FinCEN ADVISORY

FIN-2019-A007 November 12, 2019

Advisory on the Financial Action Task Force-Identified Jurisdictions with Anti-Money Laundering and Combating the Financing of Terrorism Deficiencies and Relevant Actions by the United States Government

On October 18, 2019, the Financial Action Task Force (FATF) updated its list of jurisdictions with strategic anti-money laundering and combating the financing of terrorism (AML/CFT) deficiencies. The changes may affect U.S. financial institutions' obligations and risk-based approaches with respect to relevant jurisdictions.

The Financial Crimes Enforcement Network (FinCEN) is issuing this advisory to inform financial institutions of updates to the FATF list of jurisdictions with strategic AML/CFT deficiencies. Financial institutions should be aware of these changes, which may affect their obligations and risk-based approaches with respect to these jurisdictions. The advisory also reminds financial institutions of the status of, and obligations involving, these jurisdictions, in particular the Democratic People's Republic of Korea (DPRK) and Iran.

As part of the 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.[1] These jurisdictions are named in two documents: (1) the "FATF Public Statement," which identifies jurisdictions that are subject to the FATF's call for countermeasures and/or enhanced due diligence (EDD) because of their strategic AML/CFT deficiencies; and (2) "Improving Global AML/CFT Compliance: On-going Process," which identifies jurisdictions that the FATF has determined to have strategic AML/CFT deficiencies.[2] On October 18, 2019, the FATF updated both documents. Financial institutions should consider these changes when reviewing their obligations and risk-based policies, procedures, and practices with respect to the jurisdictions noted below.[3]

1. The FATF (www.fatf-gafi.org) is a 39-member intergovernmental body that establishes international standards to combat money laundering and counter the financing of terrorism and proliferation of weapons of mass destruction. The United States is a member of the FATF.
2. The FATF's public identification of jurisdictions with strategic AML/CFT deficiencies is in response to the G20 leaders' call for the FATF to reinvigorate its process for assessing jurisdictions' compliance with international AML/CFT standards. The G20 leaders have consistently called for the FATF to issue regular updates on jurisdictions with strategic deficiencies. Specifically, within the FATF, the International Cooperation Review Group (ICRG) monitors and identifies jurisdictions with AML/CFT deficiencies. For more information on the ICRG procedures, please visit the FATF's website.
3. *See* 31 U.S.C. §§ 5318(h) and (i).

FATF Public Statement:

- DPRK and Iran

FATF Improving Global AML/CFT Compliance: On-going Process:

- Remaining on list: The Bahamas, Botswana, Cambodia, Ghana, Pakistan, Panama, Syria, Trinidad and Tobago, and Yemen
- Added to list: Iceland, Mongolia, and Zimbabwe
- Removed from the list: Ethiopia, Sri Lanka, and Tunisia

Jurisdictions that are Subject to the FATF's Call for Countermeasures and/or EDD due to their Strategic AML/CFT Deficiencies

The FATF has stated that the following jurisdictions have strategic deficiencies in their AML/CFT regimes and has called upon its members and urged all jurisdictions to (1) impose countermeasures or (2) apply select countermeasures specifically to: (i) increase supervisory examination for branches and subsidiaries of financial institutions based in Iran; (ii) enhance relevant reporting mechanisms or systematic reporting of financial transactions; and (iii) increase external audit requirements for financial groups with respect to any of their branches and subsidiaries located in Iran.

Countermeasures

DPRK

Select Countermeasures

Iran

DPRK

FATF Actions:
Public Statement on the DPRK

The FATF issued the following public statement concerning the DPRK:

"The FATF remains concerned by the DPRK's failure to address the significant deficiencies in its anti-money laundering and combating the financing of terrorism (AML/CFT) regime and the serious threats they pose to the integrity of the international financial system. The FATF urges the DPRK to immediately and meaningfully address its AML/CFT deficiencies. Further, the FATF has serious concerns with the threat posed by the DPRK's illicit activities related to the proliferation of weapons of mass destruction (WMDs) and its financing.

The FATF reaffirms its 25 February 2011 call on its members and urges all jurisdictions to advise their financial institutions to give special attention to business relationships and transactions with the DPRK, including DPRK companies, financial institutions, and those acting on their behalf. In addition to enhanced scrutiny, the FATF further calls on its members and urges all jurisdictions to apply effective counter-measures, and targeted financial sanctions in accordance with applicable United Nations Security Council Resolutions, to protect their financial sectors from money laundering, financing of terrorism and WMD proliferation financing (ML/FT/PF) risks emanating from the DPRK. Jurisdictions should take necessary measures to close existing branches, subsidiaries and representative offices of DPRK banks within their territories and terminate correspondent relationships with DPRK banks, where required by relevant UNSC resolutions."[4]

United Nations: Related Sanctions on the DPRK

The United Nations (UN) has adopted several resolutions implementing economic and financial sanctions, as well as other prohibitions and restrictions with respect to the DPRK. Member States are bound by the provisions of these United Nations Security Council Resolutions (UNSCRs), and certain provisions of these resolutions are especially relevant to financial institutions.[5] Most recently, UNSCR 2397 (2017) called upon Member States to redouble efforts to implement measures in all DPRK-related UNSCRs. For example, UNSCR 2270 (2016) requires Member States to prohibit financial institutions from establishing new joint ventures and from taking an ownership interest in or establishing or maintaining correspondent relationships with DPRK banks without advance approval from the UN. Financial institutions should also be aware of UNSCR 2321 (2016), which states that Member States must expel individuals acting on behalf of, or at the direction of, a bank or financial institution of the DPRK. UNSCR 2321 also expresses concern that individuals from the DPRK are sent abroad to earn hard currency to fund the DPRK's nuclear and ballistic missile programs, and it reiterates the concern that the DPRK may use bulk cash to evade UN measures. UNSCR 2321 also instructs Member States to close existing representative offices, subsidiaries, or banking accounts in the DPRK within 90 days of the adoption of the resolution (unless individually exempted by the 1718 Committee), and states that Member States shall prohibit public and private financial support within their territories or by persons or entities subject to their jurisdiction for trade with the DPRK.

4. Financial Action Task Force Public Statement – October 2019, (October 18, 2019).

5. Relevant UNSCRs include 2397 (December 2017), 2375 (September 2017), 2371 (August 2017), 2356 (June 2017), 2321 (November 2016), 2270 (March 2016), 2094 (March 2013), 2087 (January 2013), 1874 (June 2009), and 1718 (October 2006). *See* the United Nations Security Council Resolutions web page for more information.

United States: Related Sanctions, Prohibitions, and Other Measures Concerning the DPRK

In addition to UN sanctions, the U.S. Government maintains a robust sanctions program on North Korea.[6] Specifically, the Department of the Treasury's (Treasury) Office of Foreign Assets Control (OFAC) issued the North Korea Sanctions Regulations, 31 C.F.R. Part 510 (NKSR), to implement DPRK-related Executive Orders (E.O.s) 13466, 13551, 13570, 13687, 13722, and 13810; as well as the North Korea Sanctions and Policy Enhancement Act of 2016 (NKSPEA), as amended by Title III of the Countering America's Adversaries Through Sanctions Act of 2017 (CAATSA).[7] The NKSR generally prohibits most direct or indirect commercial, financial, or trade transactions subject to U.S. jurisdiction that involve North Korea or the property or interests in property of any individual or entity designated pursuant to the North Korea sanctions program, unless authorized by OFAC or exempted by statute.[8] Separately, using authorities granted under the Weapons of Mass Destruction (WMD) Proliferators Sanctions Regulations[9] and E.O. 13382, OFAC administers sanctions on individuals and entities responsible for the proliferation of WMD, as well as their supporters, some of whom are North Korean or tied to North Korea and North Korean-related activity.[10] Together these sanctions are a direct response to the DPRK's ongoing development of WMD and its means of delivery; launching of intercontinental ballistic missiles (ICBMs); nuclear tests; human rights abuses and censorship; destructive, coercive cyber-related actions; involvement in money laundering, the counterfeiting of goods and currency, bulk cash smuggling, and narcotics trafficking; and continued violations of UNSCRs.[11]

Financial institutions should be particularly aware of the extensive nature of the sanctions associated with E.O. 13810.[12] The E.O. provides Treasury additional tools to disrupt a broad range of DPRK-related activity, to include North Korea's ability to fund its WMD and ballistic missile programs. Specifically, E.O. 13810: (1) establishes several new designation criteria; (2) prohibits vessels and aircraft that have called or landed at a port or place in North Korea in the previous

6. The DPRK is also referred to as North Korea.

7. *See* Treasury Resource Center, North Korea Sanctions, 22 U.S.C. § 9201 et seq., and Public Law 115-44.

8. Further information about these sanctions is available at the Treasury Resource Center's North Korea Sanctions web page and the OFAC Recent Actions web page. OFAC recently designated North Korean state-sponsored malicious cyber groups, a shipping network involved in ship-to-ship transfers with North Korean vessels, and a North Korean, Vietnam-based representative of a WMD entity on September 13, 2019; August 30, 2019; and July 29, 2019, respectively. Previously, OFAC took sanctions actions related to the DPRK on September 30, 2019; June 19, 2019; March 21, 2019; December 10, 2018; November 19, 2018; October 25, 2018; October 4, 2018; September 13, 2018; September 6, 2018; August 21, 2018; August 15, 2018; August 3, 2018; February 23, 2018; January 24, 2018; November 21, 2017; October 26, 2017; September 26, 2017; August 22, 2017; December 26, 2017; June 29, 2017; June 1,2017; March 31, 2017; December 2, 2016; and September 26, 2016.

9. *See* 31 CFR Part 544.

10. *See* Executive Order 13382 (June 28, 2005).

11. *See* Executive Orders 13810 (September 20, 2017), 13687 (January 2, 2015), and 13551 (August 30, 2010).

12. *See* Treasury Resource Center, Issuance of North Korea-related Executive Order; New and Updated FAQs; New and Updated General Licenses, (September 21, 2017) and Treasury Press Release, "Remarks by Secretary Mnuchin on President Trump's Executive Order on North Korea," (September 21, 2017).

180 days, and vessels that engaged in a ship-to-ship transfer with such a vessel in the previous 180 days from entering the United States; (3) provides authority to block any funds to, from, or through foreign bank accounts with links to North Korea that come within U.S. jurisdiction; and (4) provides authority to impose secondary sanctions on a foreign financial institution (FFI) that knowingly conducts or facilitates on or after September 21, 2017, (i) any significant transaction on behalf of any person blocked under the DPRK-related Executive Orders or persons blocked under E.O. 13382 for North Korea-related activities or (ii) any significant transaction in connection with trade with North Korea. These secondary sanctions applicable to FFIs are either restrictions on correspondent or payable-through accounts in the United States or full-blocking sanctions.[13]

Since the issuance of E.O. 13810, OFAC has designated entities and individuals involved in North Korea's illicit shipping and transportation activities, trading companies, and financial and banking representatives and identified multiple vessels as blocked property.[14] For example, on August 30, 2019, OFAC designated two individuals and three entities, and further identified one vessel as blocked property, pursuant to E.O. 13810 for having engaged in at least one significant importation from or exportation to North Korea of any goods, services, or technology. This action highlighted North Korea's continued use of illicit ship-to-ship transfers to circumvent UN sanctions that restrict the import of petroleum products, as well as the U.S. Government's commitment to implement existing UNSCRs.[15]

OFAC has also designated North Korea state-sponsored malicious cyber groups, such as the Lazarus Group and two of its subgroups. On September 13, 2019, OFAC designated these groups, pursuant to E.O. 13722, for targeting institutions such as government, military, financial, manufacturing, publishing, media, entertainment, and international shipping companies, as well as critical infrastructure, using tactics such as cyber espionage, data theft, monetary heists, and destructive malware operations. Among other attacks and activities, the Lazarus Group was involved in the destructive WannaCry 2.0 ransomware attack, which the United States, Australia, Canada, New Zealand, and the United Kingdom publicly attributed to North Korea in December 2017.[16]

Treasury also continues to use its sanctions authorities to target those involved in North Korea's WMD and missile programs. This commitment is evident by OFAC's July 29, 2019, designation of a North Korean individual operating from Vietnam, Kim Su Il, for his ties to the Workers' Party of Korea (WPK), pursuant to E.O. 13687. Kim Su Il is also an employee of the Munitions Industry Department; a WPK subordinate that is UN- and U.S.-designated for its involvement in key aspects of North Korea's missile program, which is subject to a range of U.S. sanctions restrictions.[17]

13. *See* OFAC's Frequently Asked Questions (FAQs).
14. *See* Executive Order 13810 (September 20, 2017).
15. Treasury Press Release, "Treasury Designates Shipping Network Engaged in Ship-to-Ship Transfers with North Korean Vessels," (August 30, 2019).
16. Treasury Press Release, "Treasury Sanctions North Korean State-Sponsored Malicious Cyber Groups," (September 13, 2019).
17. Treasury Press Release, "Treasury Designates a Vietnam-Based Representative of a WMD Entity," (July 29, 2019).

Other Treasury actions underscore the serious risks that any financial activity involving the DPRK may facilitate WMD and ballistic missile activities. In November 2016, pursuant to Section 311 of the USA PATRIOT Act, FinCEN issued a final rule prohibiting U.S. financial institutions from opening or maintaining correspondent accounts for, or on behalf of, North Korean banking institutions and requiring covered financial institutions to apply special due diligence to their foreign correspondent accounts that is reasonably designed to guard against the use of such accounts to process transactions involving North Korean financial institutions.[18] FinCEN noted that the North Korean government continues to use state-controlled financial institutions and front companies to conduct illicit international financial transactions, some of which support the proliferation of WMDs and the development of ballistic missiles.[19]

In November 2017, FinCEN also prohibited U.S. financial institutions from opening or maintaining correspondent accounts for, or on behalf of, Bank of Dandong, and required those covered financial institutions to apply special due diligence to their foreign correspondent accounts that is reasonably designed to guard against their use to process transactions involving Bank of Dandong.[20] In promulgating the regulation, FinCEN found that the Chinese bank has acted as a conduit for illicit North Korean financial activity to access the U.S. and international financial systems, including the facilitation of millions of dollars of transactions for companies involved in WMD and ballistic missile programs. Further, FinCEN found that Bank of Dandong has also facilitated financial activity for North Korean entities designated by the United States and listed by the UN for proliferation of WMD, as well as for front companies acting on their behalf.[21]

On November 2, 2017, FinCEN also issued an advisory to further alert financial institutions to schemes commonly used by North Korea to evade U.S. and UN sanctions, launder funds, and finance the North Korean regime's weapons programs.[22]

18. 31 C.F.R. § 1010.659.

19. 81 Fed. Reg. 78,715 (Nov. 9, 2016).

20. 31 C.F.R. § 1010.660.

21. 82 Fed. Reg. 51,758, 51,759 (Nov. 8, 2017).

22. *See* FinCEN Advisory, FIN-2017-A008, "Advisory on North Korea's Use of the International Financial System" (November 2017). In addition, FinCEN has issued three other advisories relating to the DPRK: FIN-2013-A005, "Update on the Continuing Illicit Finance Threat Emanating from North Korea" (July 2013); FIN-2009-A002, "North Korea Government Agencies' and Front Companies' Involvement in Illicit Financial Activities" (June 2009); and FinCEN Advisory – Issue 40, "Guidance to Financial Institutions on the Provisions of Banking Services to North Korean Government Agencies and Associated Front Companies Engaged in Illicit Activities" (December 2005).

Iran

FATF Actions:
Public Statement on Iran

The FATF issued a public statement concerning Iran, which is provided below in its entirety.

"In June 2016, the FATF welcomed Iran's high-level political commitment to address its strategic AML/CFT deficiencies, and its decision to seek technical assistance in the implementation of the Action Plan.

In November 2017, Iran established a cash declaration regime. In August 2018, Iran has enacted amendments to its Counter-Terrorist Financing Act and in January 2019, Iran has also enacted amendments to its Anti-Money Laundering Act. The FATF recognises the progress of these legislative efforts. The bills to ratify the Palermo and Terrorist Financing Conventions have passed Parliament, but are not yet in force. As with any country, the FATF can only consider fully enacted legislation. Once the remaining legislation comes fully into force, the FATF will review this alongside the enacted legislation to determine whether the measures contained therein address Iran's Action Plan, in line with the FATF standards.

Iran's action plan expired in January 2018. In October 2019, the FATF noted that there are still items not completed and Iran should fully address: (1) adequately criminalizing terrorist financing, including by removing the exemption for designated groups 'attempting to end foreign occupation, colonialism and racism'; (2) identifying and freezing terrorist assets in line with the relevant United Nations Security Council resolutions; (3) ensuring an adequate and enforceable customer due diligence regime; (4) clarifying that the submission of [Suspicious Transaction Reports] STRs for attempted [Terrorist Financing] TF-related transactions are covered under Iran's legal framework; (5) demonstrating how authorities are identifying and sanctioning unlicensed money/value transfer service providers; (6) ratifying and implementing the Palermo and TF Conventions and clarifying the capability to provide mutual legal assistance; and (7) ensuring that financial institutions verify that wire transfers contain complete originator and beneficiary information.

The FATF decided in June 2019 to call upon its members and urge all jurisdictions to require increased supervisory examination for branches and subsidiaries of financial institutions based in Iran. In line with the June 2019 Public Statement, the FATF decided this week to call upon its members and urge all jurisdictions to introduce enhanced relevant reporting mechanisms or systematic reporting of financial transactions; and require increased external audit requirements for financial groups with respect to any of their branches and subsidiaries located in Iran.

If before February 2020, Iran does not enact the Palermo and Terrorist Financing Conventions in line with the FATF Standards, then the FATF will fully lift the suspension of counter-measures and call on its members and urge all jurisdictions to apply effective counter-measures, in line with Recommendation 19.

While acknowledging that Iran has recently adopted the AML-CFT bylaw, which the FATF has not yet reviewed, the FATF expresses its disappointment that the Action Plan remains outstanding. The FATF expects Iran to proceed swiftly in the reform path to ensure that it addresses all of the remaining items by completing and implementing the necessary AML/CFT reforms.

Iran will remain on the FATF Public Statement until the full Action Plan has been completed. Until Iran implements the measures required to address the deficiencies identified with respect to countering terrorism-financing in the Action Plan, the FATF will remain concerned with the terrorist financing risk emanating from Iran and the threat this poses to the international financial system. The FATF, therefore, calls on its members and urges all jurisdictions to continue to advise their financial institutions to apply enhanced due diligence with respect to business relationships and transactions with natural and legal persons from Iran, consistent with FATF Recommendation 19, including: (1) obtaining information on the reasons for intended transactions; and (2) conducting enhanced monitoring of business relationships, by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination."[23]

As noted by the FATF in its October 2019 and June 2019 Public Statements, jurisdictions should: (i) undertake increased supervision of branches and subsidiaries of financial institutions based in Iran; (ii) enhance relevant reporting mechanisms or systematic reporting of financial transactions; and (iii) increase external audit requirements for financial groups with respect to any of their branches and subsidiaries located in Iran. Whereas this does not affect current regulatory obligations for U.S. financial institutions, all U.S. persons are reminded that they are broadly prohibited from engaging in transactions or dealings with Iran, the Government of Iran, and Iranian financial institutions, including opening or maintaining correspondent accounts for Iranian financial institutions, unless authorized or exempt (see below for additional details).

United Nations: Related Sanctions on Iran

Financial institutions should be familiar with the requirements and prohibitions contained in UNSCR 2231 related to Iran.[24]

United States: Related Sanctions, Prohibitions, and other Measures Related to Iran

The United States has consistently underscored the risks of conducting business with entities associated with Iran. Iran continues to use deceptive tactics to fund its nefarious activities. Iran's tactics include forging documents, obfuscating data, using front and shell companies to exploit

23. Financial Action Task Force Public Statement – October 2019, (October 18, 2019).

24. UNSCR 2231 (July 2015) revises UN sanctions and other prohibitions, including financial prohibitions, concerning Iran. Financial institutions should be aware that the UN maintains a list of individuals and entities subject to targeted financial sanctions.

markets in numerous jurisdictions, and hiding illicit activities under official cover of government entities, among many others. On October 25, 2019, FinCEN found Iran to be a Jurisdiction of Primary Money Laundering Concern and issued a final rule, pursuant to Section 311 of the USA PATRIOT Act, imposing the fifth special measure available under Section 311. This rule prohibits U.S. financial institutions from opening or maintaining correspondent accounts for, or on behalf of, an Iranian financial institution, and the use of foreign financial institutions' correspondent accounts at covered United States financial institutions to process transactions involving Iranian financial institutions.[25] FinCEN based the final rule on its finding that international terrorists and entities involved in missile proliferation have conducted business in Iran, and that Iran is a jurisdiction characterized by a high level of institutional corruption and weak AML/CFT laws.[26] Previously, FinCEN issued an advisory outlining the deceptive practices the Iranian regime employs to access the international financial system with the intention of furthering its illicit and malign activities.[27]

The United States is engaged in a campaign of maximum financial pressure on the Iranian regime and intends to enforce aggressively the sanctions that are in effect. OFAC administers and enforces comprehensive trade sanctions against Iran as set forth in the Iranian Transactions and Sanctions Regulations (ITSR), 31 C.F.R. Part 560; Executive Orders, issued under the authority of the International Emergency Economic Powers Act, 50 U.S.C. §§ 1701-06; and other authorities. The ITSR generally prohibits most direct or indirect transactions with Iran by U.S. persons or within the United States, unless authorized by OFAC or exempted by statute.[28]

25. 31 C.F.R. § 1010.661.

26. Treasury Press Release, "Treasury and State Announce New Humanitarian Mechanism to Increase Transparency of Permissible Trade Supporting the Iranian People," (October 25, 2019). *See* 84 Fed. Reg. 59,302 (Nov. 4, 2019).

27. *See* FinCEN Advisory, FIN-2018-A006, "Advisory on the Iranian Regime's Illicit and Malign Activities and Attempts to Exploit the Financial System" (October 2018). FinCEN has issued numerous additional advisories related to Iran. *See* FIN-2019-A004, "Advisory on the Financial Action Task Force-Identified Jurisdictions with Anti-Money Laundering and Combatting the Financing of Terrorism Deficiencies and Relevant Actions by the United States Government" (July 2019); FIN-2019-A001, "Advisory on the Financial Action Task Force-Identified Jurisdictions with Anti-Money Laundering and Combatting the Financing of Terrorism Deficiencies" (March 2019); FIN-2018-A007, "Advisory on the FATF-Identified Jurisdictions with AML/CFT Deficiencies" (October 2018); FIN-2018-A004, "Advisory on the FATF-Identified Jurisdictions with AML/CFT Deficiencies" (September 2018); FIN-2018-A002, "Advisory on the FATF-Identified Jurisdictions with AML/CFT Deficiencies" (April 2018); FIN-2010-A008, "Update on the Continuing Illicit Finance Threat Emanating from Iran" (June 2010); FIN-2008-A002, "Guidance to Financial Institutions on the Continuing Money Laundering Threat Involving Illicit Iranian Activity" (March 2008); and FIN- 2007-A001, "Guidance to Financial Institutions on the Increasing Money Laundering Threat Involving Illicit Iranian Activity" (October 2007).

28. The ITSR also generally prohibits entities owned or controlled by a United States person and established or maintained outside the United States ("U.S.-owned or -controlled foreign entities") from knowingly engaging in any transaction directly or indirectly with the Government of Iran or any person subject to the jurisdiction of the Government of Iran that would be prohibited by the ITSR if the transaction were engaged in by a U.S. person or in the United States.

On May 8, 2018, the United States announced its decision to cease its participation in the Joint Comprehensive Plan of Action (JCPOA) and to begin reimposing the U.S. nuclear-related sanctions that were lifted to effectuate the JCPOA sanctions relief, following a wind-down period. Treasury implemented 90-day and 180-day wind-down periods for activities involving Iran that were consistent with the U.S. sanctions relief specified in the JCPOA.[29] On August 7, 2018, the United States reimposed certain sanctions that were lifted or waived under the JCPOA, and on November 5, 2018, the United States fully reimposed those sanctions. These sanctions target critical sectors of Iran's economy such as the energy, shipping, shipbuilding, and financial sectors.[30] Furthermore, E.O. 13871 of May 8, 2019, imposed sanctions, including correspondent and payable-through account sanctions on foreign financial institutions, related to, among other things, significant transactions for the purchase and sale of iron, steel, aluminum, and copper from Iran.[31] In addition, on June 24, 2019, the President signed E.O. 13876, imposing sanctions on the Supreme Leader of the Islamic Republic of Iran and the Supreme Leader's Office (SLO), and authorizing the Secretary of the Treasury, in consultation with the Secretary of State, to impose sanctions on certain affiliates of the Supreme Leader or the SLO.[32]

To combat Iran's malign activities, including its efforts to deceive the international business community, since February 2017, OFAC has issued 35 rounds of designations targeting over 1,000 persons, aircraft, and vessels in connection with a range of activities, including Iran's support for terrorism, its ballistic missile program, WMD proliferation, cyberattacks, transnational criminal activity, censorship, and human rights abuses.[33] Additionally, Treasury has continued to target Iran's proliferation networks and activities via its sanction authorities. On November 4, 2019, OFAC took action against Iran's Armed Forces General Staff and nine individuals who are appointees of, or have acted for or on behalf of, Ali Khamenei, the Iranian regime's unelected Supreme Leader whose office is responsible for advancing Iran's radical agenda. This action seeks to block funds from flowing to a shadow network of Ali Khamenei's

29. *See* Treasury Resource Center, May 2018 Guidance on Reimposing Certain Sanctions with Respect to Iran, (November 5, 2018).

30. *See* Executive Order 13846 (August 6, 2018).

31. *See* Executive Order 13871 (May 8, 2019).

32. *See* Executive Order 13876 (June 24, 2019).

33. On November 5, 2018, the United States reimposed the sanctions that were lifted or waived under the JCPOA, and OFAC posted to its website additional frequently asked questions (FAQs) that provide guidance on the sanctions that have been reimposed, amended several FAQs, and archived outdated FAQs. In addition to sanctions reimposed by E.O. 13846, OFAC issued Iran-related designations on November 4, 2019; September 25, 2019; September 20, 2019; September 4, 2019; July 31, 2019; July 22, 2019; June 24, 2019; June 12, 2019; June 7, 2019; March 26, 2019; March 22, 2019; February 13, 2019; January 24, 2019; October 16, 2018; September 14, 2018; July 9, 2018; May 30, 2018; May 24, 2018; May 22, 2018; May 17, 2018; May 15, 2018; May 10, 2018; March 23, 2018; January 12, 2018; January 4, 2018; November 20, 2017; and October 13, 2017. Furthermore, OFAC designations associated with Iran's ballistic missile program on August 28, 2019 and July 18; 2019, and previously issued sanctions related to Iran's ballistic missile program on July 28, 2017; July 18, 2017 (in conjunction with those issued by the U.S. Department of State and in coordination with the U.S. Department of Justice's release of information involving a related criminal enforcement action); September 14, 2017; May 17, 2017; April 13, 2017; and February 3, 2017. Consult OFAC's Iran Sanctions web page and the OFAC Recent Actions web page for more detailed information about the sanctions included in this footnote.

military and foreign affairs advisors who have for decades oppressed the Iranian people, exported terrorism, and advanced destabilizing policies around the world. The action targeted Ali Khamenei's appointees in the SLO, the Expediency Council, the Armed Forces General Staff, and the Judiciary. On August 28, 2019, OFAC targeted two Iranian regime-linked networks pursuant to E.O. 13382 for engaging in covert procurement activities benefitting multiple Iranian military organizations. One network, led by Hamed Dehghan, has used a Hong Kong-based front company to evade U.S. and international sanctions and facilitate tens of millions of dollars' worth of proliferation activities targeting U.S. technology and electronic components for persons related to the Islamic Revolutionary Guard Corps (IRGC) and the Iranian regime's missile program. The second network, led by Seyed Hossein Shariat, has procured various aluminum alloy products on behalf of components entities owned or controlled by Iran's Ministry of Defense and Armed Forces Logistics (MODAFL).[34] In July 2019, OFAC took action against a network of front companies and agents involved in the procurement of sensitive materials for sanctioned elements of Iran's nuclear program. The individuals and entities targeted are based in Iran, China, and Belgium and have acted as a procurement network for Iran's Centrifuge Technology Company (TESA), which plays a crucial role in Iran's uranium enrichment nuclear program through the production of centrifuges used in facilities belonging to the Atomic Energy Organization of Iran. Treasury sanctioned TESA on November 21, 2011, pursuant to E.O. 13382.[35]

In September 2019, OFAC continued to impose sanctions on IRGC-related targets and Iran's proxy network. For example, on September 20, 2019, and pursuant to its counterterrorism authority, E.O. 13224, as amended by E.O. 13886, OFAC took action against the Central Bank of Iran (CBI) and the National Development Fund of Iran (NDF), which is Iran's sovereign wealth fund and whose board of trustees include Iran's president, oil minister, and the governor of the CBI. CBI has provided billions of dollars to the IRGC, its IRGC-Qods Force (QF) and its terrorist proxy, Hizballah. Previously, in 2018, OFAC designated four CBI officials, Valiollah Seif, Ali Tarzali, Rasul Sajjad, and Hossein Yaghoobi, for facilitating financial transfers for the IRGC-QF. In the September 20, 2019, action, OFAC found that NDF has been a major source of foreign currency and funding for the IRGC-QF and Iran's MODAFL.[36]

Also in September 2019, OFAC took action against a large shipping network that is directed by and financially supports IRGC-QF and its terrorist proxy Hizballah. During the past year, the IRGC-QF has moved oil worth hundreds of millions of dollars or more through this network for the benefit of the brutal Assad regime, Hizballah, and other illicit actors. This complex network of intermediaries enables the IRGC-QF to obfuscate its involvement in selling Iranian oil. The IRGC-QF also relies heavily on Hizballah officials and front companies to broker associated contracts.[37]

34. Treasury Press Release, "Treasury Designates Supreme Leader of Iran's Inner Circle Responsible for Advancing Regime's Domestic and Foreign Oppression," (November 5, 2019) and Treasury Press Release, "Treasury Targets Procurement Networks Supporting Iran's Missile Proliferation Programs," (August 28, 2019).

35. Treasury Press Release, "Treasury Sanctions Global Iranian Nuclear Enrichment Network," (July 18, 2019).

36. Treasury Press Release, "Treasury Sanctions Iran's Central Bank and National Development Fund," (September 20, 2019).

37. Treasury Press Release, "Treasury Designates Vast Iranian Petroleum Shipping Network That Supports IRGC-QF and Terror Proxies," (September 4, 2019).

In conjunction with the September 4, 2019, action concerning the shipping network, OFAC issued a new advisory to the maritime community to warn of the risks involved with participating in Iran's illicit schemes such as the IRGC-QF's oil-for-terror shipping network. This advisory is in addition to the Maritime Petroleum Shipping Community advisory issued by OFAC on March 25, 2019, which warns of sanctions risks related to oil shipments to Syria, including those from Iran.[38]

Treasury has also issued an aviation advisory to inform the civil aviation industry, including parties providing services to the industry, of potential exposure to U.S. Government enforcement actions and economic sanctions for engaging in or supporting unauthorized transfers of aircraft or related goods, technology, or services to Iran or to designated Iranian airlines. The advisory also describes various deceptive practices used by the Iranian regime to evade sanctions and illicitly procure aircraft and aircraft parts ranging from the use of front companies and unrelated general trading companies to falsifying or fabricating documentation relating to end-use or OFAC licenses. Intermediaries should be on heightened alert to the practices highlighted in this advisory, and industry parties who engage in or support unauthorized transfers of certain aircraft or related goods, technology, or services to Iran, or who conduct business with designated Iranian airlines, risk OFAC enforcement or sanctions actions.[39]

The U.S. Department of State has designated several entities related to Iran and its malign activities. On July 22, 2019, the U.S. Department of State designated the Chinese firm Zhuhai Zhenrong Company Limited and its chief executive for knowingly purchasing or acquiring oil from Iran, contrary to U.S. sanctions. Zhuhai Zhenrong Company Limited knowingly engaged in a significant transaction for the purchase or acquisition of crude oil from Iran. The transaction in question took place after the expiration of China's Significant Reduction Exception (SRE) on May 2, 2019, and was not covered by that SRE. Additionally, the United States imposed several restrictions as well as a ban on entry into the United States on Youmin Li, a corporate officer and principal executive officer of Zhuhai Zhenrong Company Limited. This action was implemented by Treasury adding Zhuhai Zhenrong Company Limited and Youmin Li to its List of Specially Designated Nationals and Blocked Persons.[40]

On September 3, 2019, the U.S. Department of State designated the Iran Space Agency and two of its research institutes, the Iran Space Research Center and the Astronautics Research Institute, under E.O. 13382. Space launch vehicle (SLV) technologies, such as those developed by Iran's space program, are virtually identical and interchangeable with those used in ballistic missiles. Iran's civilian space launch vehicle program allows it to gain experience with various technologies

38. *See* Treasury Press Release, "Treasury Designates Vast Iranian Petroleum Shipping Network That Supports IRGC-QF and Terror Proxies," (September 4, 2019) and Treasury Resource Center, "OFAC Advisory to the Maritime Petroleum Shipping Community: Sanctions Risks Related to Shipping Petroleum and Petroleum Products from Iran," (September 4, 2019).

39. Treasury Press Release, "Treasury Advisory Highlights Iranian Airlines' Support of Destabilizing Activity," (July 23, 2019) and Treasury Resource Center, "Iran-Related Civil Aviation Industry Advisory," (July 23, 2019).

40. *See* U.S. Department of State, Press Statement, "The United States To Impose Sanctions on Chinese Firm Zhuhai Zhenrong Company Limited for Purchasing Oil From Iran," (July 22, 2019) and Treasury's Resource Center Iran-related Designations, (July 22, 2019).

necessary for development of an ICBM—including staging, ignition of upper-stage engines, and control of a multiple-stage missile throughout flight.[41] Previously, the U.S. Department of State, on April 15, 2019, designated the IRGC, including its IRGC-QF, as a Foreign Terrorist Organization under section 219 of the Immigration and Nationality Act.[42] This action followed OFAC's 2017 Treasury designation of the IRGC pursuant to E.O. 13224 for providing support to the IRGC-QF, which was itself designated in 2007 under this same authority for providing support to numerous terrorist groups, including Hizballah and Hamas.[43]

Review of Guidance on Section 312 Obligation Relating to the DPRK and Iran

Financial institutions must comply with the extensive U.S. restrictions and prohibitions against opening or maintaining any correspondent accounts, directly or indirectly, with foreign banks licensed by the DPRK or Iran.

In the case of the DPRK, existing U.S. sanctions and FinCEN regulations already prohibit any such correspondent account relationships, superseding the Section 312 obligations.

In the case of Iran, the Government of Iran and Iranian financial institutions remain persons whose property and interests in property are blocked under E.O. 13599 and section 560.211 of the ITSR. U.S. financial institutions and other U.S. persons continue to be broadly prohibited under the ITSR from engaging in transactions or dealings with Iran, the Government of Iran, and Iranian financial institutions, including opening or maintaining correspondent accounts for Iranian financial institutions. These sanctions impose obligations on U.S. persons that go beyond the obligations imposed under Section 312.

41. U.S. Department of State, Fact Sheet, "New Sanctions Designations on Iran's Space Program," (September 3, 2019).
42. *See* U.S. Department of State Office of the Spokesperson Fact Sheet, "Designation of the Islamic Revolutionary Guard Corps," (April 8, 2019).
43. *Id.*

Reminder of General 312 Obligations

As a general matter, FinCEN reminds U.S. financial institutions of their duty to apply EDD when maintaining correspondent accounts for foreign banks operating under a banking license issued by a country (1) designated as noncooperative with respect to international anti-money laundering principles or procedures, by an intergovernmental group or organization of which the United States is a member, and with which designation the U.S. representative to the group or organization concurs, or (2) that is the subject of special measures pursuant to Section 311 of the USA PATRIOT Act.[44]

The regulations implementing the Bank Secrecy Act, as amended by the USA PATRIOT Act, require covered financial institutions to ensure that their EDD programs include, at a minimum, steps to:

- Conduct enhanced scrutiny of such correspondent accounts to guard against money laundering and to identify and report any suspicious transactions in accordance with applicable law and regulation;
- Determine whether the foreign bank for which the correspondent account is established or maintained in turn maintains correspondent accounts for other foreign banks that use the foreign correspondent account established or maintained by the covered financial institution and, if so, take reasonable steps to obtain information relevant to assess and mitigate money laundering risks associated with the foreign bank's correspondent accounts for other foreign banks, including, as appropriate, the identity of those foreign banks; and
- Determine, for any such correspondent account established or maintained for a foreign bank whose shares are not publicly traded, the identity of each owner of the foreign bank and the nature and extent of each owner's ownership interest.[45]

Jurisdictions Identified by the FATF as Having Strategic AML/CFT Deficiencies

The FATF publicly identifies jurisdictions with strategic AML/CFT regime deficiencies for which the jurisdictions have developed an action plan with the FATF. Consequently, these jurisdictions are included in the following list of jurisdictions with strategic AML/CFT deficiencies, as described in the FATF's publication entitled "Improving Global AML/CFT Compliance: On-going Process."

- The Bahamas, Botswana, Cambodia, Ghana, Iceland, Mongolia, Pakistan, Panama, Syria, Trinidad and Tobago, Yemen, and Zimbabwe.

44. Referring to 31 U.S.C. § 5318(i), 31 CFR §§ 1010.610(b) and (c) (Enhanced Due Diligence obligations for correspondent accounts established, maintained, administered, or managed in the United States for certain foreign banks).

45. *Id.*

Summary of Changes

Jurisdictions Added to the List

- Iceland made a high-level political commitment to work with the FATF to strengthen the effectiveness of its AML/CFT regime. While Iceland made overall progress since its 2017 mutual evaluation report, a few deficiencies in the areas of accessing of beneficial ownership information, Financial Intelligence Unit (FIU) capacity, and implementation of targeted financial sanctions remain.
- Mongolia made a high-level political commitment to work with the FATF and the relevant FATF-Style Regional Body, the Asia Pacific Group (APG), to strengthen the effectiveness of its AML/CFT regime. While Mongolia has made progress since its 2017 mutual evaluation report, a few deficiencies related to supervision of the nonfinancial sector, money laundering investigations, currency declaration system, and cooperation on proliferation financing sanctions evasion remain.
- Zimbabwe made a high-level political commitment to work with the FATF and the relevant FATF-Style Regional Body, Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG), to strengthen the effectiveness of its AML/CFT regime. Zimbabwe is making progress since its 2016 mutual evaluation report, but some deficiencies remain concerning understanding of money laundering/terrorist financing risk, risk-based supervision for financial institutions and designated nonfinancial businesses and professions (DNFBPs), framework for beneficial ownership information, and gaps in the targeted financial sanctions regime.

Jurisdictions Removed from the List

- Ethiopia, Sri Lanka, and Tunisia made significant progress in improving their AML/CFT regimes. Ethiopia, Sri Lanka, and Tunisia have strengthened the effectiveness of their AML/CFT regimes, and addressed related technical deficiencies to meet the commitments in their action plans regarding the strategic deficiencies that the FATF identified. Ethiopia, Sri Lanka, and Tunisia are therefore no longer subject to the FATF's monitoring process under its ongoing global AML/CFT compliance process. Ethiopia, Sri Lanka, and Tunisia will continue to work with the FATF and their respective FATF-Style Regional Bodies to improve further their AML/CFT regime.

Review of Guidance Regarding Jurisdictions Having Strategic AML/CFT Deficiencies

U.S. financial institutions also should consider the risks associated with the AML/CFT deficiencies of the jurisdictions identified under this section (The Bahamas, Botswana, Cambodia, Ghana, Iceland, Mongolia, Pakistan, Panama, Syria, Trinidad and Tobago, Yemen,

and Zimbabwe).[46] With respect to these jurisdictions, U.S. covered financial institutions are reminded of their obligations to comply with the due diligence obligations for FFIs under 31 CFR § 1010.610(a) in addition to their general obligations under 31 U.S.C. § 5318(h) and its implementing regulations.[47] As required under 31 CFR § 1010.610(a), covered financial institutions should ensure that their due diligence programs, which address correspondent accounts maintained for FFIs, include appropriate, specific, risk-based, and, where necessary, enhanced policies, procedures, and controls that are reasonably designed to detect and report known or suspected money laundering activity conducted through or involving any correspondent account established, maintained, administered, or managed in the United States. Furthermore, money services businesses (MSBs) are reminded of their parallel requirements with respect to foreign agents or foreign counterparties, as described in FinCEN Interpretive Release 2004-1, which clarifies that an MSB's AML Program requires the MSB to establish adequate and appropriate policies, procedures, and controls commensurate with the risk of money laundering and the financing of terrorism posed by their relationship with foreign agents or foreign counterparties (69 FR 239, December 14, 2004). Additional information on these parallel requirements (covering both domestic and foreign agents and foreign counterparts) may be found in FinCEN's Guidance on Existing AML Program Rule Compliance Obligations for MSB Principals with Respect to Agent Monitoring.[48] Such reasonable steps should not, however, put into question a financial institution's ability to maintain or otherwise continue appropriate relationships with customers or other financial institutions, and should not be used as the basis to engage in wholesale or indiscriminate de-risking of any class of customers or financial institutions. FinCEN also reminds financial institutions of previous interagency guidance on providing services to foreign embassies, consulates, and missions.[49]

46. This advisory updates previous FATF-related guidance on identified jurisdictions with AML/CFT deficiencies. Additional FinCEN advisories on Syria include FIN-2013-A002 and FIN-2011-A010 as well as FIN-2011-A013, FinCEN's advisory on the Commercial Bank of Syria.

47. *See* generally 31 CFR § 1010.210: Anti-money laundering programs. Specific AML Program obligations are prescribed in 31 CFR § 1020.210 (Banks), 1021.210 (Casinos and Card Clubs), 1022.210 (Money Services Businesses), 1023.210 (Brokers or Dealers in Securities), 1024.210 (Mutual Funds), 1025.210 (Insurance Companies), 1026.210 (Futures Commission Merchants and Introducing Brokers in Commodities), 1027.210 (Dealers in Precious Metals, Precious Stones, or Jewels), 1028.210 (Operators of Credit Card Systems), 1029.210 (Loan or Finance Companies), and 1030.210 (Housing Government Sponsored Enterprises).

48. *See* FIN-2016-G001 (March 11, 2016).

49. *See* Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, Financial Crimes Enforcement Network, National Credit Union Administration, Office of the Comptroller of the Currency, and Office of Thrift Supervision, "Interagency Advisory: Guidance on Accepting Accounts from Foreign Embassies, Consulates, and Missions," (March 24, 2011); and Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, Financial Crimes Enforcement Network, National Credit Union Administration, Office of the Comptroller of the Currency, and Office of Thrift Supervision, "Interagency Advisory: Guidance on Accepting Accounts from Foreign Governments, Foreign Embassies, and Foreign Political Figures," (June 15, 2004).

AML Program Risk Assessment: For the jurisdictions that were removed from the FATF listing and monitoring process, financial institutions should take the FATF's decisions and the reasons behind the delisting into consideration when assessing risk, consistent with their obligations under 31 CFR §§ 1010.610(a) and 1010.210.

Suspicious Activity Reports (SARs): If a financial institution knows, suspects, or has reason to suspect that a transaction involves funds derived from illegal activity or that a customer has otherwise engaged in activities indicative of money laundering, terrorist financing, or other violation of federal law or regulation, the financial institution must file a SAR.

SAR Filing Instructions

When filing a SAR, financial institutions should provide all pertinent available information in the SAR form and narrative. **FinCEN requests financial institutions only use the updated mandatory SAR form (as of February 1, 2019) and reference this advisory in SAR field 2 (Filing Institution Note to FinCEN) by including the following key term: "October 2019 FATF FIN-2019-A007"** to indicate a connection between the suspicious activity being reported and the jurisdictions and activities highlighted in this advisory.

SAR reporting, in conjunction with effective implementation of due diligence requirements and OFAC obligations by financial institutions, has been crucial to identifying proliferation financing, other financial crimes associated with foreign and domestic political corruption, money laundering, and terrorist financing. SAR reporting is consistently beneficial and critical to FinCEN and U.S. law enforcement analytical and investigative efforts, OFAC designation efforts, and the overall security and stability of the U.S. financial system.

For Further Information

Questions or comments regarding the contents of this advisory should be addressed to the FinCEN Regulatory Support Section at frc@fincen.gov.

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). 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.

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