April 2024.[14] Though Iran's "Axis of Resistance" has suffered several setbacks in the past year, including the fall of the Iran-aligned Assad regime in Syria and the significant weakening and degradation of Hizballah and Hamas, this network of actors still presents a range of threats, including Iran-aligned militia group attacks on U.S. military personnel in Iraq and Syria and Houthi attacks against military and commercial shipping vessels in the Red Sea.[15]

To arm itself and its terrorist partners and proxies, Iran has developed a robust ballistic missile program and a large inventory of unmanned aerial vehicles (UAVs). Iran has the largest inventory of ballistic missiles in the region, and U.S. officials have raised concerns that the regime could use its nascent space program to shorten the timeline for Iran's development of ICBMs.[16] Furthermore, Iran's construction of gas centrifuge uranium enrichment facilities has raised concerns that Tehran could attempt to pursue nuclear weapons.[17]

Economically and militarily, Iran has developed strong ties with Russia and China, reflecting what analysts describe as a "look East" strategy favored by Supreme Leader Ali Hosseini Khamenei.[18] Iran's military ties with Russia have deepened since Russia's 2022 full-scale invasion of Ukraine, with Iran supplying UAVs and ballistic missiles to Russia and in exchange receiving advanced fighter jets and air defense systems.[19] Meanwhile, China is Iran's largest trading partner[20] and by far the largest importer of Iranian oil,[21] as well as a key supplier of components for Iranian ballistic missile and UAV programs.[22]

As described below, Iran relies on revenue from oil sales to fund these destabilizing activities.[23] To obscure its involvement in these sales and access the international financial system, the regime utilizes a "shadow fleet" of often old and poorly maintained vessels to move oil globally and a

multijurisdictional "shadow banking" network of financial intermediaries including exchange houses, trading companies, and front companies to move and settle funds and subsequently procure weapons and other capabilities.[24]

Illicit Oil Smuggling Activities

Though limited in its production capacity due to years of underinvestment and international sanctions, Iran's oil and petroleum exports remain a major source of revenue for the regime, and the main source of revenue for its armed forces and terrorist partners and proxies. Most of Iran's oil is sold by the National Iranian Oil Company (NIOC),[25] which is responsible for the exploration, production, refining, and export of oil and petroleum products in Iran.

Iran's budget allots billions of dollars' worth of Iranian oil to Iran's Ministry of Defense and Armed Forces Logistics (MODAFL),[26] the Iranian Armed Forces General Staff (AFGS), and the IRGC-Qods Force (IRGC-QF)[27] for sale on the international market in order to supplement their budgets.[28] Recent budget estimates point to a four-fold dollar increase in oil allocations to Iran's armed forces, exceeding 10 billion dollars annually and totaling over 500,000 barrels per day.[29] By the end of 2025, over half of Iran's total oil proceeds will be allocated to its armed forces while at the same time its population faces economic hardship.[30] As discussed in FinCEN's 2024 Advisory on Iran-backed terrorist organizations, MODAFL and the IRGC-QF, often in conjunction with terrorist partner and proxy groups such as the Houthis and Hizballah, smuggle oil to international buyers and use the proceeds to fund weapons development and terrorist activity in the region.[31]

To entice foreign buyers, Iran often sells its oil below prevailing market prices, offering a significant discount compared to other Gulf states.[32] The overwhelming majority of this oil is sold to small independent oil refineries in China, sometimes referred to as "teapot refineries," some of which have touchpoints with the U.S. financial system.[33] As of April 2025, Iran exported approximately 1.6 million barrels of petroleum a day,[34] nearly all of which went to China.[35]

The reimposition of U.S. sanctions in 2018 severely diminished Iran's ability to finance itself through sales of crude oil and petroleum products. In response, the regime established large-scale global oil smuggling and money laundering networks to surreptitiously access international markets and financial systems to sell crude oil and petroleum products and to use the proceeds to finance weapons development and terrorist activity. These networks establish and use front companies in third-country jurisdictions to obscure Iranian involvement and layer transactions, often exploiting free trade zones that offer favorable conditions for company formation.[36] Iran also relies on brokers operating in key third-country jurisdictions, and a multi-jurisdictional network of shipping facilitators.[37]

Iran's Shadow Fleet

To transport its oil, Iran typically uses a fleet of old and poorly maintained vessels sometimes referred to as the "shadow fleet," "ghost fleet," or "dark fleet," given their opaque ownership and obfuscation tactics and resulting challenges in identifying and tracking vessels carrying sanctioned oil from Iran.[38] Treasury and the Department of State have blocked over 350 vessels for carrying Iranian oil since the reimposition of U.S. sanctions in 2018.[39]

These vessels are often owned and managed by operating or shipping companies in countries outside Iran, mostly in the United Arab Emirates (UAE) and Southeast Asia, which also help facilitate Iranian oil sales by making payments on behalf of the ultimate Iranian beneficiaries for services like storage facilities.[40] These vessels may either be uninsured or underinsured or will rely on previously sanctioned or new and untested insurance providers.[41] Their advanced age, combined with the longer distances that shadow fleet ships travel to disguise the intended destination of their cargo, make Iran's tankers a growing safety risk to port infrastructure, other vessels, and the environment—and deficiencies in insurance may mean that national and port authorities are left to cover the clean-up costs in the event of an oil spill.[42]

The Iranian regime commonly uses front companies operating in countries outside Iran to lease vessels to hide its involvement and to make payments for services required by ships during their voyages, like bunkering, supplies, insurance, and short-term financing. In these cases, the leased vessels may be crewed by complicit co-conspirators.[43] To further obfuscate their connections to Iran, vessels may undergo frequent name changes, changes in nominal ownership, or frequent reflagging in different third-country jurisdictions to disguise their illicit activity. Vessels may also claim a flag of a jurisdiction in which they are not registered, called a "false flag," or may have been flagged by registries that are not authorized to provide flagging services for a particular jurisdiction.[44]

To mask the origin and ultimate destination of their cargo, vessels often engage in deceptive shipping practices, like falsifying cargo and vessel documents, disabling or manipulating automatic identification systems (AIS) on vessels, voyage irregularities, and ship-to-ship transfers.[45] In some instances, Iranian oil is blended with oil from third countries to further disguise its origins, or forged documents will relabel the oil as the product of another jurisdiction, most commonly as "Malaysian blend."[46]

"Shadow Banking" Networks

Iran relies on multi-jurisdictional "shadow banking" networks to sell oil and other commodities abroad, launder the proceeds, and procure weapons and other materiel on the international market. These networks, comprised of exchange houses,[47] trading companies,[48] and foreign front companies, facilitate access to the international financial system for sanctioned Iranian entities such as MODAFL and the IRGC, enabling them to obfuscate their trade with foreign customers and disguise the revenue they generate abroad. Iran's persistent efforts to circumvent U.S. and global sanctions have also been significantly bolstered by a network of facilitators, including

money services businesses (MSBs), legal entities, and trust and company service providers (TCSPs), that have played pivotal roles in orchestrating complex money laundering and sanctions evasion schemes that obscure illicit transactions, provide necessary liquidity across multiple jurisdictions, and further undermine the integrity of the global financial system. Revenue generated through oil sales are laundered through these shadow banking networks and financial facilitators, funding the procurement of components for advanced weapons systems and support to Iran's regional proxy groups. For example, transactions involving these networks have supported Iran's assistance to the Houthis in Yemen, who engaged in a campaign of reckless attacks on global shipping and the provision of ballistic missiles and UAVs to Russia for use in the Russia-Ukraine war.[49]

Exchange houses in Iran are often used to manage numerous front companies and trading companies registered in key third-country jurisdictions such as Hong Kong or the UAE to launder the revenue generated through the illicit sale of Iranian oil and other petroleum products.[50] These front companies—which are often recently incorporated, have minimal to no web presence, and transact in large amounts with no clear business purpose or using falsified invoices—are used to establish bank accounts outside of Iran that enable sanctioned persons to access the international banking system to receive funds and make payments to foreign entities.[51] According to BSA data, Hong Kong-based companies that bank with China-based financial institutions using non-resident accounts and UAE-based general trading companies registered in commercial free trade zones are commonly used as front companies by Iranian actors.

The exchange houses also use these front companies to launder the revenue and use it at the direction of sanctioned Iranian entities, including MODAFL, to procure weapons components and other materiel from the international market.[52] By using front company accounts outside of Iran to both receive and remit payments, sanctioned Iranian entities may be able to conduct transactions through the international financial system without ever repatriating funds to Iran. According to BSA data, indications that front companies are controlled by Iranian actors may include links to Iranian companies, such as shared counterparties, addresses, and name similarities, or a history of facilitating shipments to and from Iran according to trade data. To further obfuscate their activities, one front company may be used to transact on behalf of multiple sanctioned entities and may receive, as well as remit, funds through its accounts.

Another model used by Iran to evade sanctions and access the U.S. financial system is through third-country exchange houses and trading companies. These third-country exchange houses and trading companies rely on their regional banks, which have correspondent banking relationships with U.S. financial institutions, to access the U.S. financial system. The exchange houses convert the foreign currency into U.S. dollars using forged documents that falsify the source of the funds. The dollars are then delivered to regime personnel or proxies outside of Iran to facilitate the movement of commodities like oil or the procurement of sensitive dual-use goods. These exchange houses and trading companies often are located in jurisdictions in close geographical proximity to Iran and primarily process commercial transactions rather than personal remittances.[53]

Case Study

Treasury Sanctions Iranian Shadow Banking Network Laundering Billions for the Iranian Regime

On June 6, 2025, OFAC designated over 40 individuals and entities tied to Iranian brothers Mansour, Nasser, and Fazlolah Zarringhalam, who, primarily through Iranian exchange houses they control, have collectively laundered billions of dollars' worth of funds through the international financial system as part of Iran's "shadow banking" network. The regime leverages this network to evade sanctions and move money from its oil and petrochemical sales, which help the regime fund its nuclear and missile programs and support its terrorist proxies.

Through a network of front companies in the UAE and Hong Kong, the Zarringhalam brothers assisted sanctioned regime officials and affiliated businessmen in receiving payments from the sale of petroleum, petroleum products, and other commodities from foreign purchasers. The Zarringhalam network is used by Iran's main oil and petrochemical exporters, as well as the Iranian military, to evade sanctions and send and receive funds related to oil and petrochemical sales.

Mansour Zarringhalam (Mansour) and Nasser Zarringhalam (Nasser) operate Iran-based exchange houses Mansour Zarrin Ghalam and Partners Company (also known as GCM Exchange), and Nasser Zarrin Ghalam and Partners Company (also known as Berelian Exchange), respectively, through which they oversee a sprawling network of front companies, largely operating out of the UAE and Hong Kong. These front companies operate accounts in multiple currencies at various banks to facilitate payments for blocked Iranian entities engaged in the sale of Iranian oil and petrochemicals, among other goods, including the IRGC-QF.[54]

Weapons Procurement Efforts

The Iranian regime uses revenue generated through Iranian oil sales to procure weapons components, dual-use goods, and chemicals from the international market, primarily for its ballistic missile and UAV programs. Iran has the largest ballistic missile program in the Middle East, with more than 10 distinct ballistic missile systems either in its inventory or under development.[55] Similarly, Iran has increased its inventory of both armed and unarmed UAVs, which it has sold to the Houthis over the past 10 years and, more recently, to Russia.[56]

To obtain critical components for these weapons development programs, Iran seeks foreign-produced goods and technologies, many of which it cannot produce in sufficient quantities and qualities.[57] To prevent Iran's acquisition of these items, the United States imposes substantial controls on exports to Iran, which Iran seeks to evade via elaborate, long-standing networks of procurement agents, front companies, intermediaries, and suppliers operating in third countries and regions, including China, including Hong Kong, Türkiye, and Southeast Asia.[58] These procurement networks use a

variety of techniques to further obscure Iran as the end user, including transaction layering, falsifying documentation, and transshipping through third countries.[59] Iranian procurement networks also often use corporate vehicles, like front companies, to hide the source of funds, countries involved, and the identity of the end user.[60]

Case Study

Sahara Thunder

In April 2024, OFAC designated Sahara Thunder, the main front company that oversaw MODAFL's commercial activities in support of the clandestine sale of Iranian UAVs. Sahara Thunder also played a key role in Iran's sale of thousands of UAVs, many of them ultimately transferred to Russia for use in Ukraine.

The Iranian government allocates billions of dollars' worth of oil and other commodities to Iranian military entities including MODAFL and the AFGS as part of the Iranian military's annual budget. MODAFL has cooperated with Russia to finance and produce Iranian-designed one-way attack UAVs at the U.S.-sanctioned Joint Stock Company Special Economic Zone of Industrial Production Alabuga facility in Russia under an approximately $1.75 billion contract. As of late 2022, Russian officials were negotiating a deal for Sahara Thunder to deliver and produce thousands of UAVs per year at this facility. Such UAVs have been used by the Russian military in Ukraine against critical infrastructure and civilian targets.

Sahara Thunder, acting on behalf of MODAFL, relied on a vast shipping network involved in the sale and shipment of Iranian commodities to multiple jurisdictions, including China, Russia, and Venezuela.[61] Proceeds from these sales were laundered through exchange houses in Iran and then transferred through shadow banking networks to be used at the direction of MODAFL to acquire weapons components and other materiel on the international market.[62]

Red Flags Related to Illicit Iranian Activity

FinCEN has identified the red flags listed below, some of which were included in the 2018 Advisory and remain valid, to assist financial institutions in detecting, preventing, and reporting suspicious activity connected to Iranian illicit financial activity. As no single red flag is determinative of illicit or suspicious activity, financial institutions should consider the surrounding facts and circumstances, such as a customer's historical financial activity, whether the transactions are in line with prevailing business practices, and whether the customer exhibits multiple red flags, before determining if a behavior or transaction is indicative of Iranian illicit financial activity or is otherwise suspicious.

Red Flags Associated with Illicit Oil Smuggling and Sales

1. Documentation associated with a customer's oil shipping-related transactions is inconsistent with information contained in maritime database entries used for conducting due diligence. For example, a maritime database may indicate that a vessel called in an Iranian port, even though this information is not included in the shipping documents submitted to financial institutions for payment processing.[63]

2. Documentation associated with a customer's oil-related transactions makes reference to vessels that, according to maritime databases, have undergone recent or multiple name or flag changes, or transfer of ownership or operation to another person following OFAC's designation of its owner or operator, but the designated owner or operator appears to maintain an interest in the vessel.

3. Documentation associated with a customer's oil-related transactions makes reference to vessels that claim an International Maritime Organization (IMO) number that, on examination of maritime databases, belong to a different vessel or to vessels that have previously been scrapped.

4. Documentation associated with a customer's oil-related transactions makes reference to "Malaysian blend" oil, particularly if the vessel is bound for China by way of Southeast Asia and if maritime databases indicate that the vessel displayed AIS irregularities during its voyage or reveal evidence of a ship-to-ship transfer in proximity to Southeast Asia.

5. Transactions involving a petroleum or shipping company reveal that it does business with counterparties that have ties to Iran or transports goods using vessels that have ties to Iran or that maritime databases indicate have made stops at Iranian ports.

6. A customer makes oil-related transactions and wire transfers involving vessels that have been previously linked to suspicious financial activities or that include documentation, such as bills of lading or shipping invoices, with no consignees, that appear to be falsified, or that omit key information, in an attempt to hide the Iranian nexus.

Red Flags Associated with Iranian Shadow Banking Networks

1. A customer makes transactions that move through multiple exchange houses and/or trading companies, adding additional fees and costs as the transactions progress, where the fees, number of transactions, and pattern of transactions do not reflect standard and customary commercial practices.

2. An exchange house or trading company in a jurisdiction in close geographical proximity to Iran uses forged or falsified documents to conceal the identity of parties involved in transactions that will utilize regional banks' correspondent banking relationships with U.S. financial institutions to access U.S. dollars.

3. A customer receives wire transfers or deposits that do not contain any information about the source of funds, contain incomplete information about the source of funds, or do not match the customer's line of business, especially if they involve entities in a high-risk jurisdiction for Iranian illicit finance-related activity.

4. A general trading company registered in a commercial free trade zone in the UAE with opaque ownership and whose trading counterparties are companies mostly located in Singapore and Hong Kong has bank accounts at multiple UAE financial institutions.

5. A company based in Hong Kong, that banks using a Chinese non-resident account, has little to no web presence, is co-located with numerous other similar companies, or is recently incorporated yet transmitting large payments with no adequate explanation for the source of funds, makes numerous payments in large figures to UAE general trading companies with no clear business purpose.

Red Flags Associated with Iranian Weapons Procurement Networks

1. A customer makes transactions involving companies that originate with, or are directed to, entities that are general trading companies, suspected front companies, or companies that have a nexus with Iran. Other indicators of possible front companies include opaque ownership structures, individuals/entities with obscure names that direct the company, or business addresses that are residential or co-located with other companies, especially companies that have been previously sanctioned.

2. A customer declares information about the nature of its business that is inconsistent with other available information, such as previous transaction history or associated transactional information, particularly if trade data indicates that they have a history of facilitating shipments to and from Iran and if they transact predominantly with technology companies or chemical suppliers.

3. A customer makes transactions that are directed to companies that operate in unrelated businesses, and which do not seem to align with the customer due diligence (CDD) and other customer identification information collected during client onboarding and subsequent updates. For example, and of note with regard to illicit Iranian financial activity, customers that primarily receive funds from commodities trading companies, but send funds primarily to electronics suppliers.

4. Multiple companies incorporated at roughly the same time share counterparties, addresses, owners, or name similarities and demonstrate similar transaction profiles. Such companies may have little to no web presence and transact in large, recurring amounts.

5. A company based in the Middle East with links to Iran or that shows indications of being a front company receives payments primarily from petroleum companies and then makes payments primarily to electronics companies based in Hong Kong and China.

Reminder of Relevant BSA Obligations and Tools for U.S. Financial Institutions
Suspicious Activity Reporting
Law Enforcement Filing Tips
Other Relevant BSA Reporting

Suspicious Activity Reporting

A financial institution is required to file a suspicious activity report (SAR) if it knows, suspects, or has reason to suspect a transaction conducted or attempted by, at, or through the financial institution involves funds derived from illegal activity; is intended or conducted to disguise funds derived from illegal activity; is designed to evade regulations promulgated under the BSA; lacks a business or apparent lawful purpose; or involves the use of the financial institution to facilitate criminal activity.[64] All statutorily defined financial institutions may voluntarily report suspicious transactions under the existing suspicious activity reporting safe harbor.[65]

When a financial institution files a SAR, it is required to maintain a copy of the SAR and the original or business record equivalent of any supporting documentation for a period of five years from the date of filing the SAR.[66] Financial institutions must provide any requested documentation supporting the filing of a SAR upon request by FinCEN or an appropriate law enforcement or supervisory agency.[67] When requested to provide supporting documentation, financial institutions should take special care to verify that a requestor of information is, in fact, a representative of FinCEN or an appropriate law enforcement or supervisory agency. A financial institution should incorporate procedures for such verification into its BSA compliance or AML program. These procedures may include, for example, independent employment verification with the requestor's field office or face-to-face review of the requestor's credentials.

SAR Filing Instructions

SARs, and compliance with other BSA requirements, are crucial to identifying and stopping illicit Iranian financial activity. FinCEN requests that financial institutions indicate any connection between the suspicious activity being reported and the activities highlighted in this Advisory by including the key term "**IRAN-2025-A002**" in SAR field 2 ("Filing Institution Note to FinCEN"), as well as in the narrative. Financial institutions may highlight additional advisory or notice keywords in the narrative, if applicable.

As appropriate, financial institutions should select SAR Field 33(a) (Terrorist Financing-Known or suspected terrorist/terrorist organization) as the associated suspicious activity type if there is a suspected nexus to an Iran-backed terrorist organization. Financial institutions also should select all other relevant suspicious activity fields, such as those in SAR Fields 36 (Money Laundering) and 38 (Other Suspicious Activities), if applicable.

Financial institutions should include all available information relating to the account and locations involved in the reported activity, identifying information related to other entities and persons involved in the depositing or cashing of suspicious checks and the status of their accounts with the institution. Financial institutions also should provide all available information regarding other domestic and foreign financial institutions involved in the activity; where appropriate, financial institutions should consider filing a SAR jointly on shared suspicious activity.[68]

Financial institutions are required to file complete and accurate reports that incorporate all relevant information available. In situations involving violations requiring immediate attention, such as ongoing money laundering schemes, financial institution must also immediately notify, by telephone, an appropriate law enforcement authority, in addition to filing a timely SAR.[69] Immediate notification to law enforcement is especially important in situations involving suspected terrorist activity, as terrorists and terrorist organizations often rely on the international financial system to acquire funding to sustain and finance their operations and engage in acts of terrorism. Additionally, FinCEN emphasizes that a financial institution, and any director, officer, employee, or agent of the financial institution that makes a voluntary disclosure of any possible violation of law or regulation is protected from liability to any person for any such disclosure.[70]

Financial institutions wanting to report suspicious transactions that may potentially relate to terrorist activity should call the Financial Institutions Toll-Free Hotline at (866) 556-3974 (7 days a week, 24 hours a day).[71]

Other Relevant BSA Reporting Requirements

Financial institutions and other entities or persons may also have other relevant BSA reporting requirements to provide information in connection with the subject of this Advisory. These include obligations related to the Currency Transaction Report (CTR),[72] Report of Cash Payments Over $10,000 Received in a Trade or Business (Form 8300),[73] Report of Foreign Bank and Financial Accounts (FBAR),[74] Report of International Transportation of Currency or Monetary Instruments (CMIR),[75] Registration of Money Services Business (RMSB),[76] and Designation of Exempt Person (DOEP).[77]

Due Diligence

Banks, brokers or dealers in securities, mutual funds, and futures commission merchants and introducing brokers in commodities are required to have appropriate risk-based procedures for conducting ongoing customer due diligence that include, but are not limited to: (i) understanding the nature and purpose of customer relationships for the purpose of developing a customer risk profile; and (ii) conducting ongoing monitoring to identify and report suspicious transactions and, on a risk basis, to maintain and update customer information.[78] Covered financial institutions are required to identify and verify the identity of beneficial

owners of legal entity customers, subject to certain exclusions and exemptions.[79] Among other things, this facilitates the identification of legal entities that may be owned or controlled by foreign politically exposed persons (PEPs).

Senior foreign political figures and due diligence obligations for private banking accounts

In addition to these due diligence obligations, under section 312 of the USA PATRIOT Act (31 U.S.C. § 5318(i)) and its implementing regulations, covered financial institutions must implement due diligence programs for private banking accounts held for non-U.S. persons that are designed to detect and report any known or suspected money laundering or suspicious activity conducted through or involving such accounts.[80] Covered financial institutions must establish risk-based controls and procedures for ascertaining the identities of nominal and beneficial owners of such accounts and ascertaining whether any of these owners are senior foreign political figures, and for conducting enhanced scrutiny on accounts held by senior foreign political figures that is reasonably designed to detect and report transactions that may involve the proceeds of foreign corruption.[81]

AML/CFT program and correspondent account due diligence requirements

Financial institutions are reminded of AML/ program requirements,[82] and covered financial institutions are reminded of correspondent account due diligence requirements under Section 312 of the USA PATRIOT Act (31 U.S.C. § 5318(i)) and implementing regulations.[83] As described in FinCEN Interpretive Release 2004-1, the AML program of an MSB must include risk-based policies, procedures, and controls designed to identify and minimize risks associated with foreign agents and counterparties.[84]

Information Sharing

Information sharing among financial institutions is critical to identifying, reporting, and preventing terrorist financing. Financial institutions and associations of financial institutions sharing information under the safe harbor authorized by section 314(b) of the USA PATRIOT Act are reminded that they may share information with one another regarding individuals, entities, organizations, and countries suspected of possible terrorist financing or money laundering.[85] In accordance with the requirements of section 314(b) and its implementing regulations, FinCEN strongly encourages such voluntary information sharing as it relates to money laundering or possible terrorist financing in connection with Foreign Terrorist Organizations (FTOs)[86] and Specially Designated Global Terrorists (SDGTs).[87]

For Further Information

FinCEN's website at www.fincen.gov contains information on how to register for FinCEN Updates. Questions or comments regarding the contents of this Advisory should be addressed to the FinCEN Regulatory Support Section at www.fincen.gov/contact.

The mission of the Financial Crimes Enforcement Network is to safeguard the financial system from illicit use, counter money laundering and the financing of terrorism, and promote national security through strategic use of financial authorities and the collection, analysis, and dissemination of financial intelligence.

1. The IRGC is a parallel military institution to Iran's regular armed forces and is responsible for defending Iran's Islamic revolutionary regime. The IRGC was designated by Treasury as a Specially Designated Global Terrorist (SDGT) on October 13, 2017, pursuant to Executive Order (E.O.) 13224. E.O. 13224, 66 Fed. Reg. 49, 79 (Sept. 23, 2001). It was added to the U.S. Department of State's Foreign Terrorist Organization (FTO) list on April 15, 2019. *See* Treasury, "Treasury Designates the IRGC under Terrorism Authority and Targets IRGC and Military Supporters under Counter-Proliferation Authority" (Oct. 13, 2017). *See also* Department of State, "Designation of the Islamic Revolutionary Guard Corps" (Apr. 8, 2019). For more information about the IRGC, *see* Director of National Intelligence (DNI) National Counter Terrorism Center (NCTC) "Islamic Revolutionary Guard Corps" (Mar. 2025).

2. The White House, "National Security Presidential Memorandum/NSPM-2: Imposing Maximum Pressure on the Government of the Islamic Republic of Iran, Denying Iran All Paths to a Nuclear Weapon, and Countering Iran's Malign Influence" ("NSPM-2") (Feb. 4, 2025).

3. *See* Treasury, "Treasury Targets Oil Network Generating Hundreds of Millions of Dollars for Iran's Military" (Feb. 6, 2025); "Treasury Imposes Additional Sanctions on Iran's Shadow Fleet as Part of Maximum Pressure Campaign" ("Feb. 2025 Treasury Shadow Fleet Press Release") (Feb. 24, 2025); "Treasury Targets Covert Iranian UAV Procurement Network" ("Feb. 2025 Treasury UAV Press Release") (Feb. 26, 2025); "Treasury Sanctions Iranian Oil Minister, Shadow Fleet Operators" ("Mar. 2025 Treasury Press Release") (Mar. 13, 2025); "Treasury Sanctions Network Supporting Iran's Oil Exports" ("Mar. 2025 Treasury Oil Network Press Release") (Mar. 20, 2025); "The Departments of Treasury and Justice Take Action Against Iranian Weapons Procurement Network" (Apr. 1, 2025); "Treasury Imposes Sanctions on Enablers of Iran's Nuclear Program" (Apr. 9, 2025); "Treasury Targets Network Transporting Hundreds of Millions of Dollars' Worth of Iranian Petroleum" (Apr. 10, 2025); "Treasury Increases Pressure on Chinese Importers of Iranian Oil" ("Apr. 2025 Treasury Chinese Oil Importers Press Release") (Apr. 16, 2025).

4. *See* FinCEN, FIN-2018-A006, "Advisory on the Iranian Regime's Illicit Activities and Attempts to Exploit the Financial System" (Oct. 11, 2018).

5. Treasury, "Treasury Sanctions Iranian Network Laundering Billions for Regime Through Shadow Banking Scheme" ("June 2025 Treasury Shadow Banking Press Release") (June 6, 2025).

6. *See* FinCEN, "Anti-Money Laundering and Countering the Financing of Terrorism National Priorities" (June 30, 2021); Treasury, "2024 National Terrorist Financing Risk Assessment," ("Feb. 2024 NTFRA") (Feb. 2024), at p. 1; "2024 National Proliferation Financing Risk Assessment," at pp. 5-6.

7. *See* NSPM-2, *supra* note 2.

8. *See* Feb. 2024 NTFRA, *supra* note 6, at p. 1. The U.S. Department of State designated the Islamic Republic of Iran as a State Sponsor of Terrorism in 1984 pursuant to three laws: section 1754(c) of the National Defense Authorization Act for Fiscal Year 2019, section 40 of the Arms Export Control Act, and section 620A of the Foreign Assistance Act of 1961. Taken together, the four main categories of sanctions resulting from designation under these authorities include restrictions on U.S. foreign assistance; a ban on defense exports and sales; certain controls over exports of dual use items; and miscellaneous financial and other restrictions. *See* Department of State, "State Sponsors of Terrorism" (accessed Mar. 4, 2025).

9. As a prominent example, protests spread across Iran in response to the September 2022 death of 22-year-old Mahsa Amini, who was arrested by Iran's Morality Police for allegedly violating Iran's mandatory hijab law and died after reportedly having been beaten in custody. *See* Congressional Research Service (CRS), "Iran: Background and U.S. Policy" ("Dec. 2024 CRS Report") (Dec. 30, 2024), at pp. 1, 16, 23. *See also* Department of State, "Joint Statement Two Years After Mahsa Zhina Amini's Death" (Sept. 16, 2024); NSPM-2, *supra* note 2.

10. *See* Dec. 2024 CRS Report, *supra* note 9, at p. 3.

11. *See* FinCEN, FIN-2023-Alert006, "FinCEN Alert to Financial Institutions to Counter Financing to Hamas and its Terrorist Activities" (Oct. 20, 2023).

12. *See* FinCEN, FIN-2024-Alert003, "FinCEN Alert to Financial Institutions to Counter Financing of Hizballah and its Terrorist Activities" (Oct. 23, 2024).

13. For more information about the financing of Iran's terrorist partners and proxies, *see* FinCEN, FIN-2024-A001, "FinCEN Advisory to Financial Institutions to Counter the Financing of Iran-Backed Terrorist Organizations" ("May 2024 FinCEN Advisory") (May 8, 2024).

14. *See* NSPM-2, *supra* note 2.

15. *See* Office of the Director of National Intelligence (ODNI), "Annual Threat Assessment of the U.S. Intelligence Community" (Mar. 2025), at p. 22; NSPM-2, *supra* note 2.

16. *See* ODNI, "Iran's Nuclear Weapons Capability and Terrorism Monitoring Act of 2022—Assessment Regarding the Nuclear Activity of the Islamic Republic of Iran" (Nov. 2024), at p. 2.

17. *See* Dec. 2024 CRS Report, *supra* note 9, at pp. 18-19.

18. *Id*. at p. 14.

19. *See* ODNI, "DNI Gabbard Opening Statement for the SSCI As Prepared on the 2025 Annual Threat Assessment of the U.S. Intelligence Community" (Mar. 25, 2025).

20. *See* Dec. 2024 CRS Report, *supra* note 9, at p. 15.

21. *See* CRS, "Iran's Petroleum Exports to China and U.S. Sanctions" (Mar. 28, 2025), at p. 1.

22. *See, e.g.*, Feb. 2025 Treasury UAV Press Release, *supra* note 3.

23. *See* OFAC, "Guidance for Shipping and Maritime Stakeholders on Detecting and Mitigating Iranian Oil Sanctions Evasion" ("Apr. 2025 OFAC Guidance") (Apr. 16, 2025), at p. 1.

24. *See* Treasury, "Treasury Targets Sanctions Evasion Network Moving Billions for Iranian Regime" ("Mar. 2023 Treasury Press Release") (Mar. 9, 2023); "From FinCEN: Treasury Convenes Financial Institutions, Law Enforcement, in Washington, D.C. in Support of the U.S. Maximum Pressure Campaign Against Iran" (Apr. 2, 2025).

25. NIOC was designated pursuant to E.O. 13224 on Oct. 26, 2020. E.O. 13224, 66 Fed. Reg. 49, 79 (Sept. 23, 2001). *See* Treasury, "Treasury Sanctions Key Actors in Iran's Oil Sector for Supporting Islamic Revolutionary Guard Corps-Qods Force" ("Oct. 2020 Treasury Press Release") (Oct. 26, 2020).

26. MODAFL was designated pursuant to E.O. 13382 on Oct. 25, 2007. E.O. 13382, 70 Fed. Reg. 38567 (July 1, 2005). *See* Treasury, "Fact Sheet: Designation of Iranian Entities and Individuals for Proliferation Activities and Support for Terrorism" (Oct. 25, 2007).

27. The IRGC-QF was designated pursuant to E.O. 13224 on Oct. 25, 2007. *Id*. *See also* Mar. 2025 Treasury Press Release, *supra* note 3.

28. *See* Mar. 2025 Treasury Press Release, *supra* note 3.

29. *Id*.

30. *Id*.; Oct. 2020 Treasury Press Release, *supra* note 25.

31. *See* May 2024 FinCEN Advisory, *supra* note 13, at p. 3; Treasury, "Treasury Maintains Pressure on Iranian Shadow Fleet" ("Dec. 2024 Treasury Press Release") (Dec. 19, 2024).

32. CRS, "Iran's Petroleum Exports to China and U.S. Sanctions" ("Feb. 2024 CRS Report") (Feb. 28, 2024), at p. 2.

33. *Id*. at p. 2; Mar. 2025 Treasury Oil Network Press Release, *supra* note 3; Apr. 2025 Treasury Chinese Oil Importers Press Release, *supra* note 3.

34. *See* Apr. 2025 OFAC Guidance, *supra* note 23, at p. 1.

35. *See* Feb. 2024 CRS Report, *supra* note 32, at p. 2.

36. Department of Justice (DOJ), "Justice Department Announces Terrorism and Sanctions-Evasion Charges and Seizures Linked to Illicit, Billion-Dollar Global Oil Trafficking Network That Finances Iran's Islamic Revolutionary Guard Corps and Its Malign Activities" ("Feb. 2024 DOJ Press Release") (Feb. 2, 2024); "Department of Justice Wins Forfeiture of $12 Million Connected to Iran's Illicit Petroleum Industry" (Dec. 12, 2024). *See* June 2025 Treasury Shadow Banking Press Release, *supra* note 5.

37. *See* Feb. 2025 Treasury Shadow Fleet Press Release, *supra* note 3; Treasury, "Treasury Expands Targeted Sanctions on Iranian Petroleum and Petrochemical Sectors in Response to Attack on Israel" (Oct. 11, 2024); "Treasury Targets Financial and Shipping Facilitators of Iranian Petrochemicals and Petroleum Sales" (Sept. 29, 2022).

38. CRS, "The Global Oil Tanker Market: An Overview as it Relates to Sanctions" ("Mar. 2024 CRS Report") (Mar. 18, 2024), at pp. 1, 5. These terms are also used to characterize tankers used to transport sanctioned oil from Russia and Venezuela.

39. For recent examples, *see* Treasury, "Treasury Increases Pressure on Chinese Importers of Iranian Oil" (Apr. 16, 2025); "Treasury Targets Global Network Shipping Iranian Oil, Funding Iran's Military and Terrorist Activities" (May 13, 2025).

40. *See* Dec. 2024 Treasury Press Release, *supra* note 31; Treasury, "Treasury Sanctions Companies Involved in Production, Sale, and Shipment of Iranian Petrochemicals and Petroleum" (Feb. 9, 2023); DOJ, "Justice Department Announces First Criminal Resolution Involving the Illicit Sale and Transport of Iranian Oil in Violation of U.S. Sanctions" (Sept. 8, 2023).

41. *See* Apr. 2025 OFAC Guidance, *supra* note 23, at p. 6.

42. *See* Mar. 2024 CRS Report, *supra* note 38, at pp. 4-5, 16.

43. *See* Feb. 2024 DOJ Press Release, *supra* note 36.

44. *See* Apr. 2025 OFAC Guidance, *supra* note 23, at p. 2. *See also* Mar. 2024 CRS Report, *supra* note 38, at p. 8.

45. For more information about Iranian deceptive shipping practices and mitigation measures, *see* Apr. 2025 OFAC Guidance, *supra* note 23, at pp. 3-5.

46. Iranian oil smugglers frequently receive falsified documents in Southeast Asia relabeling their product as "Malaysian blend," despite the fact that Malaysia produces relatively little oil, before it is transported onward to refineries in China. Financial institutions may see indications of these deceptive shipping practices in the information contained in international wires, payment requests, and letters of credit. To verify trade-related documents, financial institutions may find maritime databases helpful, as well as reports, such as those generated by the International Maritime Bureau or other available services. *See, e.g.*, International Chamber of Commerce International Crime Bureau; Treasury, "Treasury Sanctions Oil Shipping Network Supporting IRGC-QF and Hizballah" (Nov. 3, 2022); Feb. 2024 DOJ Press Release, *supra* note 36.

47. Exchange houses are financial institutions licensed to deal in foreign exchange and transmit funds on behalf of individuals and companies.

48. Trading companies are entities that are not licensed to transmit funds, but in practice operate as exchange houses and rely upon their bank accounts to transmit funds on behalf of third parties.

49. *See, e.g.*, Treasury, "Treasury Targets Shadow Banking Network Moving Billions for Iran's Military" ("June 2024 Treasury Press Release") (June 25, 2024).

50. *See* Mar. 2023 Treasury Press Release, *supra* note 24; Treasury, "United States Disrupts Large Scale Front Company Network Transferring Hundreds of Millions of Dollars and Euros to the IRGC and Iran's Ministry of Defense" (Mar. 26, 2019).

51. OFAC, "Iran Ballistic Missile Procurement Advisory" ("Oct. 2023 OFAC Guidance") (Oct. 18, 2023), at p. 4.

52. *See* June 2024 Treasury Press Release, *supra* note 49; Feb. 2025 Treasury UAV Press Release, *supra* note 3.

53. *See* OFAC, "The Use of Exchange Houses and Trading Companies to Evade U.S. Economic Sanctions Against Iran" (Jan. 10, 2013), at p. 2.

54. *See* June 2025 Treasury Shadow Banking Press Release, *supra* note 5.

55. *See* Oct. 2023 OFAC Guidance, *supra* note 51, at p. 3.

56. *See* OFAC, "Guidance to Industry on Iran's UAV-Related Activity" ("June 2023 OFAC Guidance") (June 9, 2023), at pp. 1-2. *See also* Treasury, "Treasury Targets Networks Facilitating Illicit Trade and UAV Transfers on Behalf of Iranian Military" ("Apr. 2024 Treasury UAV Press Release") (Apr. 25, 2024).

57. *See, e.g.*, DOJ " Iranian Company and Two Iranian Nationals Charged with Conspiring to Provide Material Support to Islamic Revolutionary Guard Corps (IRGC) and for Scheme to Procure U.S. Technology for Iranian Attack Drones" (Apr. 1, 2025).

58. *See generally*, Bureau of Industry and Security, "Guidance on Actions Exporters Can Take to Prevent Illicit Diversion of Items to Support Iran's Nuclear Weapons or Ballistic Missile Programs" (accessed Mar. 19, 2025). *See also* Treasury, "Treasury Sanctions Actors Supporting Iran's Missile and UAV Programs" (Oct. 18, 2023); Feb. 2025 Treasury UAV Press Release, *supra* note 3; "Treasury Targets Multiple Procurement Networks Supporting Iran's Proliferation-Sensitive Programs" (Mar. 20, 2024).

59. *See* Oct. 2023 OFAC Guidance, *supra* note 51, at pp. 3-4; DOJ, "Chinese Nationals Charged with Illegally Exporting U.S.-Origin Electronic Components to Iran and Iranian Military Affiliates" (Jan. 31, 2024).

60. *See* June 2023 OFAC Guidance, *supra* note 56, at p. 9; DOJ, "Iranian National Extradited to the Western District of Texas for Illegally Exporting Military Sensitive Items from the U.S. to Iran" (Mar. 17, 2020); Department of Commerce, "Commerce Department Adds 34 Entities to the Entity List to Target Enablers of China's Human Rights Abuses and Military Modernization, and Unauthorized Iranian and Russian Procurement" (July 9, 2021).

61. *See* Apr. 2024 Treasury UAV Press Release, *supra* note 56.

62. *See* June 2024 Treasury Press Release, *supra* note 49.

63. Major ports in Iran are: Bandar Abbas, Assaluyeh, and Bandar-e Emam Khomenyi, which is also known as Abadan. Port cities on the Gulf include Ahvaz, Bushehr, Bandar-e Lengeh, Bandar-e Mahshahr, Chabahar, Kharg Island, and Lavan Island. Kharg Island and Lavan Island are major oil and gas ports.

64. 31 U.S.C. § 5318(g)(1); 31 CFR §§ 1020.320, 1021.320, 1022.320, 1023.320, 1024.320, 1025.320, 1026.320, 1029.320, 1030.320.

65. *See* 31 U.S.C. § 5318(g)(3). Financial institutions may report suspicious transactions regardless of amount involved and still take advantage of the safe harbor.

66. *See* 31 CFR §§ 1020.320(d), 1021.320(d), 1022.320(c), 1023.320(d), 1024.320(c), 1025.320(d), 1026.320(d), 1029.320(d), 1030.320(d).

67. *Id.*; FinCEN, "Suspicious Activity Report Supporting Documentation" (June 13, 2007).

68. *See* 31 CFR §§ 1020.320(e)(1)(ii)(A)(2))(i), 1021.320(e)(1)(ii)(A)(2)), 1022.320(d)(1)(ii)(A)(2), 1023.320(e)(1)(ii)(A)(2)(i), 1024.320(d)(1)(ii)(A)(2), 1025.320(e)(1)(ii)(A)(2), 1026.320(e)(1)(ii)(A)(2)(i), 1029.320(d)(1)(ii)(A)(2), 1030.320(d)(1)(ii)(A)(2).

69. *See* 31 CFR §§ 1020.320(b)(3), 1021.320(b)(3), 1022.320(b)(3), 1023.320(b)(3), 1024.320(b)(4), 1025.320(b)(3), 1026.320(b)(3), 1029.320(b)(4), 1030.320(b)(4).

70. 31 U.S.C. 5318(g)(3); 31 CFR §§ 1020.320(f), 1021.320(f), 1022.320(e), 1023.320(f), 1024.320(e), 1025.320(f), 1026.320(f), 1029.320(e), 1030.320(e).

71. The purpose of the hotline is to expedite the delivery of this information to law enforcement. Financial institutions should immediately report any imminent threat to local-area law enforcement officials.

72. A report of each deposit, withdrawal, exchange of currency, or other payment or transfer, by, through, or to a financial institution that involves a transaction in currency of more than $10,000. Multiple transactions may be aggregated when determining whether the reporting threshold has been met. *See* 31 CFR §§ 1010.310-313, 1020.310-313, 1021.310-313, 1022.310-313, 1023.310-313, 1024.310-313, and 1026.310-313.

73. A report filed by a trade or business that receives currency in excess of $10,000 in one transaction or two or more related transactions. The transactions are required to be reported on a joint FinCEN/Internal Revenue Service form when not otherwise required to be reported on a CTR. *See* 31 CFR §§ 1010.330-331. A Form 8300 also may be filed voluntarily for any suspicious transaction, even if the total amount does not exceed $10,000.

74. A report filed by a U.S. person that has a financial interest in, or signature or other authority over, foreign financial accounts with an aggregate value exceeding $10,000 at any time during the calendar year. *See* 31 CFR § 1010.350; FinCEN Form 114.

75. A form filed to report the transportation of more than $10,000 in currency or other monetary instruments into or out of the United States. *See* 31 CFR § 1010.340.

76. A form filed to register a money services business (MSB) with FinCEN, or to renew such a registration. *See* 31 CFR § 1022.380.

77. A report filed by banks to exempt certain customers from currency transaction reporting requirements. *See* 31 CFR § 1010.311.

78. *See* 31 CFR §§ 1020.210(a)(2)(v), 1023.210(b)(5), 1024.210(b)(6), 1026.210(b)(5).

79. *See* 31 CFR §§ 1010.230, 1010.650(e)(1) (defining "covered financial institution").

80. *See* 31 CFR § 1010.620. The definition of "covered financial institution" is found in 31 CFR § 1010.605(e)(1). The definition of "private banking account" is found in 31 CFR § 1010.605(m). The definition of "non-U.S. person" is found in 31 CFR § 1010.605(h).

81. *See* 31 CFR § 1010.620(c).

82. *See* 31 CFR §§ 1010.210, 1020.210, 1021.210, 1022.210, 1023.210, 1024.210, 1025.210, 1026.210, 1027.210, 1028.210, 1029.210, 1030.210.

83. *See* 31 CFR § 1010.610.

84. *See* FinCEN, Anti-Money Laundering Program Requirements for Money Services Businesses with Respect to Foreign Agents or Foreign Counterparties, Interpretive Release 2004-1, 69 Fed. Reg. 74,439 (Dec. 14, 2004). *See also* FinCEN, "Guidance on Existing AML Program Rule Compliance Obligations for MSB Principals with Respect to Agent Monitoring" (Mar. 11, 2016).

85. *See* 31 CFR § 1010.540; FinCEN, "Section 314(b) Fact Sheet" (Dec. 2020).

86. *See* Department of State, "Foreign Terrorist Organizations" (accessed May 5, 2025).

87. *See* E.O. 13224, 66 Fed. Reg. 49, 79 (Sept. 23, 2001).