Department of the Treasury

2026 National Proliferation Financing Risk Assessment

March 2026

Department of the Treasury

2026 National Proliferation Financing Risk Assessment

CONTENTS

EXECUTIVE SUMMARY

In the current risk environment, the United States faces an elevated threat from illicit actors seeking to finance the proliferation or use of biological, chemical, nuclear, or radiological weapons or related materials. Global efforts to develop adequate legal frameworks and implement effective controls are insufficient to combat the proliferation financing (PF) of Weapons of Mass Destruction (WMD).[1] Moreover, the United States is exposed to a higher risk of WMD PF because of the size of the U.S. economy, international prominence of the U.S. dollar, and the industrial base that produces sensitive dual-use goods and items. Consequently, the United States implements a whole-of-government approach to mitigate WMD PF risk, including when threats target the U.S. financial system directly or indirectly.

Since the 2024 National PF Risk Assessment (NPFRA), many of the same state actors and those who support them represent the largest PF threat. Well-funded state and non-state actors are targeting the U.S. financial system and the United States to raise revenue, move funds, and illicitly procure dual-use items to support WMD programs. The main WMD PF threats include those associated with the Democratic People's Republic of Korea (DPRK) and Iran, and other state actors like Russia. Also, Chinese individuals and entities are playing a more widespread role in facilitating sanctions evasion activities.[2]

The DPRK continues to leverage various revenue generation activities and financial connectivity, often supported by China- and Russia-based actors, to finance its WMD program. Without an agile UN framework to keep up with the pace and sophistication of the DPRK's sanctions evasion activities, the United States leverages various disruption, enforcement, and monitoring tools to address the multifaceted threat. Despite recent setbacks to the Iranian nuclear program and network of proxies around the world, Iran continues to use complex evasion schemes to support its ballistic missiles, nuclear, and unmanned aerial vehicle (UAV) programs. In response, the United States maximum pressure campaign is designed to deny Iran all paths to a nuclear weapon, and to counter its malign activities around the world.[3]

While Russia's strengthening economic and military ties to the DPRK represent a major PF threat, the country is also circumventing export controls to use U.S.-origin dual-use items to bolster advanced weaponry for its war in Ukraine. The United States also remains concerned about the potential for other non-state actors to facilitate PF or otherwise pursue biological, chemical, nuclear, or radiological weapons. Because illicit fentanyl is designated as a WMD, the United States is redoubling efforts to disrupt drug cartels that threaten U.S. national security.

Vulnerabilities identified in the 2024 NPFRA persisted over the past two years. The most relevant national-level factors are economic, trade, regulatory, industrial, and technological, while sectoral-level vulnerabilities include financial institutions and industries that are not subject to the same anti-money laundering, countering the financing of terrorism, and countering proliferation financing (AML/CFT/CPF) controls globally. To stay ahead of highly adaptive illicit procurement networks and other PF-related actors, the United States implements the world's most comprehensive export controls and sanctions programs to restrict the movement of sensitive goods and sever access to the U.S. financial system.

Building on previous risk assessments, the 2026 NPFRA spotlights two broad typologies relevant to PF: the abuse of the global technology ecosystem (Typology 1), and the use of money laundering techniques to support proliferation activities (Typology 2). Under Typology 1, the DPRK remains focused on targeting the IT worker sector to generate

1 According to the Financial Action Task Force (FATF) report entitled *Complex PF and Sanctions Evasion Schemes*, less than 20% of jurisdictions demonstrated effective implementation of PF controls, and nearly half lacked an appropriate legal framework to meet technical compliance requirements in the fourth round of FATF mutual evaluations. For more information, see Complex-PF-Sanctions-Evasions-Schemes.pdf.coredownload.inline.pdf

2 Office of the Director of National Intelligence (DNI), "Annual Threat Assessment of the U.S. Intelligence Community," (March 2025) ATA-2025-Unclassified-Report.pdf

3 White House, "Fact Sheet: President Donald J. Trump Restores Maximum Pressure on Iran," (February 2025) Fact Sheet: President Donald J. Trump Restores Maximum Pressure on Iran – The White House

revenue. Also, state and non-state actors are using digital assets to obscure and move funds. Under Typology 2, a variety of threat actors are enlisting intermediaries and exploiting front/shell companies to evade sanctions and circumvent export controls.

This risk assessment aims to update the national understanding of WMD PF risk. The United States assesses that both state and non-state actors will accelerate efforts to probe for weaknesses in CPF regimes in the coming years. Given the potential for heightened PF activity, the United States will continue to employ a whole-of-government approach to address the evolving PF risk. Because of the rise of new technologies and uneven implementation of PF-Targeted Financial Sanctions (TFS) globally, it is also crucial that the public and private sectors collaborate to address vulnerabilities in CPF controls and ensure sound AML/CFT frameworks allow for a proactive approach to anticipate emerging risks.

INTRODUCTION

In 2018, the United States published the first standalone NPFRA in the world. The 2018 NPFRA found that the DPRK and Iran posed the most significant PF threats for the United States, where PF networks sought to exploit national and sectoral vulnerabilities. Examples of PF vulnerabilities susceptible to exploitation by PF networks include the size of the U.S. financial system, the centrality of the U.S. dollar in global trade, the nature of nested accounts in correspondent banking relationships and maritime sectors, and the role of U.S. manufacturers in the production of dual-use items.

In 2022, other state actors like Russia expanded their efforts to acquire U.S.-origin goods and services in violation of export control laws. Additionally, PF networks increasingly exploited the digital economy, including by engaging in the systematic mining and trading of digital assets and cyber-enabled theft. In particular, the DPRK's capacity and willingness to engage in increasingly sophisticated malicious cyber activity and the digital assets sector grew considerably. Also, the COVID-19 pandemic focused global attention on biological threats, whether naturally occurring, accidental, or deliberate. In 2024, Russia and the DPRK were identified as the highest-risk PF threat actors because of the scope and sophistication of their illicit procurement and revenue generation efforts. The varying levels of AML/CFT/CPF controls for the digital asset sector globally, as well as some compliance deficiencies within the United States, were cited as PF vulnerabilities.

The 2026 NPFRA updates the United States' three previous NPFRAs.[4,5] The United States defines WMDs as biological, chemical, nuclear, radiological, or other destructive devices that can cause mass casualties. The United States defines WMD PF risk in terms of individuals, entities, or states that raise, move, or use funds to acquire goods, technology, or expertise involved in the illicit proliferation ecosystem.[6] Through close interagency coordination and international cooperation, the United States develops and implements a strategic policy that detects and maps PF networks. The United States continues to take strong actions to disrupt PF threat actors, utilizing investigations, prosecutions, and other tools, such as the Department of the Treasury's TFS authorities—the strongest TFS regime in the world.[7]

The U.S. CPF regime maintains its focus on major PF threats, especially those emanating from the DPRK and Iran. However, recent developments within the UN-TFS framework send mixed messages on the global commitment against WMD PF by DPRK and Iran. As it relates to the DPRK, the UN Security Council resolution (UNSCR) 1718 Committee's Panel of Experts (POE), which was established in 2009 to analyze non-compliance with the UN 1718 sanctions regime, was disbanded shortly after Russia's March 2024 veto of the POE's mandate renewal. Failure to

4 Department of the Treasury (Treasury), "2018 National Proliferation Financing Risk Assessment," (December 2018), https://home.treasury.gov/system/files/136/2018npfra_12_18.pdf; Treasury, "2022 National Proliferation Financing Risk Assessment," (March 2022), home.treasury.gov/system/files/136/2022-National-Proliferation-Financing-Risk-Assessment.pdf; and Treasury, "2024 National Proliferation Financing Risk Assessment," (February 2024), https://home.treasury.gov/system/files/136/2024-National-Proliferation-Financing-Risk-Assessment.pdf

5 In line with the FATF's PF risk assessment guidance, the United States finds that conducting an assessment to identify and better understand PF risk on a regular basis is essential to strengthen our ability to prevent individuals and entities from raising, storing, moving, and using funds, financial assets, or other economic resources in connection with the proliferation of weapons of mass destruction. For more information, see FATF, "Guidance on Proliferation Financing Risk Assessment and Mitigation," (June 2021), https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Guidance-Proliferation-Financing-Risk-Assessment-Mitigation.pdf.coredownload.inline.pdf

6 U.S. law defines and criminalizes WMD through multiple, intersecting authorities. Under a criminal statute prohibiting the use of WMDs, 18 U.S.C. § 2332a, WMDs include (1) destructive devices (as defined in 18 U.S.C. § 921), including explosive or incendiary devices; (2) biological agents or toxins; (3) radiation-emitting or radioactive weapons; and (4) chemical weapons. Section 2332a criminalizes the use, attempted use, or threat to use such weapons against persons or property within the United States. Beyond criminal law, the U.S. employs broader definitions of WMD within its national security, export control, and sanctions regimes. Authorities such as the International Emergency Economic Powers Act (IEEPA), the Export Control Reform Act, and the Arms Export Control Act enable the identification and disruption of prohibited WMD-related procurement, logistics, and financing. These are implemented in part through E.O. 13382, which targets proliferators and their financial facilitators. Together, these frameworks support U.S. implementation of CPF obligations by defining WMD, criminalizing their use, and enabling targeted financial measures to disrupt proliferation networks.

7 Consistent with FATF, the term *targeted financial sanctions* means both asset freezing and prohibitions to prevent funds or other assets from being made available, directly or indirectly, for the benefit of designated persons and entities. See p.138 in the FATF Recommendations, https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html.

extend the POE's mandate has created a gap in the UN's ability to track sanctions compliance and identify violations of UN PF-related sanctions, which weakens the global non-proliferation architecture.[8] The United States is playing a leading role in multilateral efforts outside of the UN to address the monitoring gap arising from the disbandment of the POE.[9]

In contrast, in late September 2025, all previous UN sanctions and measures on Iran as of January 2016 were reimposed due to Iran's failure to adhere to its Joint Comprehensive Plan of Action (JCPOA) commitments.[10,11] Member states are now required to implement UN sanctions under their domestic sanctions regimes to comply with their UN obligations, which include asset freezes on individuals and entities involved in Iranian nuclear and missile activities. In addition, member states are also called upon to exercise vigilance over Iranian banks in their jurisdictions and to prohibit the opening of new Iranian bank offices. Further, in October 2025, the Financial Action Task Force (FATF) reiterated its call on its members and urged all jurisdictions to apply effective countermeasures against Iran.[12]

Finally, the United States removed comprehensive U.S. sanctions on Syria in 2025 after the Bashar al-Assad regime collapsed in December 2024. However, sanctions remain for individuals and entities linked to the proliferation and use of WMD. Despite commitments made by the new Syrian government to cooperate with the Organisation for the Prohibition of Chemical Weapons (OPCW), PF risks remain in Syria, especially regarding the potential for malign state and non-state actors seeking to acquire any remnants of the Assad regime's past chemical weapons activities that remain in the country.[13,14]

8 UN, "Security Council Fails to Extend Mandate for Expert Panel Assisting Sanctions Committee on DPRK," (March 2024), https://press.un.org/en/2024/sc15648.doc.htm; The FATF Plenary Statement noted in June 2024, "the ability to obtain reliable and credible information to support the assessment of PF risks related to the DPRK is hampered by the recent termination of the 1718 Committee Panel of Experts mandate." See https://www.fatf-gafi.org/en/publications/High-risk-and-other-monitored-jurisdictions/Call-for-action-june-2024.html

9 Department of State (State), "Joint Statement of the Multilateral Sanctions Monitoring Team (MSMT) on the First Report Covering DPRK-Russia Military Cooperation," (May 2025), https://www.state.gov/joint-statement-of-the-multilateral-sanctions-monitoring-team-msmt-on-the-first-report-covering-dprk-russia-military-cooperation; and FATF, "Complex Proliferation Financing and Sanctions Evasion Schemes," (June 2025), https://www.fatf-gafi.org/en/publications/Financingofproliferation/complex-proliferation-financing-sanction-evasion-schemes.html

10 In May 2025, the International Atomic Energy Agency (IAEA) expressed serious concern that Iran was breaching key commitments, including exceeding enrichment limits and removing monitoring equipment since 2018. In particular, the IAEA expressed serious concern with Iran's significant increase in the production and accumulation of highly enriched uranium, which means the country is the only non-nuclear-weapon state to produce such nuclear material. For more information, see IAEA, "Verification and monitoring in the Islamic Republic of Iran in light of United Nations Security Council resolution 2231 (2015), (May 2025), https://www.iaea.org/sites/default/files/25/06/gov2025-24.pdf

11 UNSCR 2231, which endorsed the JCPOA in July 2015, set out the process by which UN sanctions would be lifted, while establishing a mechanism to reimpose them in case of "significant non-performance" by any of its participants – China, France, Germany, Russia, the UK, the US, the EU, and Iran. Under paragraph 11, if one of the signatories notifies the Council of a significant breach, the Council president must, within 30 days, put a draft resolution to the vote for sanctions relief to continue. If the draft is not adopted, the previous UN sanctions are automatically reimposed, meaning that unless the Council explicitly votes to keep sanctions relief in place, previous UN sanctions are automatically restored. For more information, see UN, "UN Security Council rejects bid to continue Iran sanctions relief," (September 2025), https://news.un.org/en/story/2025/09/1165891?_gl=1*nt1dos*_ga*MTIwMjIxNzM4Ny4xNzE4NjMxODUx*_ga_TK9BQL5X7Z*czE3NTk5NDQxMzQkbzU4JGcxJHQxNzU5OTQ0NTI5JGoyNSRsMCRoMA.

12 FATF, "High-Risk Jurisdictions Subject to a Call for Action," (October 2025), https://www.fatf-gafi.org/en/publications/High-risk-and-other-monitored-jurisdictions/Call-for-action-october-2025.html.

13 The OPCW is the implementing body for the Chemical Weapons Convention, which entered into force on 29 April 1997. The OPCW, with its 193 member states, oversees the global endeavor to permanently and verifiably eliminate chemical weapons.

14 UN, "Syria Chemical Weapons Concerns Widen with New Evidence, United Nations Disarmament Chief Tells Security Council," (September 2025), https://press.un.org/en/2025/sc16167.doc.htm.

CURRENT SITUATION AND THREATS

This section examines the PF threat actors confronting the United States and outlines key geopolitical and security developments since the 2024 NPFRA. State-sponsored or state-affiliated actors remain the primary PF threat to the U.S. financial system. These actors utilize substantial technical knowledge to develop and implement covert procurement and funding operations to support advanced weapons and WMD programs. Their proliferation activities occur on a large scale, despite extensive international, supranational, and national (including U.S.) sanctions and export controls. Other actors, such as individuals and entities based in China, play a frequent role in facilitating sanctions evasion relevant to PF.

Main Actors Linked to PF Threats

DPRK

The DPRK continues to advance its capabilities to deliver a nuclear device through its testing of intercontinental ballistic missiles (ICBM), in violation of UN sanctions in place since 2006. For example, on October 31, 2024, the DPRK conducted an ICBM test, the first since December 2023.[15] This test is the 11th ICBM launch by the DPRK since announcing a new five-year military expansion plan in 2021.[16] Also, on January 6, 2025, the DPRK allegedly tested its latest hypersonic missile, which represents a potential threat to U.S. allies in Northeast Asia.[17] There are two main factors supporting the financing of the DPRK's WMD program: the diversity of the country's revenue generation around the world, and its increasing financial connectivity, which is facilitated by actors primarily based in China and Russia.[18]

Diversity of Revenue Generation Activities

The DPRK engages in a broad range of revenue generation activities to evade sanctions and finance its WMD program. The DPRK continues to deploy information technology (IT) workers around the world, including to U.S. companies, often using forged or stolen identity documents, to generate revenue from employment. These schemes often target the United States financial system both directly (for example, U.S. enablers are paid to host DPRK laptop farms and unwitting U.S. companies are defrauded by the IT workers) and indirectly (for example, facilitating the movement of funds through U.S. correspondent banks).[19] Consequently, the prevalence of DPRK IT worker schemes led to the creation of the Department of Justice (DOJ)'s *DPRK RevGen: Domestic Enabler Initiative*, which prioritizes targeting and disrupting the DPRK's illicit revenue generation schemes and its U.S.-based

15 Treasury, "Treasury Sanctions Key Facilitators Behind North Korea's Illicit Financial Activities and Military Support to Russia," (December 2024), https://home.treasury.gov/news/press-releases/jy2751.

16 FATF, "Complex Proliferation Financing and Sanctions Evasion Schemes," (June 2025), https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Complex-PF-Sanctions-Evasions-Schemes.pdf.coredownload.inline.pdf.

17 UN, "Security Council Delegates Trade Barbs over Democratic People's Republic of Korea's Hypersonic-Missile Launch, Military Ambitions," (January 2025), https://press.un.org/en/2025/sc15962.doc.htm.

18 See Footnote 16.

19 See, e.g., Department of Justice (DOJ), "Two North Korean Nationals and Three Facilitators Indicted for Multi-Year Fraudulent Remote Information Technology Worker Scheme that Generated Revenue for the Democratic People's Republic of Korea," (January 2025), https://www.justice.gov/opa/pr/two-north-korean-nationals-and-three-facilitators-indicted-multi-year-fraudulent-remote; DOJ, "Justice Department Announces Coordinated, Nationwide Actions to Combat North Korean Remote Information Technology Workers' Illicit Revenue Generation Schemes," (June 2025), https://www.justice.gov/opa/pr/justice-department-announces-coordinated-nationwide-actions-combat-north-korean-remote; DOJ, "Department Files Civil Forfeiture Complaint Against Over $7.74M Laundered on Behalf of the North Korean Government," (June 2025), https://www.justice.gov/opa/pr/department-files-civil-forfeiture-complaint-against-over-774m-laundered-behalf-north-korean; and DOJ, "Arizona Woman Sentenced in $17M IT Worker Fraud Scheme That Illegally Generated Revenue for North Korea," (July 2025), https://www.justice.gov/usao-dc/pr/arizona-woman-sentenced-17m-it-worker-fraud-scheme-illegally-generated-revenue-north.

enablers.[20] There are other examples of the DPRK carrying out employment-related schemes, such as sending construction workers to Russia, where they earn foreign currency and enable the DPRK to continue to evade sanctions.[21]

Consistent with the findings of the 2024 NPFRA, the DPRK continues to use advanced cyber schemes to fund its unlawful WMD and ballistic programs, including digital asset theft and identity fraud.[22] In recent years, the DPRK has been responsible for the largest heists in the digital asset ecosystem, successfully stealing billions of dollars' worth of digital assets from various global digital asset service providers (DASPs), including Bybit, DMM Bitcoin, WazirX, BingX, and Phemex.[23] In addition to stealing digital assets, the DPRK often uses digital assets to launder theft proceeds and revenue generated from other sources. In October 2025, FinCEN published a final rule under Section 311 of the USA PATRIOT Act that severed Huione Group from the U.S. financial system.[24] Huione Group acted as a critical node for laundering proceeds of cyber heists carried out by the DPRK. This Cambodia-based financial service conglomerate helped the DPRK launder at least $37 million worth of digital assets stemming from cyber heists.[25]

The DPRK's other common revenue generation activities include multiple types of fraud, including forgery, and trafficking of arms, drugs, wildlife, contraband, and other items, such as tobacco. North Korea-linked individuals and entities engage in these illicit activities and exploit legitimate businesses, particularly targeting countries or sectors with weak or inadequate AML/CFT/CPF controls.[26] To further enhance revenue generation opportunities, the DPRK also takes advantage of jurisdictional differences in the implementation of various sanctions regimes, including in commercial, financial, and trade centers across the world.

Increasing Financial Connectivity

Recently, North Korea expanded its connectivity with certain parts of the international financial system. For instance, the 2024 *DPRK-Russia Comprehensive Strategic Partnership Treaty* commits both countries to creating favorable conditions for economic cooperation in customs, finance, and banking, working together to establish direct ties between the two countries.[27]

Russia is supporting the DPRK's direct access to the international financial system, which enables transactions related to North Korea's WMD program. For instance, in September 2024, the Office of Foreign Assets Control (OFAC) designated a network of five entities and one individual—based in Russia and in the Russian-occupied Georgian region of South Ossetia—that used illicit financial schemes to enable the DPRK to access the international financial system in violation of TFS requirements under UNSCR 1718.[28] The entities and individual violated a ban on correspondent relationships with DPRK banks under UNSCR 2270 and further emphasized by the FATF. In a scheme orchestrated by the Central Bank of Russia, MRB Bank (MRB), based in Georgia's South Ossetia region, acted as a

20 DOJ, "Justice Department Announces Coordinated, Nationwide Actions to Combat North Korean Remote Information Technology Workers' Illicit Revenue Generation Schemes," (June 2025), https://www.justice.gov/opa/pr/justice-department-announces-coordinated-nationwide-actions-combat-north-korean-remote.

21 See Footnote 16.

22 For more information, see Treasury, "2024 National Proliferation Financing Risk Assessment," (February 2024), https://home.treasury.gov/system/files/136/2024-National-Proliferation-Financing-Risk-Assessment.pdf.

23 MSMT, "The DPRK's Violation and Evasion of UN Sanctions through Cyber and Information Technology Worker Activities," (October 2025), https://www.mofa.go.jp/files/100922718.pdf.

24 Federal Register, "Imposition of Special Measure Regarding Huione Group, as a Foreign Financial Institution of Primary Money Laundering Concern," (October 2025), https://www.federalregister.gov/documents/2025/10/16/2025-19571/imposition-of-special-measure-regarding-huione-group-as-a-foreign-financial-institution-of-primary.

25 Treasury, "U.S. and U.K. Take Largest Action Ever Targeting Cybercriminal Networks in Southeast Asia," (October 2025), https://home.treasury.gov/news/press-releases/sb0278.

26 See Footnote 16.

27 More specifically, the *DPRK-Russia Comprehensive Strategic Partnership Treaty* commits to strengthening cooperation by creating favorable conditions for economic cooperation in customs, finance, and banking; working together to create favorable conditions for establishing direct ties between the DPRK and Russia; and promoting mutual understanding of the economic and investment potential on a local level.

28 Treasury, "Treasury Targets Key Actors in Sanctions Evasion Scheme to Support Russia and North Korea," (September 2024), https://home.treasury.gov/news/press-releases/jy2590.

cut-out for a Russian bank, TSMR-Bank, OOO (TSMR-Bank), to establish a secret banking relationship with the UN-designated Foreign Trade Bank (FTB). A senior official at TSMR-Bank facilitated cash deposits from FTB through TSMR-Bank to MRB. The senior official at TSMR-Bank organized the opening of correspondent accounts for FTB and UN-designated Korea Kwangson Banking Corporation (KKBC) at MRB and coordinated with DPRK representatives to ensure the delivery of millions of dollars and rubles in banknotes to FTB and KKBC accounts at MRB. At least some of the DPRK accounts at MRB were used to pay for fuel exports from Russia to the DPRK.

Strengthening economic ties, particularly in reestablishing banking connections with DPRK financial institutions or entities linked to PF, introduces new vulnerabilities in the international financial system. Between 2016 and 2024, the number of countries known to host DPRK bankers shrank from 14 to four due to host-country sanctions enforcement and DPRK personnel withdrawals. Yet, from 2023 to mid-2024, DPRK bankers in China and Russia facilitated transactions valued at hundreds of millions of dollars to support the DPRK's trade and revenue generation. As of late 2025, North Korean bankers were only known to be located in China and Russia.[29,30] The prevalence of China-based individuals acting on behalf of the DPRK provides myriad opportunities for access to the international financial system (see the Chinese facilitator section below for more information on the relevant financial channels, including UnionPay debit and credit cards).[31]

In 2025, the DPRK further expanded its money laundering toolkit to remit government funds. Pyongyang tested newly identified methods to convert fiat into digital assets and acquire automated clearing house (ACH)-enabled bank accounts at U.S. and Western financial institutions. For instance, North Korean IT workers in Russia sought to obtain ACH-enabled bank accounts through a number of Western financial institutions, including U.S. institutions, using fraudulent U.S. identification documents. Access to an ACH account could streamline the ability to receive direct deposit payments from U.S. clients.

Iran

During the period covered by the 2026 NPFRA, Iran continued to evade U.S. sanctions to support its nuclear and ballistic missiles programs.[32] Additionally, Iran continues to develop unmanned aerial vehicles (UAVs), which Tehran has provided to Russia and affiliated groups in the Middle East.[33] The sophisticated evasion tactics employed by Iran's state- and non-state-affiliated actors target sectors and locations with strong economic and financial linkages to the U.S. financial system, most notably in prominent financial centers in the Middle East and Asia.

29 North Korean state-owned enterprises use covert representatives based abroad to obfuscate the true originator, beneficiary, and purpose of transactions, enabling millions of dollars of North Korean illicit activity to flow through U.S. correspondent accounts. To conduct these transactions, the DPRK typically orchestrates elaborate trade-based payment schemes, including the sale/export of natural resources, indirect payment for natural resources, and import/smuggling of goods. These types of trade-based schemes allow the North Korean government to evade sanctions by directing payments for natural resource sales to front and shell companies, which in turn are used to access the international financial system and acquire technology for use in its WMD and missile programs. The network of DPRK financial representatives is believed to be primarily located in China. For more information on this longstanding typology, see FinCEN, "Advisory on North Korea's Use of the International Financial System," (September 2017), https://www.fincen.gov/system/files/advisory/2017-09-22/DPRK%20Financing%20Advisory%20%28v16%29%2Blanguage2.pdf.

30 UNSCR 2397 requires Member States to repatriate all DPRK nationals earning income by December 2019. UNSCR 2321 requires host countries to take proactive steps, such as expelling DPRK banking representatives and prohibiting public and private financial support from within their territories or by persons or entities subject to their jurisdiction for trade with the DPRK.

31 For more information on the role of individuals linked to China acting on behalf of the DPRK, see Footnote 23.

32 On June 21, 2025, the United States carried out air- and sea-launched strikes on three nuclear facilities in Iran to destroy or severely degrade the country's nuclear program. For more information on initial U.S. assessments of the strikes, see Library of Congress, "U.S. Strikes on Nuclear Sites in Iran," (June 2025), https://www.congress.gov/crs-product/IN12571.

33 Iran has become a key military supplier to Russia, especially of UAVs, and in exchange, Moscow has offered Tehran military and technical support to advance Iranian weapons, intelligence, and cyber capabilities. For more details on the historic size and scale of Iran's UAV program and linkages to Russia, see, e.g., DOJ, "United States Issues Advisory to Industry on Unmanned Aerial Vehicle Activity Connected to Iran," (June 2023), https://www.justice.gov/archives/opa/pr/united-states-issues-advisory-industry-unmanned-aerial-vehicle-activity-connected-iran; and Footnote 2.

A common typology employed by Iran to finance its weapons programs is the use of foreign-based front and shell companies to conduct opaque movements of dual-use items and funds.[34] In October 2025, a FinCEN financial trend analysis report found that shell companies appear to play the largest role in Iranian shadow banking. Within the dataset analyzed for the report, alleged shell companies linked to Iran sent approximately $4.2 billion, 89% of which was from China-based non-resident accounts operated by Hong Kong-based entities. Furthermore, alleged shell companies received approximately $4.3 billion, 72% of which was received by United Arab Emirates (UAE)-based shell companies.[35]

Iran also systematically uses militarized proxies and transnational criminal organizations (TCOs) to circumvent economic sanctions, relying on well-connected overseas businesspeople for oil smuggling, procurement agents for certain sensitive purchases, and banks, gold traders, and foreign exchange houses as conduits for money laundering and sanctions evasion that supports its missiles, weapons, and WMD program development (see Non-State Actors section).

Russia

As referenced in previous NPFRAs, Russia has the world's largest and most diverse nuclear weapons stockpile and a significant deployment of delivery systems. In recent years, Russia has withdrawn from or purported to suspend its obligations under certain international arms control arrangements, including treaties related to nuclear weapons. Russia continues to engage in procurement activities in support of its chemical and biological weapons programs.[36]

Russia has used chemical munitions across the front lines in Ukraine. In 2024, the United States made public assessments that Russia had used the chemical weapon chloropicrin and riot control agents as a method of warfare in Ukraine against Ukrainian forces.[37]

The Russia-Ukraine War has led to expansion in other non-conventional capabilities for Russia. For example, Russia adapted and innovated its use of UAVs in Ukraine. To mitigate the effects of international sanctions, Russia imported UAVs and UAV technology from Iran, and artillery shells, munitions, and ballistic missiles from the DPRK. Russia's defense spending accounts for the greatest share of budgetary expenditure in more than two decades, and the importation of weaponry from the DPRK and Iran reduces the impact of sanctions.[38]

The DPRK has unlawfully transferred arms, including ballistic missiles, to Russia and deployed its soldiers to fight in the Russia-Ukraine War. As described in the May 2025 Multilateral Sanctions Monitoring Team's (MSMT) report, "the DPRK and Russia conducted unlawful transfers of arms and military equipment through actors and networks that evaded sanctions by using front companies," and the report identified "individuals and entities [that] have facilitated Russia-DPRK military shipments."[39] Further, Russia's central bank was instrumental in establishing a payment channel between the DPRK and the international financial system, orchestrating an illicit finance scheme

34 FinCEN, "FinCEN Advisory on the Iranian Regime's Illicit Oil Smuggling Activities, Shadow Banking Networks, and Weapons Procurement Efforts," (June 2025), https://www.fincen.gov/system/files/advisory/2025-06-06/FinCEN-Advisory-Illicit-Oil-Smuggling-508.pdf.

35 FinCEN, "Financial Trend Analysis: Iranian Shadow Banking," (October 2025) https://www.fincen.gov/system/files/2025-10/FTA-Iranian-Shadow-Banking.pdf.

36 Treasury, "U.S. Continues to Degrade Russia's Military-Industrial Base and Target Third-Country Support with Nearly 300 New Sanctions," (May 2024) https://home.treasury.gov/news/press-releases/jy2318#Annex4.

37 State, "Condition (10)(C) Annual Report on Compliance with the Chemical Weapons Convention (CWC)," (April 2024), https://2021-2025.state.gov/condition-10c-annual-report-on-compliance-with-the-chemical-weapons-convention-cwc/; State, "Imposing New Measures on Russia for its Full-Scale War and Use of Chemical Weapons Against Ukraine," (May 2024), https://2021-2025.state.gov/imposing-new-measures-on-russia-for-its-full-scale-war-and-use-of-chemical-weapons-against-ukraine-2/.

38 See DNI, *2025 Threat Assessment*, (n 2) 18.

39 The Multilateral Sanctions Monitoring Team (MSMT), a mechanism established to monitor and report violations of UN sanctions on North Korea, was launched in 2024 after Russia vetoed the renewal of the UN 1718 Committee POE mandate, which previously served this function. Also, see State, "Joint Statement of the MSMT on the First Report Covering DPRK-Russia Military Cooperation," (May 2025), https://www.state.gov/joint-statement-of-the-multilateral-sanctions-monitoring-team-msmt-on-the-first-report-covering-dprk-russia-military-cooperation.

for the DPRK to evade UN sanctions.[40] According to the FATF, Russia's efforts to re-establish banking connections with the DPRK "could introduce new vulnerabilities in the global financial system since several DPRK financial institutions and their overseas representatives are designated under UNSCR 1718."[41]

Russia routinely employs sophisticated export control circumvention and sanctions evasion schemes to procure dual-use items for advanced weaponry used in the Russia-Ukraine War. Russian-affiliated individuals have violated export control laws by supplying sensitive U.S.-sourced, dual-use technologies to entities in Russia involved in the development and manufacture of UAVs for the Russian war effort in Ukraine. In response, the Department of Commerce (Commerce)'s Bureau of Industry and Security (BIS) has taken swift and severe action to impose and enforce stringent export controls on Russia in recent years.[42] In particular, BIS has imposed controls on a range of items subject to the Export Administration Regulations (EAR) that did not previously require export licenses when destined for Russia. Because of the attention on procurement efforts, however, Russia-affiliated actors continue to deploy complex schemes to outmaneuver trade restrictions, including through layering business entities, shell and front companies, as well as transshipment involving second and third countries (see Typology 2). Also, certain Chinese individuals and entities are known to act as major suppliers of dual-use items to aid Russia's war effort in Ukraine.

Chinese Individuals and Entities Facilitating Sanctions Evasion

The Chinese financial system is targeted as a primary conduit for sanctions evasion by PF threat actors such as the DPRK, Iran, and Russia. China-based financial institutions are being exploited to move funds on behalf of the DPRK and those who support the regime. According to the FATF, DPRK-associated individuals are increasingly using illegally-obtained accounts in the name of Chinese nationals. Through these efforts, the DPRK is also exploiting digital assets to make payments and access Chinese renminbi to circumvent UN sanctions. There are indications that the DPRK is using illegally-obtained UnionPay debit cards to receive deposits of fiat currency derived from stolen digital assets, as well as coordinated transactions for a range of WMD-related entities.[43] UnionPay is a financial services corporation and card network, which has expanded its global presence in recent years through its subsidiary, UnionPay International, and it partners with more than 2,600 institutions worldwide, including in the United States.

It is suspected that DPRK bankers are fraudulently managing numerous illegally-obtained UnionPay debit cards issued by major China-based commercial banks in the names of hundreds of domestic account holders to conduct local currency payments.[44] In recent years, the DPRK was associated with multiple UnionPay accounts at the Agricultural Bank of China, China Construction Bank, and Industrial and Commercial Bank of China. According to the October 2025 MSMT report, a Shenyang, China-based DPRK official working on behalf of the UN-designated Tanchon Commercial Bank processed nearly $4 million in transactions using UnionPay cards associated with Chinese banks on behalf of DPRK nationals, including for a China-based IT worker from the OFAC-designated 313 General Bureau.[45] Moreover, UN-designated DPRK banks, such as FTB and KKBC, are known to obscure financial ties to the DPRK by establishing networks of front companies in the name of Chinese nationals who hold accounts at China-based banks, to move funds through the international financial system.

40 See Footnote 28.

41 See Footnote 16.

42 See, e.g., Commerce, Bureau of Industry and Security (Commerce BIS), "BIS Imposes $180,000 Mitigated Penalty Against Indium Corporation for 11 Exports of Electronics Manufacturing Components to Russia," (December 2024), bis.gov/press-release/bis-imposes-180000-mitigated-penalty-against-indium-corporation-11-exports-electronics-manufacturing; Commerce BIS, "BIS Imposes Penalty Against Integra Technologies, Inc. for Unlicensed Shipments of Common High Priority List Items to Russia," (December 2024), bis.gov/press-release/bis-imposes-penalty-against-integra-technologies-inc.-unlicensed-shipments-common-high-priority-list; Commerce BIS, "Commerce Targets Illicit Procurement Networks Supplying Russia's Military and Restricts Chemical Precursors Enabling Russia's Use of Chemical Weapons Against Ukraine," (October 2024), bis.gov/press-release/commerce-targets-illicit-procurement-networks-supplying-russias-military-restricts-chemical-precursors.

43 See Footnote 16.

44 See Footnote 16.

45 See Footnote 23; and Treasury, "GUIDANCE ON THE DEMOCRATIC PEOPLE'S REPUBLIC OF KOREA INFORMATION TECHNOLOGY WORKERS," (May 2022), https://ofac.treasury.gov/media/923126/download?inline.

The UN Yemen POE has reported on the transfer of dual-use items China-based individuals and entities to Houthi weapons programs, including in its October 2025 final report.[46] Also, the United States has identified multiple Chinese individuals and entities for their roles in exporting and smuggling U.S.-origin electronic components for UAVs to Iran. For example, in April 2025, OFAC designated a network of 12 entities and individuals engaged in the export of chemical precursors for controlled missile technology to Iran. This network used a China-based shipping company to transport the chemicals;[47] the U.S. Department of State designated the same company in 2019 for being a shipping agent for Iranian proliferation and procurement agents.[48] Also, in January 2024, the DOJ indicted four Chinese nationals who used an array of China-based front companies to funnel dual-use U.S.-origin items to the OFAC-designated Islamic Revolutionary Guard Corps (IRGC).[49]

Similarly, certain Chinese individuals and entities have provided Russia with support in its war in Ukraine. The United States has sanctioned numerous Chinese entities for supplying military-applicable goods to Russia for use in UAVs and other weapons systems. For instance, in January 2025, the United States designated more than 150 individuals and entities enabling Russia's war in Ukraine, including China-based actors that facilitated the supply of hundreds of millions of dollars' worth of dual-use items.[50]

Other State Actors

Pakistan

Since the 2024 NPFRA, the United States continues to monitor individuals and entities that may act on behalf of Pakistan related to illicit procurement for its long-range ballistic missile program, including specific U.S.-origin goods. In October 2024, the United States added 16 Pakistan-linked entities to the Department of Commerce Entity List for alleged export control violations.[51] Nine of the entities were added for acting as Pakistan-based front companies and procurement agents for the Advanced Engineering Research Organization, a Pakistan-based company added to the Entity List in 2014. Additionally, the United States imposed new controls on commodities exported to Pakistan to address diversion concerns.[52] The United States also designated a total of nine entities based in Belarus, China, and Pakistan throughout 2024 involved in supporting Pakistan's long-range missile development, pursuant to E.O. 13382, which targets proliferators of WMD and their means of delivery. These designations included Pakistan's National Development Complex, which is responsible for Pakistan's ballistic missile program, and has worked to acquire items to advance Pakistan's long-range ballistic missile program.[53]

---

46 UN, "Letter dated 15 October 2025 from the Panel of Experts on Yemen addressed to the President of the Security Council," (October 2025), https://docs.un.org/en/S/2025/650.

47 Treasury, "Treasury Targets Network Procuring Missile Propellant Ingredients for Iran," (April 2025), https://home.treasury.gov/news/press-releases/sb0116.

48 State, "Designation of the Islamic Republic of Iran Shipping Lines, E-Sail Shipping Company Ltd, and Mahan Air," (December 2019), https://2017-2021.state.gov/designation-of-the-islamic-republic-of-iran-shipping-lines-e-sail-shipping-company-ltd-and-mahan-air/.

49 For more information on the case, see DOJ, "Chinese Nationals Charged With Illegally Exporting U.S-Origin Electronic Components to Iran and Iranian Military Affiliates," (January 2024), https://www.justice.gov/usao-dc/pr/chinese-nationals-charged-illegally-exporting-us-origin-electronic-components-iran-and.

50 State, "Sanctions to Disrupt Russia's Military Industrial Base and Sanctions Evasion," (January 2025), https://2021-2025.state.gov/office-of-the-spokesperson/releases/2025/01/sanctions-to-disrupt-russias-military-industrial-base-and-sanctions-evasion/; and Treasury, "Treasury Targets Actors Involved in Drone Production for Russia's War Against Ukraine," (October 2024), https://home.treasury.gov/news/press-releases/jy2651.

51 Commerce BIS, "Commerce Adds 26 Entities to the Entity List for Actions Contrary to U.S. National Security Interests," (October 2024), https://www.bis.gov/press-release/commerce-adds-26-entities-entity-list-actions-contrary-u.s.-national-security-interests.

52 The remaining seven Pakistani entities were added for contributions to Pakistan's ballistic missile program. For more information, see Commerce BIS, "Commerce Adds 26 Entities to the Entity List for Actions Contrary to U.S. National Security Interests," (October 2024), https://www.bis.gov/press-release/commerce-adds-26-entities-entity-list-actions-contrary-u.s.-national-security-interests.

53 State, "U.S. Sanctions on Four Entities Contributing to Pakistan's Ballistic Missile Program," (December 2024), https://2021-2025.state.gov/u-s-sanctions-on-four-entities-contributing-to-pakistans-ballistic-missile-program/.

Syria

In December 2024, the Bashar al-Assad regime collapsed. Following President Trump's decision in May 2025 to recognize the new government in Damascus and cease U.S. sanctions on Syria, the comprehensive economic sanctions program previously administered by OFAC against the Syrian government was lifted.[54] In November 2025, the United States issued a suspension of mandatory Caesar Act sanctions.[55] In December 2025, the Department of the Treasury, Department of State, and Department of Commerce issued updated industry guidance on sanctions and export controls relief to support Syria's efforts to rebuild its economy.[56] More broadly, the European Union, the United Kingdom, and other jurisdictions provided sanctions relief to Syria.[57,58,59]

The United States maintains sanctions on certain individuals and entities linked to Syria's proliferation and use of WMD. The 2024 NPFRA highlighted past illicit procurement and fundraising by the Assad regime, which is itself no longer a threat. The new Syrian government has also demonstrated commitment to fully eliminating the Assad regime's chemical weapons program and is currently cooperating with the International Atomic Energy Agency (IAEA) to resolve the IAEA's investigation into Syria's nuclear program. However, as the new government consolidates control and attempts to combat malign actors—including ISIS and Iran-backed terrorist groups—opportunities could arise for continued procurement and fundraising activities to support potential WMD activities within terrorist networks or in third countries, given the country's extensive historical research, development, and production of chemical weapons.

Non-State Actors

Lebanese Hizballah

Iran's strategic partner, Lebanese Hizballah (LH), continues to exploit criminalized markets. LH operates extensive smuggling networks for oil, weapons, and sanctioned goods while penetrating financial institutions globally.[60] LH also conducts multi-continental money laundering schemes that include seeking weapons and equipment on Iran's behalf, demonstrating how criminal markets supporting Iran's foreign operations serve as catalysts for multiple security threats.

While Iran has supported LH and others through a vast network of front companies, banks, and individuals, LH also finances itself through a broad range of illicit activities, including oil smuggling, money laundering, drug trafficking, counterfeiting, and illegal weapons procurement. LH also utilizes networks of front companies and legitimate businesses like money exchange companies, as well as digital assets, to raise, launder, and transfer funds. LH financiers make use of free trade zones and jurisdictions with weak regulatory frameworks to establish import-export companies that facilitate trade-based money laundering schemes. These companies are often held in the

54 Treasury, "OFAC Frequently Asked Questions," (June 2025), https://ofac.treasury.gov/faqs/added/2025-06-30.

55 State, "Sanctions Relief that Gives the Syrian People a Chance at Greatness," (November 2025), https://www.state.gov/releases/office-of-the-spokesperson/2025/11/sanctions-relief-that-gives-the-syrian-people-a-chance-at-greatness.

56 Treasury, "Sanctions and Export Controls Relief for Syria," (December 2025), https://ofac.treasury.gov/media/934736/download?inline.

57 Canada, "Canadian Sanctions Related to Syria," (August 2025), https://www.international.gc.ca/world-monde/international_relations-relations_internationales/sanctions/syria-syrie.aspx?lang=eng.

58 Council of Europe, "Syria: EU adopts legal acts to lift economic sanctions on Syria, enacting recent political agreement," (May 2025), https://www.consilium.europa.eu/en/press/press-releases/2025/05/28/syria-eu-adopts-legal-acts-to-lift-economic-sanctions-on-syria-enacting-recent-political-agreement/.

59 United Kingdom, "Syria Sanctions: Guidance," (July 2025), https://www.gov.uk/government/publications/syria-sanctions-guidance#full-publication-update-history.

60 For more information, see FinCEN, "FinCEN Advisory to Financial Institutions to Counter the Financing of Iran-Backed Terrorist Organizations," (May 2024), https://www.fincen.gov/system/files/advisory/2024-05-07/FinCEN-Advisory-Iran-Backed-TF-508C.pdf.

name of a relative of the financier, for example, a spouse.[61,62] LH has been known to operate through networks in Europe, the Middle East, and West Africa, and has pursued weapons and explosives precursor procurement efforts in Asia and the Western Hemisphere.[63] Also, the organization has a presence in the Tri-Border Area of Argentina, Brazil, and Paraguay, and in free trade zones in Chile and Panama, with members and supporters identified in Colombia and Peru as well.[64]

Houthis

Ansarallah, commonly known as the Houthis, continues to exploit illicit trade routes to smuggle goods into areas under their control, ensuring a steady supply of weapons and bolstering their combat capabilities. This is evidenced by significant government seizures of weapons and other dual-use items, underscoring ongoing violations and evasion of the UN arms embargo. Furthermore, access to financial resources remains a key factor in sustaining the Houthis' supply networks and production capacity, as noted by the most recent UN POE report, which assessed that the UN asset freeze provisions have had a limited impact.[65]

Moreover, the Houthis have engaged in PF by using a sophisticated international network to procure tens of millions of dollars' worth of weapons and sensitive goods from China, Iran, and Russia for shipment to Yemen. The Houthis are known to benefit from Iran's multi-jurisdictional "shadow banking" networks. For example, transactions involving these networks have supported Iran's assistance to the Houthis, including in their efforts to attack global shipping vessels.[66] In September 2025, OFAC designated 32 individuals and entities and identified four vessels to target those involved in financing and moving advanced military-grade materials, including ballistic missile, cruise missile, and UAV components, for the Houthis.[67] Also, this OFAC action demonstrated how the Houthis engage in the seizure of state and private assets under fraudulent pretenses, redirecting the profits for their own use. Revenue from these illicit operations funds the Houthis' international weapons procurement network, which depends on operatives, front companies, and a range of suppliers. Houthi financiers engage in operations involving digital assets to move and launder large sums of money. OFAC has designated several individuals and entities in relation to Houthi digital asset schemes.[68]

Another illicit procurement network, coordinated by senior Houthi financial officials and backed by Iran's IRGC, regularly participates in financial schemes, including money laundering operations across the Gulf, Türkiye, and Russia in support of Iran and its allies.[69] Houthi financial facilitators also participate in illicit oil smuggling to finance activities.

---

61 *Id.*

62 In November 2025, OFAC sanctioned Hizballah operatives exploiting money exchange companies and the cash economy to launder illicit funds. For more information, see Treasury, "Treasury Sanctions Hizballah Operatives Exploiting Lebanon's Cash Economy," (November 2025), https://home.treasury.gov/news/press-releases/sb0308.

63 FinCEN, "FinCEN Alert to Financial Institutions to Counter Financing of Hizballah and its Terrorist Activities," (October 2024), https://www.fincen.gov/system/files/shared/FinCEN-Alert-Hizballah-Alert-508C.pdf.

64 See Footnote 60.

65 See Footnote 46.

66 See Footnote 34.

67 Treasury, "Treasury Sanctions Houthi Illicit Revenue and Procurement Networks," (September 2025), https://home.treasury.gov/news/press-releases/sb0243.

68 See, e.g., Treasury, "Treasury Maintains Pressure on Houthi Procurement and Financing Schemes," (December 2024), https://home.treasury.gov/news/press-releases/jy2757; Treasury, "Counter Terrorism and Iran-Related Designations Removals and Updates," (May 2024), https://ofac.treasury.gov/recent-actions/20240524; and Chainalysis, "OFAC Highlights Hundreds of Millions of Dollars in Cryptocurrency Transactions Related to IRGC-connected Houthi Financier Sa'id al-Jamal," (December 2024), https://www.chainalysis.com/blog/ofac-highlights-hundreds-of-millions-of-dollars-in-cryptocurrency-transactions-related-to-irgc-connected-houthi-financier-said-al-jamal/.

69 Treasury, "Treasury Sanctions Houthi Network Procuring Weapons and Commodities from Russia," (April 2025), https://home.treasury.gov/news/press-releases/sb0068#:~:text=WASHINGTON%20%E2%80%94%20Today%2C%20the%20Department%20of,funds%20associated%20with%20their%20activities.

TCOs/Foreign Terrorist Organizations (FTOs)

In December 2025, President Donald Trump signed an Executive Order designating illicit fentanyl and its core precursor chemicals as WMD. Two milligrams of fentanyl, equivalent to 10 to 15 grains of table salt, constitutes a lethal dose. The manufacture and distribution of fentanyl, primarily performed by organized criminal networks, threatens U.S. national security and fuels armed conflict and lawlessness in the Western Hemisphere.[70] Between 1999 and 2023, more than 800,000 people in the United States died from an opioid overdose, enriching foreign-based cartels at the expense of American lives.[71] Drug overdose deaths in the United States declined nearly 24 percent from 2023 to 2024, but illicit fentanyl continues to be the largest driver of overdose deaths and the top counternarcotics priority for the U.S. government.[72]

Western Hemisphere-headquartered TCOs, including the Sinaloa Cartel and Cártel de Jalisco Nueva Generación (CJNG) in Mexico, remain the dominant producers and suppliers of illicit drugs, including fentanyl.[73,74] TCOs can use various methods to launder their drug trafficking proceeds through the U.S. financial system, posing risks to banks and money services businesses (MSBs), as well as non-financial businesses and professions (such as attorneys and real estate professionals). In recent years, these TCOs have increasingly used Chinese money laundering networks (CMLNs), which move value across borders through informal value transfer systems (IVTS), trade-based money laundering (TBML) schemes, and digital assets. For more information about how fentanyl trafficking is driven by the illicit proceeds that TCOs seek to gain, see the 2026 National Money Laundering Risk Assessment.

70 White House, "DESIGNATING FENTANYL AS A WEAPON OF MASS DESTRUCTION," (December 2025), https://www.whitehouse.gov/presidential-actions/2025/12/designating-fentanyl-as-a-weapon-of-mass-destruction/.

71 Centers for Disease Control and Prevention (CDC), "Understanding the Opioid Overdose Epidemic," (June 2025), https://www.cdc.gov/overdose-prevention/about/understanding-the-opioid-overdose-epidemic.html.

72 CDC, "CDC Reports Nearly 24% Decline in U.S. Drug Overdose Deaths," (February 2025), https://www.cdc.gov/media/releases/2025/2025-cdc-reports-decline-in-us-drug-overdose-deaths.html.

73 See DNI, *2025 Threat Assessment*, (n 2) 5.

74 On January 20, 2025, President Trump issued an executive order establishing a process through which several such cartels have been designated as FTOs, consistent with section 219 of the INA (8 U.S.C. 1189), or Specially Designated Global Terrorists, consistent with IEEPA (50 U.S.C. 1702) and Executive Order 13224 of September 23, 2001.

VULNERABILITIES

PF vulnerabilities refer to factors that can be exploited by threat actors that may support or facilitate the breach, non-implementation, or evasion of PF-TFS. Because U.S. technology is critical for cyber, economic, and military competitiveness, the DPRK and other actors target U.S. firms, especially those with access to dual-use items that are difficult to acquire elsewhere in the global supply chain. For the United States, the most relevant national-level factors are economic, trade, regulatory, industrial, and technological. The most relevant sectoral-level vulnerabilities include financial institutions, especially through correspondent banking and financial institutions providing digital asset services,[75] and other industries that are not subject to the same AML/CFT/CPF controls globally (such as IT workers and the maritime and shipping sectors).

National-Level Vulnerabilities

a. Economic and Trade

PF and sanctions evasion threat actors target countries that act as international financial centers, given their importance to global financial flows and transportation. The PF risk stems from the extensive array of financial products and services provided by global financial centers that cater to diverse customers. The United States has the largest and most complex financial sector in the world. The financial sector offers extensive services to private sector entities, including foreign banks, through correspondent banking relationships and other financial connections. While essential for facilitating international commerce and economic growth, this also encourages misuse and exploitation by illicit procurement networks.

Also, the prominent role of the U.S. financial system stems from the U.S. dollar being the preferred currency for key global economic functions, particularly as an international reserve currency, currency anchor, and medium for cross-border transactions. The sheer volume of trade linked to the U.S. financial system means that a notable volume of global illicit procurement and sanctions evasion activity occurs in U.S. dollars and transits through U.S. bank accounts.[76]

b. Regulatory

In line with longstanding sanctions obligations, all U.S. persons, such as U.S. financial institutions, including DASPs and designated non-financial businesses and professions (DNFBPs), are required to comply with the sanctions regulations administered by OFAC, including those applicable to PF and PF sanctions evasion.[77] U.S. persons are also required to adhere to export control regulations administered by the U.S. Department of Commerce. Specifically, the export, re-export, or transfer of U.S.-origin items and other items subject to the EAR must also comply with U.S. export controls. Since 2021, PF has been one of FinCEN's enumerated AML/CFT priorities, which helps financial institutions and other covered entities to categorize top financial crime issues in line with their risk exposure.

75 The BSA and its implementing regulations take an activities-based approach, which ensures that virtual asset service providers (VASPs), as defined by the FATF, have AML/CFT obligations as financial institutions in the U.S. AML/CFT framework based on the activities that they conduct and the attendant illicit finance risks. Because the FATF definition for VASP excludes entities otherwise covered by the FATF Recommendations (*e.g.*, financial institutions), the U.S. will use the term "digital asset service providers" (DASPs) when referring to financial institutions subject to U.S. jurisdiction that conduct activities covered in the FATF VASP definition. This is to clarify that DASPs are covered functionally as financial institutions based on the activities that they conduct.

76 The United States maintains a robust and expansive economy representing 26% of global GDP, supported by a history of economic stability rooted in strong investor safeguards and legal frameworks. This economic scale and reliability make the dollar an attractive store of value and refuge for international investors. International companies and governments use dollars for trade and currency exchanges through the correspondent banking system.

77 Code of Federal Regulations, "§ 544.312 United States person; U.S. person," (January 2026), https://www.ecfr.gov/current/title-31/section-544.312

As outlined in previous NPFRAs, illicit actors craft schemes that evade sanctions and circumvent export controls. The threat actors may conduct jurisdictional arbitrage by operating through countries with weaker CPF controls or limited cooperation with U.S. authorities, effectively moving operations outside U.S. regulatory reach.[78] Also, PF networks exploit regulatory blind spots, including jurisdictions where businesses can be utilized to disguise beneficial ownership. Connected to the correspondent banking vulnerability is the misuse of legal persons and arrangements, especially since foreign-based shell and front companies often appear in schemes that exploit transshipment hubs (many of which have meaningful financial links to the United States) with goods destined for high-risk countries. These deceptive practices can cause U.S. companies to export dual-use goods to front companies in transshipment countries under the guise that the ultimate destination is not a country like Iran, which is under strict U.S. sanctions and export control laws and regulations.

As described in the 2024 NPFRA and exemplified through certain case studies in the 2018 and 2022 NPFRAs, illicit proliferation schemes can also involve U.S.-based front and shell companies. The availability of beneficial ownership information collected through the 2016 Customer Due Diligence (CDD) Rule via judicial processes helps to mitigate the vulnerability of opaque ownership structures for law enforcement. For an example of how U.S. authorities addressed Pakistani PF actors using U.S.-based front and shell companies, see p. 30-31 of the 2018 NPFRA.[79] For an example of how U.S. authorities addressed Iranian PF actors using U.S.-based front and shell companies, see p. 21 of the 2022 NPFRA.[80]

More broadly, the United States assesses that the main PF threat actors predominantly rely on foreign-based front and shell companies rather than U.S.-based front and shell companies. This PF vulnerability is mitigated by U.S. comprehensive sanctions that generally prohibit U.S. persons from direct or indirect commercial, financial, or trade transactions, including transactions involving the Government of North Korea or Workers' Party of Korea, unless authorized by OFAC or exempt. U.S. persons, including legal entities, that engage in such prohibited transactions face potential civil or criminal enforcement actions. The United States has allocated significant resources toward multiagency cooperation and coordination to enable the use of intelligence, law enforcement, and other relevant tools to target proliferation actors.

c. Industrial and Technological

A significant component of WMD proliferation involves technology transfer, particularly in relation to dual-use goods and technologies. Dual-use goods and technologies include items that are applicable to civilian use but may be export-controlled. Illicit actors operate in sectors relevant to the smuggled dual-use goods or items, such as electronics, chemicals, or industrial equipment, or other goods subject to sanctions or export control regulations. Proliferation networks target vulnerabilities in U.S. industrial and technological sectors to acquire prohibited goods illegally. The United States' position as a major manufacturer of sensitive technology and dual-use items makes it inherently vulnerable to PF and export control breaches. The U.S. defense industry's reliance on numerous contractors and suppliers also provides proliferation actors with opportunities to infiltrate these intricate supply networks. The complex nature of dual-use technologies can make it difficult to identify illicit procurement activity as well. However, the United States employs the world's most comprehensive export controls and sanctions programs to restrict the movement of sensitive goods to illicit actors and cut off their access to funds and financial networks, respectively, in order to disrupt illicit procurement.

78 In certain instances, a threat actor providing money transmission services may be subject to the U.S. AML/CFT regime as a money services business if the threat actor is doing business wholly or in substantial part in the United States. For more information, see Code of Federal Regulations, "§ 1010.100 General Definitions (Money services business, Money transmitter)," (January 2026), https://www.ecfr.gov/current/title-31/subtitle-B/chapter-X/part-1010/subpart-A/section-1010.100#p-1010.100(ff)(5).

79 See Footnote 4.

80 *Id.*

Sectoral-Level Vulnerabilities

a. Banking and Other Financial Sectors

As described in previous NPFRAs, the U.S. economy, which is the world's largest by GDP, acts as a vital base for an extensive financial sector. Funds that support PF actors or operations may originate from or pass through numerous accounts and industries, and thus flow through the U.S. financial sector and its banking system. Foreign correspondent banks face heightened sanctions evasion vulnerabilities due to their lack of direct relationships with respondent bank customers in other jurisdictions. These indirect relationships, in turn, can be exploited for PF when the correspondent banks do not generally conduct due diligence on their customers' (respondent banks) customers.[81] For more information on vulnerabilities related to correspondent banking, see the Regulatory section in this report.

b. Digital Asset Service Providers

Since the 2024 NPFRA, the digital asset ecosystem, including in the United States, has grown substantially. For example, the number of successful monthly transactions on public blockchains reached highs of 3.8 billion in early 2025—a 96% increase year-over-year.[82] Notably, the use of stablecoins has also increased—for example, the total market capitalization of U.S. dollar-backed stablecoins, which dominate stablecoin activity, grew over 66% between 2022 and mid-2025.[83] This growth in digital assets, paired with the relative stability of stablecoins, has attracted both legitimate users as well as criminal groups and syndicates that seek to exploit any developments in payment technology, especially DPRK cybercriminals, who are using digital assets to launder illicit proceeds. The ability to transfer assets quickly across borders and perceptions of anonymity make digital assets attractive to both licit and illicit actors.

PF networks often seek to exploit the lack of effective implementation of AML/CFT/CPF measures for digital assets across jurisdictions, opting to use foreign-based service providers of digital assets with weak controls.[84] This is particularly challenging given the gaps in implementation of the FATF Standards for digital assets in several jurisdictions—illicit actors choose to use DASPs based in jurisdictions without AML/CFT obligations. The global nature of digital assets and inconsistent international implementation of the FATF Standards complicates efforts to halt the misuse of digital assets by the DPRK and other sanctioned entities. Additionally, in some instances, PF networks may exploit AML/CFT/CPF weaknesses at DASPs operating wholly or in substantial part within the United States.

The DPRK uses sophisticated laundering networks to convert stolen digital assets into revenue for the regime's weapons programs. In its laundering process, the DPRK uses services like mixers[85] and techniques such as establishing DASP accounts with fictitious information, using U.S.-based online accounts to legitimize activity, and exploiting DASPs with weak AML/CFT controls. These methods are used to exploit U.S. DASPs, in particular IT workers receiving digital assets as payment for their services prior to the laundering of the funds. The DPRK often converts laundered digital

81 In foreign correspondent banking, financial institutions in two different countries maintain accounts with one another to process transactions on behalf of themselves and their clients. While these cross-border banking partnerships between foreign banks and U.S. institutions are essential for enabling global trade and investment flows, they also create elevated illicit finance risks due to the complexity and international nature of these financial arrangements. For more information, see FDIC, "Risk Management Manual Examination Policies: Bank Secrecy Act, Anti-Money Laundering, and Office of Foreign Assets Control, Section 8.1," (October 2025), https://www.fdic.gov/risk-management-manual-examination-policies/section-8-1.pdf.

82 a16zcrypto, "State of Crypto Index," (January 2026), https://a16zcrypto.com/stateofcryptoindex. This data serves as a proxy for activity across certain blockchains (specifically Ethereum, Polygon, Solana, Avalanche, Fantom, Celo, Optimism, Base, and Arbitrum).

83 White House, "STRENGTHENING AMERICAN LEADERSHIP IN DIGITAL FINANCIAL TECHNOLOGY," (July 2025), https://www.whitehouse.gov/wp-content/uploads/2025/07/Digital-Assets-Report-EO14178.pdf.

84 *See* FATF, Targeted Update on Implementation of the FATF Standards on Digital Assets and Digital Asset Service Providers (June 2025), https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/2025-Targeted-Upate-VA-VASPs.pdf.coredownload.pdf; and Footnote 16.

85 Mixers use various mechanisms to functionally obfuscate the source, destination, or amount in a digital asset transaction.

assets into stablecoins before exchanging them for fiat currency through over-the-counter (OTC) brokers.[86] In certain instances, the DPRK directs foreign OTC brokers to use laundered digital assets to purchase goods for the DPRK regime through foreign-based front companies.[87] In at least one case, one such OTC broker facilitated the conversion of digital assets stolen by DPRK actors working with the Lazarus Group to fiat currency.[88] The OTC broker also allegedly operated as an unlicensed trader on a U.S.-based DASP and conducted over 1,500 trades for U.S. customers, illustrating potential exposure to the U.S. financial system.[89]

The DPRK presents a substantial risk to U.S. DASPs because the providers may unwittingly employ DPRK IT workers or perpetuate ransomware attacks. Additionally, the DPRK generates significant revenue by stealing from service providers of digital assets, turning many DASPs into victims of theft.[90] In fact, in February 2025, DPRK cybercriminals stole digital assets valued at $1.5 billion from Bybit—one of the largest digital assets thefts ever.[91] The DPRK also generates revenue in digital assets obtained through salaries paid to IT workers, in particular stablecoins, that are remitted back to the government, and, to a smaller degree, in ransom payments following ransomware attacks.

c. Non-Financial Sectors

There are PF vulnerabilities in non-financial sectors like remote IT workers and the maritime and shipping sectors, which are generally not subject to uniform AML/CFT/CPF controls globally. Consequently, the 2024 NPFRA, like its 2018 and 2022 predecessors, considers the entire illicit procurement supply chain.[92] Not only do PF networks need to illicitly access financial services, but they also depend on global shipping. This vulnerability arises in revenue-raising activities (such as natural resource trade in breach of UNSCR or U.S. sectoral sanctions), as well as procuring U.S.-origin goods in ways to obfuscate their end-user or end-destination. In the latter case, the U.S. monitors the use of transshipment hubs, often paired with foreign-based front and shell companies to obscure transactions and the origin of funds (as referenced in the National-Level Vulnerabilities section). Consequently, the United States prioritizes issuing guidance related to relevant sectors not subject to the same AML/CFT/CPF controls as other sectors to strengthen sanctions and AML/CFT compliance posture. For further information, see the May 2022 and July 2025 guidance documents related to DPRK IT Workers, and OFAC's October 2024 *Compliance Communiqué* for the maritime shipping industry.[93]

86 DOJ, "Department Files Civil Forfeiture Complaint Against Over $7.74M Laundered on Behalf of the North Korean Government," (June 2025), https://www.justice.gov/opa/pr/department-files-civil-forfeiture-complaint-against-over-774m-laundered-behalf-north-korean; and DOJ, "U.S. vs. Virtual Currency Associated with North Korean IT Worker Money Laundering and Sanctions Evasion Conspiracies," paragraph 59, (June 2025), https://www.justice.gov/usao-dc/media/1402691/dl.

87 See, e.g., DOJ, "North Korean Foreign Trade Bank Representative Charged in Crypto Laundering Conspiracies," (April 2023), https://www.justice.gov/archives/opa/pr/north-korean-foreign-trade-bank-representative-charged-crypto-laundering-conspiracies; DOJ, "U.S. vs. Sim Hyon Sop, et al." (April 2023), https://www.justice.gov/usao-dc/press-release/file/1581286/dl; and DOJ, "Treasury Targets Actors Facilitating Illicit DPRK Financial Activity in Support of Weapons Programs," (April 2023), https://home.treasury.gov/news/press-releases/jy1435.

88 Treasury, "Treasury Targets Actors Facilitating Illicit DPRK Financial Activity in Support of Weapons Programs," (April 2023), https://home.treasury.gov/news/press-releases/jy1435.

89 DOJ, "North Korean Foreign Trade Bank Rep Charged for Role in Two Crypto Laundering Conspiracies," (April 2023), https://www.justice.gov/usao-dc/pr/north-korean-foreign-trade-bank-rep-charged-role-two-crypto-laundering-conspiracies.

90 DOJ, "Four North Koreans Charged in Nearly $1 Million Cryptocurrency Theft Scheme," (June 2025), https://www.justice.gov/usao-ndga/pr/four-north-koreans-charged-nearly-1-million-cryptocurrency-theft-scheme.

91 Federal Bureau of Investigation (FBI), "Public Service Announcement: North Korea Responsible for $1.5 Billion Bybit Hack," (February 2025), https://www.ic3.gov/psa/2025/psa250226.

92 See Footnote 4.

93 See Treasury, "GUIDANCE ON THE DEMOCRATIC PEOPLE'S REPUBLIC OF KOREA INFORMATION TECHNOLOGY WORKERS," (May 2022), https://ofac.treasury.gov/media/923131/download?inline; FBI, "Public Service Announcement: North Korean IT Worker Threats to U.S. Businesses," (July 2025), https://www.ic3.gov/PSA/2025/PSA250723-4; and Treasury, "Compliance Communique: Sanctions Guidance for the Maritime Shipping Industry," (October 2024), https://ofac.treasury.gov/media/933556/download?inline.

TYPOLOGIES

Based on a review of U.S. cases and actions since the publication of the 2024 NPFRA, this section summarizes two broad categories of typologies relevant to PF. The typologies include case studies that illustrate the intersection between relevant threats and vulnerabilities. Because there can be notable overlap between the techniques employed across the following typologies, the case examples are tagged with key information such as their main threats and vulnerabilities.

Typology 1: Abusing the Global Technology Ecosystem

On an ongoing basis, the DPRK and other well-resourced illicit actors probe for weaknesses in global CPF enforcement, preventive measures, and legal frameworks, especially related to new and emerging technologies. While the remote IT worker sector presents the DPRK with revenue generation opportunities, digital assets offer perceived anonymity and speed of funds movement to evade sanctions. Consequently, it is important that the public and private sectors establish mechanisms that account for and adapt to emerging risks.

DPRK Targeting IT Worker Sector to Generate Revenue

Arizona Woman Sentenced for $17M IT Worker Fraud Scheme for the DPRK

(#China #DPRK #ITWorkers)

In July 2025, DOJ announced that Christina Marie Chapman was sentenced to 102 months in prison following a guilty plea to conspiracy to commit wire fraud, aggravated identity theft, and conspiracy to commit money laundering. From October 2020 to October 2023, she orchestrated a "laptop farm" scheme in which North Korean IT workers, posing as U.S. citizens using stolen identities to obtain remote IT jobs at more than 300 U.S. companies, generated over $17 million in illicit revenue for herself and the DPRK. Chapman stored and managed more than 90 company-supplied laptops at her home, and shipped 49 devices to Dandong, China. She was ordered to pay a judgment of $176,850 and forfeit $284,666 that was intended for North Korean operatives. In a coordinated effort, FBI Phoenix also issued guidance for HR professionals on detecting North Korean IT workers.[94] Prior guidance on this threat was issued by the FBI, Department of State, and Department of the Treasury.[95]

Sanctions Imposed on DPRK IT Workers and Associates Generating Revenue for the DPRK

(#China #DPRK #Laos #Russia #Intermediaries #FrontCompanies #ITWorkers)

In August 2025, OFAC designated Vitaliy Sergeyevich Andreyev, Kim Ung Sun, Shenyang Geumpungri Network Technology Co. Ltd., and Korea Sinjin Trading Corporation (Sinjin) for their roles in a fraudulent IT worker scheme orchestrated by the DPRK.[96] Andreyev, a Russian national, facilitated payments to OFAC-designated Chinyong Information Technology Cooperation Company, an entity associated with the DPRK defense ministry that employs delegations of IT workers in Russia and Laos. Since at least December 2024, Andreyev has worked with Kim Ung Sun, a Russia-based DPRK economic and trade consular official, to facilitate multiple financial transfers worth

94 DOJ, "Arizona Woman Sentenced for $17M Information Technology Worker Fraud Scheme that Generated Revenue for North Korea," (July 2025), https://www.justice.gov/opa/pr/arizona-woman-sentenced-17m-information-technology-worker-fraud-scheme-generated-revenue.

95 See, e.g., FBI, "Public Service Announcement: North Korean IT Workers Conducting Data Extortion," (January 2025), https://www.ic3.gov/PSA/2025/PSA250123?utm_medium=email&utm_source=govdelivery; FBI, "Public Service Announcement: Democratic People's Republic of Korea Leverages U.S.-Based Individuals to Defraud U.S. Businesses and Generate Revenue," (May 2024), https://www.ic3.gov/PSA/2024/PSA240516?utm_medium=email&utm_source=govdelivery; and Treasury, "GUIDANCE ON THE DEMOCRATIC PEOPLE'S REPUBLIC OF KOREA INFORMATION TECHNOLOGY WORKERS," (May 2022), https://ofac.treasury.gov/media/923131/download?inline.

96 Treasury, "Treasury Sanctions Fraud Network Funding DPRK Weapons Programs," (August 2025), https://home.treasury.gov/news/press-releases/sb0230.

a total of nearly $600,000 by converting digital assets to cash in U.S. dollars. Shenyang Geumpungri Network Technology Co., Ltd. (Shenyang Geumpungri) is a Chinese front company for Chinyong, consisting of a delegation of DPRK IT workers. Since 2021, Shenyang Geumpungri's delegation of DPRK IT workers has earned over $1 million in profits for Chinyong and Sinjin.[97]

Separately, in July 2025, OFAC designated Song Kum Hyok, a malicious cyber actor linked to North Korea's Reconnaissance General Bureau,[98] who facilitated an IT worker fraud scheme. DPRK nationals—working from China, Russia, and elsewhere—used stolen U.S. identities and forged documents to obtain remote employment at companies worldwide and generate revenue that supports the DPRK's weapons programs. Some of these workers also introduced malware to their target networks. OFAC also sanctioned one individual, Gayk Asatryan, and four associated entities based in Russia for participating in similar schemes. The actors were involved in a Russia-based IT worker scheme that generated illicit revenue for the DPRK. In mid-2024, Asatryan signed a 10-year contract with a DPRK company to dispatch 30 DPRK IT workers to operate from his company in Russia. Asatryan also signed a contract with another DPRK company, in which the company planned to dispatch 50 DPRK IT workers to Russia for another one of his companies.[99]

In another July 2025 OFAC action, one entity and three individuals were designated for their involvement in the evasion of U.S. and UN sanctions and efforts to generate revenue clandestinely for the DPRK, including through fraudulent IT worker schemes. Operating as a front company for the DPRK's Munitions Industry Department, the entity dispatched IT workers using stolen identities and false personas to infiltrate legitimate companies and generate revenue.[100]

NJ Resident and Others Indicted for Supporting DPRK IT Worker Scheme

(#China #DPRK #Taiwan #IDTheft #ITWorkers #ShellCompanies)

In June 2025, a U.S. national was indicted for his role in a multi-year DPRK IT worker scheme that defrauded U.S. companies and generated more than $5 million in revenue. The indictment also charged six Chinese nationals and two Taiwanese nationals for their roles in the scheme.[101, 102]

According to the indictment, from approximately 2021 until October 2024, the defendants and other co-conspirators compromised the identities of more than 80 U.S. persons to obtain remote jobs at more than 100 U.S. companies, including many Fortune 500 companies, and caused U.S. victim companies to incur legal fees, computer network remediation costs, and other damages and losses of at least $3 million. Overseas IT workers were assisted by co-conspirators and at least four other U.S. facilitators. To deceive U.S. companies into believing the IT workers were located in the United States, co-conspirators and the other U.S. facilitators received and/or hosted laptops belonging to U.S. companies at their residences, and enabled overseas IT workers to access the laptops remotely by, among other things, connecting the laptops to hardware devices designed to allow for remote access (referred to as keyboard-video-mouse or "KVM" switches).

---

97 Sinjin is a DPRK company subordinate to the U.S.-sanctioned DPRK Ministry of People's Armed Forces General Political Bureau. For more information, see Treasury, "Treasury Sanctions Fraud Network Funding DPRK Weapons Programs," (August 2025), https://home.treasury.gov/news/press-releases/sb0230.

98 UN-designated Reconnaissance General Bureau is a DPRK military intelligence agency.

99 Treasury, "Sanctions Imposed on DPRK IT Workers Generating Revenue for the Kim Regime," (July 2025), https://home.treasury.gov/news/press-releases/sb0190.

100 Alongside Treasury, DOJ also unsealed indictments against seven DPRK nationals for the criminal avoidance of sanctions under IEEPA involving the illicit trafficking of counterfeit cigarettes. For more information on this case example, see Treasury, "Treasury Sanctions Clandestine IT Worker Network Funding the DPRK's Weapons Programs," (July 2025), https://home.treasury.gov/news/press-releases/sb0205.

101 DOJ, "Justice Department Announces Coordinated, Nationwide Actions to Combat North Korean Remote Information Technology Workers' Illicit Revenue Generation Schemes," (June 2025), https://www.justice.gov/opa/pr/justice-department-announces-coordinated-nationwide-actions-combat-north-korean-remote.

102 A second U.S. national agreed to plead guilty to his role in this scheme and was charged separately. See DOJ, "US vs Kejia Wang," (June 2025), https://www.justice.gov/opa/media/1406386/dl?inline.

Two of the co-conspirators also created shell companies with corresponding websites and financial accounts to make it appear as though the overseas IT workers were affiliated with legitimate U.S. businesses. The two co-conspirators established these and other financial accounts to receive money from victimized U.S. companies, much of which was subsequently transferred to overseas co-conspirators. In exchange for their services, the foreign national co-conspirators and the four other U.S. facilitators received a total of at least $696,000 from the IT workers.

In a concurrent action with the indictment, the FBI and Defense Criminal Investigative Service (DCIS) seized 17 web domains used in furtherance of the charged scheme and further seized 29 financial accounts, holding tens of thousands of dollars in funds, used to launder revenue for the North Korean regime through the remote IT worker scheme.[103]

Using Digital Assets to Obscure and Move Funds

DOJ Files Civil Forfeiture Complaint involving DPRK

(#DPRK #China #Russia #DigitalAssets #ITWorkers)

In June 2025, the DOJ filed a civil forfeiture complaint targeting over $7.74 million in digital assets, including stablecoins, that were laundered on behalf of the DPRK. These funds were linked to an April 2023 indictment of an OFAC-designated representative of North Korea's FTB, who allegedly collaborated with North Korean IT workers deployed globally—including in China and Russia—to obtain remote employment in the tech sector under false identities, generating illicit digital asset revenue by asking to be paid in stablecoin.[104] The laundering strategy involved a variety of sophisticated techniques: establishing fictitious accounts, structured transfers in small amounts, leveraging "chain hopping" and "token swapping," purchasing non-fungible tokens (NFTs) to obscure asset origin, using U.S.-based online accounts to legitimatize activity, and commingling proceeds before funneling them back to North Korea.[105]

Four DPRK Nationals Charged in Digital Assets Theft Scheme

(#DPRK #Malaysia #Serbia #UAE #CyberTheft #DigitalAssets #ITWorkers)

In June 2025, four DPRK nationals were charged in a five-count wire fraud and money laundering indictment arising from a scheme in which they were hired as remote IT workers and then stole and laundered over $900,000 in digital assets.[106]

In October 2019, the defendants traveled to the United Arab Emirates on North Korean documents and worked there as a team. In approximately December 2020 and May 2021, respectively, two of the defendants were hired as developers by an Atlanta, Georgia-based blockchain research and development company and a Serbian virtual token company. Both defendants concealed their North Korean identities from their employers by providing false identification documents containing a mix of stolen and fraudulent identity information. Neither company would have hired the individuals had they known the defendants were DPRK nationals. Later, on a recommendation from one of the defendants, the Serbian company hired a third DPRK national.

After gaining their employers' trust, the defendants were assigned projects that provided them with access to their employers' digital assets. In February 2022, one defendant used that access to steal digital assets then worth approximately $175,000. In March 2022, another defendant stole digital assets then worth approximately $740,000 by modifying the source code of two of his employer's smart contracts.

103 In October 2024, as part of this investigation, federal law enforcement executed searches at eight locations across three states that resulted in the recovery of more than 70 laptops and remote access devices, such as KVMs. Simultaneously with that action, the FBI seized four web domains associated with the co-conspirators' shell companies used to facilitate North Korean IT work.

104 See DOJ, "North Korean Foreign Trade Bank Representative Charged in Crypto Laundering Conspiracies," (April 2023), https://www.justice.gov/archives/opa/pr/north-korean-foreign-trade-bank-representative-charged-crypto-laundering-conspiracies.

105 DOJ, "Department Files Civil Forfeiture Complaint Against Over $7.74M Laundered on Behalf of the North Korean Government," (June 2025), https://www.justice.gov/opa/pr/department-files-civil-forfeiture-complaint-against-over-774m-laundered-behalf-north-korean.

106 See Footnote 90.

To launder the funds after the thefts, the defendants used a digital asset mixer and then transferred the funds to digital asset exchange accounts controlled by other DPRK nationals but held in the names of aliases. The accounts were opened using fraudulent Malaysian identification documents.

Digital Assets Company Founder Charged with Evading Sanctions and Export Controls

(#Russia #Banks #DigitalAssets #FrontCompanies)

In June 2025, a 22-count indictment was unsealed charging a U.S.-based Russian national with various offenses related to using his digital asset company, Evita, to funnel more than $500 million of overseas payments through U.S. banks and digital asset exchanges while hiding the source and purpose of the transactions.[107]

As alleged in the indictment, the defendant is the founder, president, treasurer, and compliance officer of two associated U.S-based companies. The defendant used both companies to enable foreign customers—many of whom held funds at sanctioned Russian banks—to provide him with digital assets, which he then laundered through digital asset wallets and U.S. bank accounts. The defendant converted the funds into U.S. dollars or other fiat currencies and then made payments through bank accounts in Manhattan on behalf of his foreign customers. In the process, the sources of the funds were obscured, disguising the audit trail and hiding the true counterparties to the transactions. Between June 2023 and January 2025, the defendant used his company as a front to facilitate the movement of approximately $530 million through the U.S. financial system, most of which he received in the form of stablecoins.

To effectuate the scheme, the defendant defrauded various banks and digital asset exchanges through which he converted funds and made wire transfers. The defendant repeatedly lied to these banks and exchanges, telling them that his company did not conduct business with entities in Russia and did not deal with sanctioned entities. In fact, many of the defendant's customers were located in Russia, and he facilitated payments in funds held at sanctioned Russian banks. He also facilitated payments by foreign customers to procure sensitive electronics, including an export-controlled server designed by a U.S. technology company, and laundered funds from a Moscow-based supplier to purchase parts for Rosatom, Russia's state-owned nuclear technology company. To conceal his activities, the defendant regularly obfuscated invoices by digitally "whiting out" the names and addresses of his Russian customers.

Update on Maui Ransomware Scheme

(#China #DPRK #HongKong #DigitalAssets #Ransomware)

In July 2024, a North Korean national was indicted for his involvement in a conspiracy to hack and extort U.S. hospitals and other health care providers, launder the ransom proceeds, and then use these proceeds to fund additional computer intrusions into defense, technology, and government entities worldwide.[108] In 2022, the Maui ransomware attacks prevented victim health care providers from providing full and timely care to patients.[109]

According to court documents, the defendant and his co-conspirators worked for North Korea's Reconnaissance General Bureau (known to the private sector as "Andariel," "Onyx Sleet," and "APT45."). The defendant and his co-conspirators laundered ransom payments through China-based facilitators and used these proceeds to purchase internet infrastructure, which the co-conspirators then used to hack and exfiltrate sensitive defense and technology information from entities across the globe.

These DPRK actors received ransom payments in digital assets and then laundered the payments with the

107 DOJ, "Founder of Cryptocurrency Payment Company Charged with Evading Sanctions and Export Controls, Defrauding Financial Institutions, and Violating the Bank Secrecy Act," (June 2025), https://www.justice.gov/opa/pr/founder-cryptocurrency-payment-company-charged-evading-sanctions-and-export-controls.

108 DOJ, "North Korean Government Hacker Charged for Involvement in Ransomware Attacks Targeting U.S. Hospitals and Health Care Providers," (July 2024), https://www.justice.gov/archives/opa/pr/north-korean-government-hacker-charged-involvement-ransomware-attacks-targeting-us-hospitals.

109 For more information on the Maui ransomware attacks, see Treasury, "2024 National Proliferation Financing Risk Assessment," (February 2024), https://home.treasury.gov/system/files/136/2024-National-Proliferation-Financing-Risk-Assessment.pdf.

assistance of Hong Kong-based facilitators. In at least one case, these Hong Kong facilitators converted ransom funds from digital assets to Chinese yuan. The yuan was then accessed from an ATM in China in the immediate vicinity of the Sino-Korean Friendship Bridge, which connects Dandong, China, and Sinuiju, North Korea.

The Justice Department and the FBI also announced the interdiction of approximately $114,000 in digital assets proceeds of ransomware attacks and related money laundering transactions, as well as the seizure of online accounts used by co-conspirators to carry out their malicious cyber activity. Previously, the FBI seized approximately $500,000 in virtual currency proceeds of ransomware attacks and related money laundering transactions.[110] Also, the FBI and other parts of the U.S. government released a cybersecurity advisory to highlight cyber espionage activity associated with this DPRK hacking group.[111]

Typology 2: Using Money Laundering Techniques to Support Proliferation Activities

PF threat actors have operated increasingly decentralized schemes to generate revenue, access the financial system, and secure sensitive weapons components and technology in circumvention of sanctions and export controls. While specific typologies will vary across networks, PF actors have been found to use deceptive practices to obscure the origin and purpose of funds through complex legal structures and multi-jurisdictional layering. The public and private sectors must be prepared to counter illicit procurement networks that employ a variety of sophisticated laundering techniques involving intermediaries, front companies, and shell companies.

Enlisting Intermediaries to Evade Sanctions and Circumvent Export Controls

Sanctions Evasion Schemes to Smuggle U.S.-origin Electronic Components to Iran's Military

(#China #HongKong #Iran #UAE #FrontCompanies #Intermediaries #UAV)

In October 2025, OFAC targeted an Iran-based procurement network that acquires weapons components on behalf of Iran's Ministry of Defense and Armed Forces Logistics (MODAFL)-associated entities, including a Shiraz Electronics Industries (SEI)-related network based in Iran, Hong Kong, and China. Additionally, OFAC targeted a network operating out of Iran, Germany, Türkiye, Portugal, and Uruguay procuring equipment, including a U.S.-origin helicopter, for the MODAFL subsidiary, Iran Helicopter Support and Renewal Company.[112] This October OFAC action builds on previous U.S. government efforts to disrupt this illicit procurement network.

In January 2024, four Chinese nationals were indicted on various federal crimes related to a years-long conspiracy to unlawfully export and smuggle U.S.-origin electronic components from the United States to Iran. The defendants allegedly unlawfully exported and smuggled U.S. export-controlled items through China and Hong Kong for the benefit of entities affiliated with the IRGC and MODAFL that supervise Iran's development and production of missiles, weapons, and military aerial equipment, including UAVs.[113] Beginning as early as May 2007 and continuing until at least July 2020, the individuals used front companies in China to funnel dual-use U.S.-origin items, including electronics and components that could be used in the production of UAVs, ballistic missile systems, and other

110 DOJ, "Justice Department Seizes and Forfeits Approximately $500,000 from North Korean Ransomware Actors and their Conspirators," (July 2022), https://www.justice.gov/archives/opa/pr/justice-department-seizes-and-forfeits-approximately-500000-north-korean-ransomware-actors.

111 Cybersecurity & Infrastructure Security Agency, "North Korea Cyber Group Conducts Global Espionage Campaign to Advance Regime's Military and Nuclear Programs," (July 2024), https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-207a.

112 Treasury, "Treasury Targets Iranian Weapons Procurement Networks Supporting Ballistic Missile and Military Aircraft Programs," (October 2025), https://home.treasury.gov/news/press-releases/sb0270.

113 DOJ, "Chinese Nationals Charged With Illegally Exporting U.S-Origin Electronic Components to Iran and Iranian Military Affiliates," (January 2024), https://www.justice.gov/usao-dc/pr/chinese-nationals-charged-illegally-exporting-us-origin-electronic-components-iran-and.

military end uses, to sanctioned entities with ties to the IRGC and MODAFL such as SEI, Rayan Roshd Afzar, and their affiliates.[114]

Separately, in June 2024, OFAC sanctioned nearly 50 entities and individuals that constitute multiple branches of a sprawling "shadow banking" network used by MODAFL and the IRGC to generate revenue to, among other activities, illicitly procure the U.S.-origin electronic components to develop advanced weapons, such as UAVs, and support Yemen's Houthis and Russia's war in Ukraine. To gain access to the international financial system, MODAFL used exchange houses in Iran that managed numerous front companies in Hong Kong, the UAE, and elsewhere to launder revenue generated through foreign commercial activity, including oil sales, into clean foreign currency. The same front companies used the laundered foreign currency to procure weapons components on the international market.[115]

Chinese National Sentenced for Arms Trafficking on Behalf of the DPRK

(#China #DPRK #Intermediaries #Firearms #Transshipment)

In August 2025, Shenghua Wen, a Chinese national, was sentenced to 96 months in prison for illegally exporting firearms, ammunition, and other military items to the DPRK by concealing them inside shipping containers that departed from the Port of Long Beach, and for committing this crime at the direction of DPRK government officials, who wired him approximately $2 million for his efforts.[116]

In 2023, at the direction of DPRK government officials, Wen shipped at least three containers of firearms out of the Port of Long Beach to China en route to their ultimate destination in North Korea. He took steps to conceal that the illegal shipments were going to the DPRK by, among other things, filing false export information regarding the contents of the containers. In May 2023, Wen purchased a firearms business in Houston, paid for with money sent through intermediaries by one of Wen's DPRK contacts. He purchased many of the firearms he sent to the DPRK in Texas and drove the firearms from Texas to California, where he arranged for them to be shipped.

In December 2023, one of the weapons shipments—which falsely reported to U.S. officials that it contained a refrigerator—left the Port of Long Beach and arrived in Hong Kong in January 2024. This weapons shipment was later transported from Hong Kong to Nampo, North Korea. In September 2024, the individual—once again acting at the direction of DPRK officials—bought approximately 60,000 rounds of 9mm ammunition that he intended to ship to the DPRK.

OFAC Designated Entities Procuring Sensitive Machinery for Iran's Defense Industry

(#China #Iran #HongKong #Panama #Singapore #Intermediaries #Transshipment)

In June 2025, OFAC designated one individual and eight entities, and identified one vessel as blocked property, for their involvement in the procurement and transshipment of sensitive machinery for Iran's defense industry. In late 2024, a Panama-flagged bulk carrier was carrying sensitive goods bound for Iran. The scheme involved a network of companies involved in the shipping supply chain. Two China-based companies were responsible for shipping the items to the OFAC-designated, Iran-based consignees, while the Hong Kong-based registered owner of the bulk carrier prepared to obfuscate the Iranian clients through the falsification of the shipping paperwork, with the intent to later facilitate the shipments to Bandar Abbas, Iran.

---

114 Throughout the course of the conspiracy, the defendants concealed the fact that the goods were destined for Iran and Iranian entities and made material misrepresentations to U.S. companies regarding end destination and end users. These deceptive practices caused the U.S. companies to export dual-use goods to the front companies under false pretenses and under the guise that the ultimate destination of these products was China, as opposed to Iran, in violation of U.S. sanctions and export control laws and regulations.

115 Treasury, "Treasury Targets Shadow Banking Network Moving Billions for Iran's Military," (June 2024), https://home.treasury.gov/news/press-releases/jy2431.

116 DOJ, "Chinese National Sentenced for Acting at North Korea's Direction to Export Firearms, Ammo, Tech to N. Korea," (August 2025), https://www.justice.gov/opa/pr/chinese-national-sentenced-acting-north-koreas-direction-export-firearms-ammo-tech-n-korea.

Also, a Singapore-based charterer of the bulk carrier was directly involved in the coordination of cargo consigned to OFAC-designated entities. This charterer was aware that it was their responsibility to ensure that shipper and consignees for cargo were not on sanctions lists. Other individuals and entities involved in the shipment supply chain either proactively disguised the destination or did not exercise their responsibility to ensure the sensitive machinery was not bound for sanctioned entities.[117]

Spanish National Pleads Guilty to Conspiring to Export U.S. Military-Grade Radios to Russian Government End Users

(#Russia #Latvia #UAE #Intermediaries #Transshipment)

In June 2025, a Spanish national living in the United Arab Emirates, who was arrested in the United States, pleaded guilty in connection with conspiring to illegally export U.S.-origin radio communications technology to Russian end users without a license.[118]

According to court documents, beginning at least around January 2023, the defendant and others initiated discussions with a small U.S. radio distribution company about procuring and exporting to Russia U.S.-manufactured military-grade radios and related accessories. Over the next several months, the defendant continued his efforts to secure those items, which he intended to transship to Russia via a freight forwarder in Latvia.

As part of the conspiracy, the defendant purchased 200 of the military-grade radios and intended to export them to Russia. But he was not successful, as U.S. Customs and Border Protection detained the shipment, preventing the radios from falling into the hands of prohibited Russian end users.

OFAC Sanctions Houthi Network Procuring Weapons from Russia

(#Afghanistan #Houthis #Iran #Russia #Türkiye #DigitalAssets #UAV)

In April 2025, OFAC sanctioned a network of Houthi financial facilitators and procurement operatives working under a senior Houthi financial official backed by Iran's Islamic Revolutionary Guard Corps-Qods Force (IRGC-QF). This network orchestrated sophisticated procurement schemes that secured tens of millions of dollars' worth of commodities from Russia, including weapons and sensitive goods.

The financial infrastructure supporting these illicit activities relied heavily on money laundering operations to circumvent international sanctions and facilitate payments. A Türkiye-based Iranian money launderer played a crucial role in this financial web, working directly with two Russia-based Afghan businessmen to launder dollars on behalf of the network and enable their sanctions evasion schemes. The network arranged payments worth millions of dollars to support shipments benefiting the Houthis, while OFAC also identified eight digital asset wallets used by the Houthis to transfer funds associated with their activities. This multifaceted approach to financial facilitation—combining traditional money laundering with digital assets and complex international transactions—enabled the network to procure critical goods. The Houthis have deployed missiles, UAVs, and naval mines to attack commercial shipping interests in the Red Sea, as well as enabled the Iranian regime in its continued quest for nuclear acquisition.[119]

TCO Attempted to Traffic Nuclear Materials

(#Afghanistan #Iran #Japan #Myanmar #Yakuza #Intermediaries #Narcotics #Uranium)

In January 2025, a Japanese Yakuza leader pleaded guilty to conspiring to traffic nuclear materials, including uranium and weapons-grade plutonium, from Myanmar to other countries, as well as to international narcotics

117 Treasury, "Treasury Targets Entities Procuring Sensitive Machinery for Iran's Defense Industry," (June 2025), https://home.treasury.gov/news/press-releases/sb0175.

118 DOJ, "Spanish National Pleads Guilty to Conspiring to Export U.S. Military-Grade Radios to Russian Government End Users," (June 2025), https://www.justice.gov/opa/pr/spanish-national-pleads-guilty-conspiring-export-us-military-grade-radios-russian-government.

119 See Footnote 69.

trafficking and weapons charges.[120]

During this conspiracy, the individual and his co-conspirators showed samples of nuclear materials in Thailand to a Drug Enforcement Administration (DEA) undercover agent ("UC-1") who was posing as a narcotics and weapons trafficker. With the assistance of Thai authorities, the nuclear samples were seized and subsequently transferred to the custody of U.S. law enforcement. A U.S. nuclear forensic laboratory later analyzed the samples and confirmed that they contained uranium and weapons-grade plutonium. The defendant and his co-defendant were previously charged in April 2022 with international narcotics trafficking and firearms offenses, and both were ordered to be detained.

According to court documents, beginning in early 2020, the defendant informed UC-1 and a DEA confidential source ("CS-1") that the defendant had access to a large quantity of nuclear materials that he wanted to sell.[121] In response to the defendant's repeated inquiries, UC-1 agreed, as part of the DEA's investigation, to help the defendant broker the sale of his nuclear materials to UC-1's associate, who was posing as an Iranian general (the "General"), for use in a nuclear weapons program.

During their discussions regarding the defendant's access to nuclear materials, the defendant also engaged with UC-1 concerning his desire to purchase military-grade weapons. To that end, in May 2021, the defendant sent UC-1 a list of weapons, including surface-to-air missiles, that he wished to purchase from UC-1 on behalf of the leader of an ethnic insurgent group in Myanmar ("CC-1"). Together with two other co-conspirators ("CC-2" and "CC-3"), the defendant proposed to UC-1 that CC-1 sell uranium to the General, through the defendant, to fund CC-1's weapons purchase.

Finally, the defendant conspired to broker the purchase, from UC-1, of U.S.-made surface-to-air missiles, as well as other heavy-duty weaponry, and to accept large quantities of heroin and methamphetamine for distribution as partial payment for the weapons. The defendant understood the weapons to have been manufactured in the U.S. and taken from U.S. military bases in Afghanistan. He planned for the heroin and methamphetamine to be distributed in the New York market. In addition, the defendant conspired to sell, in a separate transaction, 500 kilograms of methamphetamine and 500 kilograms of heroin to UC-1 for distribution in New York. In furtherance of that transaction, on or about June 16, 2021, and on or about September 27, 2021, one of the co-defendants provided samples of approximately one kilogram of methamphetamine and approximately 1.4 kilograms of heroin. The defendant also worked to launder $100,000 in purported narcotics proceeds from the United States to Japan.

Exploiting Front and Shell Companies

OFAC Sanctions DPRK Bankers and Institutions Involved in Laundering Cybercrime Proceeds and IT Worker Funds

(#DPRK #Russia #China #Banks #FrontCompanies)

In November 2025, OFAC designated eight individuals and two entities for their role in laundering funds derived from a variety of illicit DPRK schemes, including cybercrime and IT worker fraud. These targets were part of a vast network comprised of banking representatives, financial institutions, and front and shell companies located in the DPRK and internationally, including in China and Russia. For example, Ri Jin Hyok is a representative of UN- and OFAC-designated FTB and has facilitated transactions on behalf of an FTB front company worth over $350,000 in USD, CNY, and Euros. The DPRK relies on Ri and many other representatives to provide access to international markets and financial systems to launder funds from revenue generation schemes.[122]

120 DOJ, "Japanese Yakuza Leader Pleads Guilty To Nuclear Materials Trafficking, Narcotics, And Weapons Charges," (January 2025), https://www.justice.gov/usao-sdny/pr/japanese-yakuza-leader-pleads-guilty-nuclear-materials-trafficking-narcotics-and.

121 Later that year, the defendant sent UC-1 a series of photographs depicting rocky substances with Geiger counters measuring radiation, as well as pages of what the defendant represented to be lab analyses indicating the presence of thorium and uranium in the depicted substances.

122 Treasury, "Treasury Sanctions DPRK Bankers and Institutions Involved in Laundering Cybercrime Proceeds and IT Worker Funds," (November 2025), https://home.treasury.gov/news/press-releases/sb0302.

Dual U.S.-Russian National Sentenced for Export Control and Sanctions Evasion Scheme

(#Russia #Estonia #AdvancedTech #Banks #ShellCompanies)

In August 2025, a New Jersey resident and dual U.S. and Russian national, Vadim Yermolenko, was sentenced to 30 months in prison for his role in a transnational arms dealing and money laundering network that sought to acquire ammunition and sensitive dual-use electronics for Russian military and intelligence services.[123]

As alleged in court documents, the defendant was affiliated with Serniya Engineering (Serniya) and Sertal LLC (Sertal), two Moscow-based procurement companies. Serniya and Sertal operated a vast network of shell companies and bank accounts throughout the world, including in the United States, that were used in furtherance of the scheme to conceal the involvement of the Russian government and the true Russian end users of U.S.-origin equipment.

The defendant and his co-conspirators unlawfully purchased and exported highly sensitive, export-controlled electronic components, some of which can be used in the development of nuclear and hypersonic weapons, quantum computing, and other military applications. Serniya, Sertal, and several individuals and companies involved in the scheme were designated by the OFAC in March 2022.[124]

To carry out the scheme, Yermolenko helped set up numerous shell companies and bank accounts in the U.S. to illicitly move money and export-controlled goods. During the period charged in the indictment, more than $12 million passed through accounts owned or controlled by the defendant, which he failed to report to the IRS. These funds were used in part to purchase sensitive equipment used in radar, surveillance, and military research and development. In one instance, money from one of the defendant's accounts was used to purchase export-controlled sniper bullets, which were intercepted in Estonia before they could be smuggled into Russia.

Iranian Network Designated for Using Shadow Banking Scheme to Fund WMD Activities

(#Iran #FrontCompanies #Intermediaries #ShadowBanking)

In June 2025, OFAC designated over 30 individuals and entities tied to three Iranian nationals who collectively laundered billions of dollars through the international financial system via Iranian exchange houses and foreign front companies under their control as part of Iran's "shadow banking" network. The government of Iran 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.[125]

As part of this shadow banking scheme, one Iran-based exchange house has assisted IRGC-QF in receiving funds from the U.S.-sanctioned Astan Quds Foundation via money transfers through China and has also assisted Astan Quds Foundation and the IRGC-QF in collecting approximately $100 million through currency exchanges. Another Iran-based exchange house also facilitated transactions on behalf of Iran's MODAFL, while a third exchange house in the network has transferred foreign currency on behalf of MODAFL, in addition to transferring funds related to Iranian petrochemical sales and procurement activities.

123 DOJ, "New Jersey Resident Sentenced for Role in Global Export Control and Sanctions Evasion Scheme," (August 2025), https://www.justice.gov/opa/pr/new-jersey-resident-sentenced-role-global-export-control-and-sanctions-evasion-scheme.

124 Treasury, "Treasury Targets Sanctions Evasion Networks and Russian Technology Companies Enabling Putin's War," (March 2022), https://home.treasury.gov/news/press-releases/jy0692.

125 Treasury, "Treasury Sanctions Iranian Network Laundering Billions for Regime Through Shadow Banking Scheme," (June 2025), https://home.treasury.gov/news/press-releases/sb0159.

Iranian Network Indicted and Sanctioned for Illicit Procurement Scheme Related to UAVs

(#Iran #China #UAE #CorrespondentBanks #FrontCompanies #ShellCompanies #UAV)

In April 2025, the DOJ coordinated concurrent actions with the rest of the U.S. interagency related to a scheme to procure U.S. technology for UAVs. A criminal complaint was unsealed, charging two Iranian individuals and one Iranian company with conspiring to procure U.S. parts for Iranian UAVs, conspiring to provide material support to the IRGC, a U.S.-designated FTO, and conspiring to commit money laundering. Concurrently, OFAC targeted a network of six entities and two individuals based in Iran, the UAE, and China responsible for the procurement of UAV components on behalf of Qods Aviation Industries (QAI)—a leading manufacturer for Iran's UAV program.[126,127]

To facilitate their scheme, the defendants falsely purported to represent other companies, including a company based in the UAE and a company based in Belgium. The defendants used a "spoofed" email address, containing a misspelled version of the UAE-based company's name, to communicate regarding the procurement of parts, including parts manufactured by U.S. companies. The defendants also used various front or shell companies to pay for UAV parts and to obfuscate the true end destination and the true identities of the sanctioned end users, including U.S.-designated entities. The defendants also used aliases to obfuscate their true identities in furtherance of the scheme.

The indicted individuals also conspired to commit money laundering. They used at least three shell companies, which were all based in the UAE, to pay a China-based company that sent invoices to an Iran-based company for the sale of motors. Those payments were processed through U.S.-based correspondent bank accounts. The defendants also used two of these shell companies to pay a separate China-based company for the sale of pneumatic masts, which are a component of the operation of the Mohajer-6 drone.

Two Indicted for Illicit Procurement Scheme Related to Iranian UAVs

(#Iran #Switzerland #DigitalAssets #FrontCompanies #Intermediaries #UAV)

In December 2024, a Massachusetts-based individual and a Tehran-based individual were indicted for illegally exporting sophisticated electronic components from the United States to Iran through an elaborate front company scheme. The operation ultimately contributed to a deadly drone attack on U.S. service members.

The defendants, a dual U.S.-Iranian national working for American microelectronics companies and an Iranian company director, conspired to evade U.S. export control and sanctions laws by establishing a Swiss front company. The Swiss company contracted with U.S. manufacturers to develop and procure advanced semiconductors and navigation components for use in missiles and drones. The Iranian defendant's company manufactured navigation systems used in military drones for the IRGC. To circumvent export restrictions, they created the Swiss entity to serve as an intermediary for obtaining U.S.-origin technology that was then transferred to Iran for military applications.

The scheme involved the American co-conspirator leveraging his position within U.S. companies and his connections to Iranian funding sources to facilitate the illegal procurement, with the front company serving as the crucial mechanism to disguise the true Iranian end-users and evade detection by U.S. authorities. The navigation systems obtained through this deceptive operation were subsequently used in IRGC attack drones, including one that killed three U.S. service members in a January 2024 attack.[128]

126 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," (April 2025), https://www.justice.gov/opa/pr/iranian-company-and-two-iranian-nationals-charged-conspiring-provide-material-support.

127 Treasury, "The Departments of Treasury and Justice Take Action Against Iranian Weapons Procurement Network," (April 2025), https://home.treasury.gov/news/press-releases/sb0066.

128 DOJ, "Iranian Man Indicted for Providing Material Support to Foreign Terrorist Organization Resulting in Death, and for Scheme To Procure Sensitive U.S. Technology Used in Military Drones," (December 2024), https://www.justice.gov/usao-ma/pr/iranian-man-indicted-providing-material-support-foreign-terrorist-organization-resulting.

In September 2025, the DOJ filed a civil forfeiture action to recover approximately $584,741 in digital assets alleged to be the property of the Iran-based individual and/or his company. Previously, the U.S. government seized stablecoins from an un-hosted digital asset wallet alleged to be controlled by the individual.[129]

Front Companies Facilitate Tobacco Smuggling to the DPRK

(#Australia #China #DPRK #FrontCompanies #Tobacco)

In September 2024, three Chinese nationals and an OFAC-designated DPRK banker were all charged in connection with a multi-year scheme to facilitate the sale of tobacco to the DPRK through the U.S. financial system. One of the Chinese nationals was extradited from Australia to face charges in the United States. Between 2009 and 2019, the defendants engaged in a scheme to purchase leaf tobacco for North Korean-owned entities and used front companies and false documentation to cause U.S. financial institutions to process at least 310 transactions worth approximately $74 million. The transactions resulted in an estimated nearly $700 million in revenue for DPRK entities, and ultimately, for the government.

This case is part of a larger DOJ response to the ongoing efforts of the DPRK to evade sanctions and use the U.S. financial system to engage in illicit trafficking of tobacco products. As alleged in the indictment, the DPRK exploits the U.S. financial system through elaborate deception schemes involving front companies and falsified documentation to conduct illicit tobacco trafficking, which serves as a major revenue source for weapons development programs. Smuggled tobacco is estimated to generate revenue of as much as $20 on every $1 spent in cost.[130]

Front Companies Used in Multi-Jurisdiction Sanctions Evasion Scheme

(#China #DPRK #Russia #UAE #FrontCompanies #ITWorkers)

In March 2024, OFAC, in coordination with the Republic of Korea (ROK), designated six individuals and two entities based in Russia, China, and the United Arab Emirates for generating revenue and facilitating financial transactions that ultimately supported North Korea's WMD. The action targeted agents of designated North Korean banks and companies that employ North Korean IT workers abroad, as these actors generate revenue and provide access to foreign currencies essential to the North Korean government. These individuals and entities, operating primarily through networks in Russia and China, orchestrate schemes by establishing front companies and managing covert bank accounts to move illicit funds and evade sanctions.[131]

129 DOJ, "United States Seeks Civil Forfeiture of Cryptocurrency Associated with Iranian National Mohammad Abedini," (September 2025), https://www.justice.gov/usao-ma/pr/united-states-seeks-civil-forfeiture-cryptocurrency-associated-iranian-national-mohammad.

130 DOJ, "Chinese National and DPRK Facilitator Extradited to the United States; Faces Charges of Conspiracy, Bank Fraud, and Violating North Korea Sanctions," (September 2024), https://www.justice.gov/archives/opa/pr/chinese-national-and-dprk-facilitator-extradited-united-states-faces-charges-conspiracy-bank.

131 Treasury, "Treasury Sanctions Actors Financing the North Korean Weapons of Mass Destruction Program," (March 2024), https://home.treasury.gov/news/press-releases/jy2215.

METHODOLOGY AND TERMINOLOGY

The methodology and terminology of the 2026 NPFRA are informed by guidance of the FATF, which is the international standard-setting body for AML/CFT/CPF safeguards.[132] This guidance lays out a process for conducting a PF risk assessment at the national level.[133] The underlying concepts for this risk assessment are threats, vulnerabilities, consequences, and risk. This approach uses the following key concepts:

- *Threat*: A threat refers to individuals or entities, or activity undertaken by those individuals and entities, with the potential to cause harm. The threats, which may include nation-state authorities, those acting under their control or on their behalf, or those wittingly or unwittingly supporting either, are the ones who exploit the U.S. financial system to move funds, assets, or other economic resources that could be used to: (1) directly acquire WMDs, their delivery systems, or the goods, technology, or expertise to allow them to build WMDs or their delivery systems, or (2) support a WMD program through a variety of revenue-raising activities.
- *Vulnerability*: To acquire or expand their WMD capabilities, a threat actor must exploit aspects of a jurisdiction or a private sector entity to obtain components or financial services it would otherwise be prohibited from acquiring. These vulnerabilities may arise from weaknesses or loopholes in national laws or regulations, effectiveness issues impeding the ability of national authorities to properly investigate or disrupt proliferation networks, or unique circumstances that make a particular jurisdiction especially vulnerable to this kind of activity.
- *Consequence*: A consequence derives directly from a threat capitalizing on a vulnerability. In the context of PF, the consequence would be funds, assets, or other economic resources being made available to a proliferation network such that it can be used to acquire or augment a specific WMD capability.
- *Risk*: The risk is a function of threat, vulnerability, and consequence. It represents a summary judgment, considering the impact of mitigating measures, including regulation, supervision, and enforcement.

132 In line with the prior assessments, the NPFRA is based on a review of public and private sector publications, international organizations, think tanks, media reporting, government datasets, and analyses. Data collected is current as of January 31, 2026. With respect to information collected from pending law enforcement cases, the charges in an indictment or similar charging documents are merely allegations. A defendant is presumed innocent until proven guilty beyond a reasonable doubt in a court of law. A seizure warrant is based on allegations. The government bears the burden of proving forfeitability in a civil forfeiture proceeding.

133 The United States takes a broader view of PF risk than what the FATF Standards require and what the 2021 FATF PF Guidance conveys. That guidance restricts a consideration of threat, vulnerability, and consequence in the context of UN-targeted financial sanctions. The United States has a view of PF risk that includes both United Nations targeted financial sanctions and sectoral sanctions, as well as sanctions imposed under U.S. law, and restrictions imposed through U.S. export control authorities. See FATF, "Guidance on Proliferation Financing Risk Assessment and Mitigation," (June 2021), p.7, paragraph 11, https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Guidance-Proliferation-Financing-Risk-Assessment-Mitigation.pdf.coredownload.inline.pdf.

LIST OF ACRONYMS

DNI	Director of National Intelligence
DPRK	Democratic People's Republic of Korea
FATF	Financial Action Task Force
IAEA	International Atomic Energy Agency
ICBM	Intercontinental Ballistic Missile
IEEPA	International Emergency Economic Powers Act
IRGC	Islamic Revolutionary Guard Corps
IT	Information Technology
OFAC	Office of Foreign Assets Control
PF	Proliferation Finance
TCO	Transnational Criminal Organization
TFS	Targeted Financial Sanctions
UAE	United Arab Emirates
UAVs	Unmanned Aerial Vehicles
UNSCR	United Nations Security Council Resolution
DASPs	Digital Asset Service Providers
WMD	Weapons of Mass Destruction

INTERAGENCY PARTICIPANTS

In drafting this risk assessment, the Department of the Treasury's Office of Terrorist Financing and Financial Crimes consulted with staff from the following U.S. government agencies, who also reviewed this report:

- **Department of Commerce**
  - Bureau of Industry and Security
- **Department of Homeland Security**
  - Homeland Security Investigations
- **Department of Justice**
  - Criminal Division
  - Federal Bureau of Investigation
  - National Security Division
- **Department of State**
  - Bureau of Economic and Business Affairs
  - Bureau of Arms Control and Nonproliferation
  - Bureau of International Organization Affairs
- **Department of the Treasury**
  - Financial Crimes Enforcement Network
  - Office of Foreign Assets Control
  - Office of Intelligence and Analysis
  - Office of Terrorist Financing and Financial Crimes
- **Staff of the Federal Functional Regulators**[134]

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

ANNEX 1: SNAPBACK OF UN SANCTIONS AGAINST IRAN

In October 2025, the FATF confirmed that Recommendation 7 once again applies to Iran, following the re-application of key UN Security Council resolutions related to proliferation financing.[135] Pursuant to the process set forth in paragraphs 11 and 12 of UN Security Council Resolution 2231 (2015), **as of 8:00 pm EDT on 27 September 2025**, all of the provisions of resolutions 1696 (2006), 1737 (2006), 1747 (2007), 1803 (2008), 1835 (2008), and 1929 (2010) related to Iran have been re-applied in the same manner as they applied before the adoption of resolution 2231 (2015).[136]

Member states are required to implement UN sanctions under their domestic sanctions regimes to comply with their UN obligations, which include asset freezes on individuals and entities involved in Iranian nuclear and missile activities. In addition, member states are also called upon to exercise vigilance over Iranian banks in their jurisdictions and to prohibit the opening of new Iranian bank offices.

Impact on the FATF Process

- Minor reference updates have been made to the FATF Standards and Methodology.
- Under Recommendation 7 and Immediate Outcome 11, jurisdictions are being assessed for the implementation of Iran-related UN TFS as part of FATF mutual evaluations.
- Under Recommendation 1, the public and private sectors are being assessed for how they identify, assess, and mitigate PF risks, which link to threat actors like the DPRK and Iran.

Practical Implications for the Private Sector- Potential Actions:

- Identify which reimposed measures from pre-JCPOA resolutions may impact your business.
- Update your enterprise-wide approach to Iran through PF risk assessments, policies, controls, and procedures.
- Review risk-based measures for products, customers, transactions, sectors, and jurisdictions to ensure they are adequate to address PF risk linked to Iran-related UN sanctions.
- Assess the degree to which correspondent banking relationships are exposed, especially in high-risk jurisdictions, to new PF risks after the reimposition of Iran-related UN sanctions, and take appropriate measures to reevaluate and oversee these relationships.
- Be ready to describe how your PF-TFS framework addresses the new risk environment.
- Prepare for Iran to accelerate its use of front companies and financial intermediaries to evade international, supranational, and national sanctions regimes.
- Engage with public and private sector counterparts to exchange information and good practices in response to the evolving PF and sanctions evasion threat landscape.

135 FATF, "Update: Re-application of UN Security Council Resolutions related to Iran," (October 2025), https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Fatfgeneral/Update--Re-application-of-UN-Security-Council-Resolutions-related-to-Iran.html.

136 On August 28, 2025, France, Germany, and the United Kingdom (collectively known as the "E3") initiated the Iran "snapback" process under UN Security Council Resolution 2231, asserting that Iran had significantly violated its Joint Comprehensive Plan of Action (JCPOA) commitments.

ANNEX 2: ADDITIONAL READING ON PROLIFERATION FINANCING

In June 2025, the FATF published a report on Complex PF and Sanctions Evasion Schemes.[137] The project, which was co-led by Japan and the United States, was developed by an international team of more than 20 jurisdictions and four international organizations. This is the first FATF typologies report on PF in 17 years. It is designed to inform how the public and private sectors identify and mitigate relevant PF risks, which will be assessed under the revised Recommendation 1 in the fifth round of FATF mutual evaluations.

The FATF report's main takeaways include:

- Based on submissions across the FATF Global Network and input from the private sector, the **main PF threat actors** are the DPRK, Iran, and Russia.[138]
- Illicit actors are implementing sophisticated PF-related schemes that the report categorizes under **four typologies**: (1) enlisting intermediaries; (2) obscuring beneficial ownership information to access the financial system; (3) using virtual assets and other technologies; and (4) exploiting the maritime and shipping sectors.
- To address PF and sanctions evasion schemes, the report highlights **challenges and good practices** related to detecting PF and sanctions evasion, investigation and prosecution, domestic coordination and collaboration, and international cooperation.
- To conclude, the report provides **four recommendations** for the FATF Global Network:

  1. Update the understanding of PF risk and typologies on a periodic basis;
  2. Encourage more substantive information sharing to strengthen the public and private sectors' ability to detect PF and/or sanctions evasion;
  3. Add a definition of WMD PF to the FATF General Glossary within five years; and
  4. Conduct a horizontal review of PF risk assessments within three years.

In addition to the FATF report, the Department of the Treasury encourages a review of other relevant documents.[139]

137 FATF, "Complex Proliferation Financing and Sanctions Evasion Schemes," (June 2025), https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Complex-PF-Sanctions-Evasions-Schemes.pdf.coredownload.inline.pdf.

138 The report's broader framing of sanctions evasion does not create any new obligations related to Recommendation 1 or any other part of the FATF Standards. Instead, FATF typologies reports aim to support the public and private sectors to assess and mitigate risk based on their unique context.

139 See, e.g., Department of Finance Canada, "G7 Finance Ministers and Central Bank Governors' Communiqué," (May 2025), https://www.canada.ca/en/department-finance/news/2025/05/g7-finance-ministers-and-central-bank-governors-communique.html; State, "Joint Statement of the MSMT on the First Report Covering DPRK-Russia Military Cooperation," (May 2025), https://www.state.gov/joint-statement-of-the-multilateral-sanctions-monitoring-team-msmt-on-the-first-report-covering-dprk-russia-military-cooperation; and MSMT, "The DPRK's Violation and Evasion of UN Sanctions through Cyber and Information Technology Worker Activities," (October 2025), https://www.mofa.go.jp/files/100922718.pdf.


THE DEPARTMENT OF THE TREASURY
1789