<Provisional Translation>

NATIONAL PROLIFERATION FINANCING RISK ASSESSMENT 2025

Inter-Ministerial Council for Anti-Money Laundering (AML),
Countering the Financing of Terrorism (CFT),
and Countering Proliferation Financing (CPF) Policy

Contents

Acronyms

The meanings of the acronyms used in this report are as follows:

FATF	Financial Action Task Force
ICBM	Intercontinental Ballistic Missile
IAEA	International Atomic Energy Agency
DoS	Denial of Service attack
DDoS	Distributed Denial of Service attack
FSB	Financial Stability Board
G-SIBs	Global Systemically Important Banks
DeFi	Decentralized Finance
DNFBPs	Designated Non-Financial Businesses and Professions
BO	Beneficial Owner

Overview

The overview of this report is as follows.

Chapter 1. Proliferation Financing (PF)

1. Definition of and Background to PF

(1) Definition of PF and FATF Recommendations

PF refers to the act of providing funds or financial services to persons or entities that are subject to asset freezing or other measures for their involvement in the development, possession, or export of weapons of mass destruction (WMD), including nuclear, chemical, and biological weapons.[1]

International standards for counter-PF have been developed and published by the FATF[2] since 2012, including Recommendation 7 (Targeted financial sanctions related to proliferation[3]). Under these standards, countries are required to implement targeted financial sanctions, such as asset freezing measures, in order to comply with the relevant UNSCRs aimed at preventing, suppressing, and disrupting the proliferation of WMD and its financing.

Nevertheless, despite the international community, including Japan, cooperating within this framework and implementing economic sanctions against North Korea and Iran, transfers of WMD, related materials, and technologies to these countries/regions of concern have continued to occur. Against this backdrop, in October 2020, the FATF revised Recommendation 1 (Assessing risks and applying a risk-based approach) and its Interpretative Note. Through this revision, the FATF required countries, in addition to existing AML and CFT measures, to identify, assess, and understand the "PF risk," defined as "the potential breach, non-implementation, or evasion of the targeted financial sanctions obligations referred to in Recommendation 7." Countries are also required to take actions to mitigate both higher and lower risks in order to ensure the effective implementation of targeted financial sanctions related to PF.

The revised Recommendation 1 and its Interpretative Note have been applied to FATF assessments

---

[1] Ministry of Finance (MOF), *About AML/CFT/CPF,* https://www.mof.go.jp/english/policy/international_policy/amlcftcpf/2.measures.html

[2] In response to the Economic Declaration that was issued at the Summit of the Arch in 1989, the FATF was established as a multilateral framework responsible for formulating and enforcing international standards related to AML measures. Following the simultaneous, multiple terrorist attacks in the United States in 2001, CFT was added to the scope of its missions. The FATF's members comprise 38 countries and regions and two regional organizations. Decisions on matters relating to the FATF's activities are made at FATF plenary meetings, which are held three times a year.

[3] Recommendation 7 requires countries to implement targeted financial sanctions to comply with the United Nations Security Council resolutions (UNSCR) related to the prevention, suppression and disruption of proliferation of WMD and the financing of WMD. Specifically, countries are required to freeze, without delay, the funds or other assets of any person or entity designated by the United Nations Security Council (UNSC) under Chapter VII of the Charter of the United Nations (UN), and to ensure that no funds and other assets are made available to them or available for their benefit.

conducted under the Fifth Round Mutual Evaluations, which have been progressively implemented since 2024.

In Japan, following the publication of the Fourth Round Mutual Evaluation Report of Japan in August 2021, the Inter-Ministerial Council for AML, CFT, and CPF Policy (hereinafter referred to as the "Policy Council"), co-chaired by the National Police Agency (NPA) and the MOF, was established in the same month to promote AML/CFT/CPF measures on a government-wide basis.[4] In May 2022, the Policy Council adopted the Strategic Policy on the Promotion of AML/CFT/CPF Measures (hereinafter referred to as the "Strategic Policy"), [5] which identified the following four pillars:

(i) Full implementation of a risk-based approach
(ii) Swift responses to new technologies
(iii) Strengthening international cooperation and coordination
(iv) Enhancing inter-agency coordination and public-private partnerships

As one of the specific measures under the Strategic Policy, the Government stated that "it would conduct a PF risk assessment in parallel with AML/CTF risk assessment, with the aim of enhancing the effectiveness of asset freezing measures."

In addition, the Foreign Exchange and Foreign Trade Act (Act No. 228 of 1949; hereinafter referred to as "FEFTA") was amended to require banks, etc., funds transfer service providers, electronic payment instruments service providers, etc.,[6] and currency exchange operators to conduct self-risk assessment regarding asset freezing measures, with reference to this National Risk Assessment of PF in Japan (hereinafter referred to as the "National Risk Assessment") and to guidelines and other regulatory documents formulated by the relevant authorities.[7]

(2) Background

Due to the globalization of economic and financial services and technological innovation, such as the diffusion of crypto assets, fund flows have become more diverse, making cross-border transactions easier. Under these circumstances, facilitating the proliferation of WMD through PF poses a major

[4] MOF, *Policy Council*, https://www.mof.go.jp/policy/international_policy/councils/aml_cft_policy/index.html
[5] MOF, *Strategic Policy, May 19,2022*, https://www.mof.go.jp/policy/international_policy/councils/aml_cft_policy/20220519.html
[6] "Electronic payment instruments service providers, etc." include electronic payment instruments service providers, electronic payment handling service providers, etc., and crypto asset exchange service providers.
[7] "Foreign exchange transaction service providers" as defined under Article 55-9-2, paragraph (1) of the amended FEFTA (which came into force on June 1, 2025), are required to assess the risk of breaches of sanctions based on Article 1, item (i) of the Ministerial Order Prescribing the Standards for Compliance on Foreign Exchange Transaction Service Providers (Order of the MOF and the METI No. 1 of 2023). In the assessment of the risk, the National Risk Assessment also needs to be taken into consideration.

threat to Japan and the international community.

Moreover, Japan, as the only country to have ever suffered atomic bombings during wartime, has played a leading role in international discussions on nuclear disarmament and non-proliferation, with the aim of realizing a world without nuclear weapons. Japan has also called on all countries possessing nuclear weapons to take nuclear disarmament measures while enhancing the transparency of armaments.

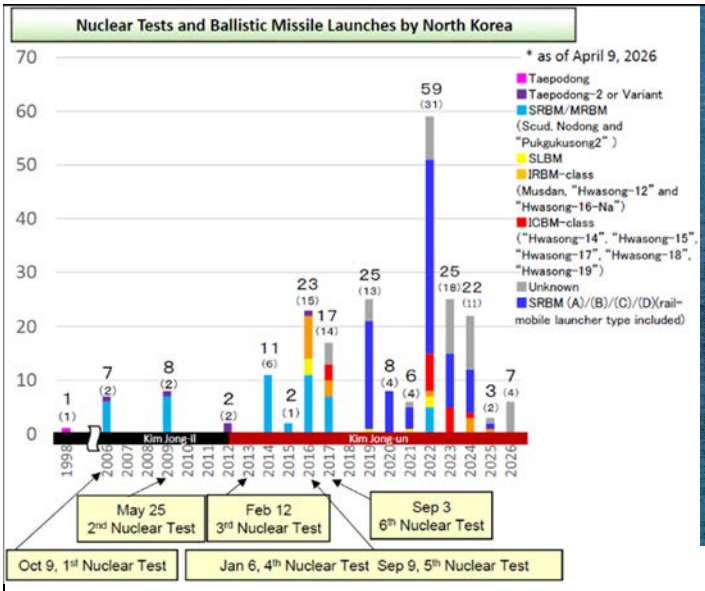
However, unfortunately, even today, some countries/regions still have not stopped the development of nuclear weapons. G7 leaders' Communiqués and other related documents have repeatedly sent strong messages against the development of nuclear weapons by North Korea and Iran, but both continue their nuclear-related activities.[8]

(i) North Korea
North Korea has been concentrating its efforts on strengthening WMD and ballistic missiles in order to maintain its regime. In particular, with regard to ballistic missiles, North Korea has been rapidly enhancing related technologies and operational capabilities, such as by diversifying launch modes. In September 2023, North Korea added a provision to its Constitution stating that it would "develop nuclear weapons to a higher level[9]" and launched ballistic missiles and other projectiles 18 times in 2023, 11 times in 2024, and 4 times in 2025. According to a report by the United States Defense Intelligence Agency[10], North Korea has exported ballistic missiles and other weapons over several decades. In the context of advancing military cooperation between Russia and North Korea, it has been reported that North Korea exported artillery shells and ballistic missiles to Russia, and that Russian forces have used North Korean-made missiles in Ukraine.

[8] A chair's summary issued at the G7 Summit (Canada) held in June 2025 stated as follows: "They expressed concern about DPRK's nuclear weapons and ballistic missile programs and the need to jointly address DPRK cryptocurrency thefts fueling these programs." Ministry of Foreign Affairs (MOFA), *CHAIR'S SUMMARY*, June 17, 2025, https://www.mofa.go.jp/mofaj/files/100864611.pdf

[9] Ministry of Defense/Self-Defense Forces (MOD/SDF), *Defense of Japan*, https://www.mod.go.jp/en/publ/w_paper/index.html

[10] Defense Intelligence Agency (DIA), *North Korean Military Power: A Growing Regional and Global Threat*, 2021, p67; and *North Korea: Enabling Missile Strikes Against Ukraine*, 2024, pp.3-5, https://www.dia.mil/Military-Power-Publications/



(Source) MOD

(Source) MOD

Furthermore, the first report of the Multilateral Sanctions Monitoring Team[11] [12] (MSMT) reported that North Korea provided Russia with at least 100 ballistic missiles and components for three brigades of heavy artillery; that since November 2024 Russia has provided North Korea with short-range air defense systems, advanced electronic warfare systems including jamming equipment, and related operational know-how; and that North Korea deployed more than 11,000 soldiers to Russia in late 2024, where they received training from Russian forces in artillery, unmanned aerial vehicles, and basic infantry operations.

(ii) Iran

After the agreement between EU3+3 (China, France, Germany, Russia, the United Kingdom, and the United States) and Iran on the Joint Comprehensive Plan of Action (JCPOA) regarding the Iranian nuclear development issue on July 14, 2015, the UNSC adopted UNSCR 2231 on July 20, 2015. This resolution called for the phased lifting of the licensing system for transactions related to large conventional weapons five years after the "Adoption Day" (October 18, 2015), which falls 90 days after the adoption of the JCPOA; those related to nuclear weapons delivery systems eight years after the Adoption Day; and those related to nuclear development 10 years after the Adoption Day.

[11] In response to the termination of the activities of the UNSC North Korea Sanctions Committee Panel of Experts in April 2024 due to Russia's veto at the Security Council, Japan, the United States, the Republic of Korea (ROK), and other like-minded countries (Australia, Canada, France, Germany, Italy, the Netherlands, New Zealand, and the United Kingdom) established the MSMT to share information on violations and evasion of sanctions under the relevant UNSCRs among participating countries and disseminate such information to the international community for the purpose of contributing to the full implementation of the relevant UNSCRs.

[12] MSMT, *Unlawful Military Cooperation including Arms Transfers between North Korea and Russia (MSMT/2025/1)*, May 29, 2025, https://msmt.info/Publications/detail/MSMT%20Report/4195

In accordance with the resolution, a prohibition on transactions related to conventional weapons was lifted in October 2020 and one on transactions related to ballistic missiles (nuclear weapons delivery systems, etc.) in October 2023. Although the licensing system for transactions related to nuclear development and all other sanctions under the resolution were scheduled to end in October 2025, which marks the 10th anniversary of the JCPOA adoption, the E3 (the United Kingdom, France, and Germany) notified the UNSC President on August 28, 2025 of Iran's serious non-compliance with its JCPOA commitments, leading the UNSC to reject a resolution for continuing the termination of sanctions against Iran on September 19. As a result, sanctions against Iran under past UNSCRs (UNSCRs 1737, 1747, 1803, 1929, etc.), as stipulated in operative paragraph 12 of UNSCR 2231, were reapplied on September 28.

With regard to the manufacture and use of nuclear weapons, Iran's Supreme Leader Khamenei is reported to have prohibited even their manufacture through a fatwa (religious decree). On the other hand, Iran has expanded its nuclear-related activities in recent years and Japan has expressed concern over this trend while calling on Iran to take a constructive response, including the resumption of full cooperation with the IAEA.[13]

(iii) Russia

In June 2024, Russia signed the Comprehensive Strategic Partnership Treaty with North Korea (hereinafter referred to as the "Russia-North Korea Partnership Treaty"), and the treaty entered into force in December. The treaty stipulates the establishment of favorable conditions for economic cooperation, including in the financial and other fields, in order to encourage and protect investment by both parties.

In response, 10 major countries issued their foreign ministers' joint statement in December 2024[14], which condemned in the strongest possible terms the expanding military cooperation between North Korea and Russia, including the deployment of North Korean troops to Russia for use on the battlefield in Ukraine, and encouraged the broader international community to join their call and continue to act in concert, including through imposition of economic sanctions, to respond to the dangers posed by the North Korea-Russia partnership. Japan, which has imposed economic

[13] According to information available prior to Israel's attack on Iran's nuclear facilities, the IAEA stated that, as of June 13, 2025, Iran possessed approximately 440 kilograms of uranium enriched up to 60 percent. International Atomic Energy Agency, *NPT Safeguards Agreement with the Islamic Republic of Iran*, GOV/2025/65, November 12, 2025, https://www.iaea.org/sites/default/files/gov2025-65.pdf

[14] A joint statement was issued by the foreign ministers of Japan, Australia, Canada, France, Germany, Italy, the ROK, New Zealand, the United Kingdom, and the United States, together with the High Representative of the European Union for Foreign Affairs and Security Policy. MOFA, *Joint Statement by the Foreign Ministers Condemning Russia–North Korea Cooperation*, December 16, 2024, https://www.mofa.go.jp/press/release/pressite_000001_00854.html

sanctions on Russia along with the United States and the European Union, is required to ensure the effectiveness of measures taken by law-enforcement authorities in consideration of cooperation between Russia and North Korea, as well as specific cases and methods of violations and evasion of sanctions across various fields.

(3) Purpose of the National Risk Assessment

The National Risk Assessment analyzes and assesses PF risks in Japan, serving as a prerequisite for private business operators' effective and efficient counter-PF measures based on a risk-based approach. As the FATF calls on financial institutions and DNFBPs[15] to identify, assess, and understand PF risks and respond to these risks (risk-based approach), these business operators are required to take into account the National Risk Assessment and reports published by international organizations described later, and to take appropriate risk mitigation measures in order to effectively prevent PF funds or financial services from being provided. Other private business operators are also expected to take similar measures.

2. Risk Assessment Approach

(1) FATF Guidance

In preparing the National Risk Assessment, we referred to "Guidance on Proliferation Financing Risk Assessment and Mitigation" (hereinafter the "FATF PF Guidance")[16], published by the FATF. While the Guidance states that there is not a one-size-fits-all approach to PF risk assessment that should be used by all countries and that countries should conduct assessment flexibly in accordance with their respective circumstances, it sets out the following concepts as ones on which there should be a common understanding.

[15] DNFBPs stands for Designated Non-Financial Businesses and Professions. In Japan, DNFBPs refer to business operators such as real estate brokers, dealers in precious metals and stones, postal receiving service providers, telephone receiving service providers, and telephone forwarding service providers, and professionals such as lawyers, judicial scriveners, certified administrative procedures specialists, certified public accountants, and certified public tax accountants.

[16] FATF, *Guidance on Proliferation Financing Risk Assessment and Mitigation*, June 29, 2021, https://www.fatf-gafi.org/en/publications/Financingofproliferation/Proliferation-financing-risk-assessment-mitigation.html

Guidance on Proliferation Financing Risk Assessment and Mitigation
(Published in June 2021)

(Source) FATF

(i) Risk Factors

Like the risks related to money laundering and terrorist financing (hereinafter "ML/TF"), the PF risks are considered to be comprised of the following three factors.

Threat	Persons and entities that have previously caused or have the potential to evade, breach or exploit a failure to implement targeted financial sanctions related to PF in the past, present or future.
Vulnerabilities	Matters that can be exploited by the threat or that may support or facilitate the breach, non-implementation or evasion of targeted financial sanctions related to PF.
Consequences	The outcome where funds or assets are made available to designated persons and entities, which could ultimately allow them, for instance, to source the required materials, items, or systems for developing and maintaining illicit nuclear, chemical or biological weapon systems (or their means of delivery), or where frozen assets of designated persons or entities would be used without authorization, (including the possibility of causing reputational damage to the country or private-sector firms, and punitive measures by the UN and/or national authorities).

(ii) Points of Attention Regarding Assessment

The FATF PF Guidance states that, for national assessment of PF risks, the same approach as the one applied to the assessment of ML/TF risks may be used. The Guidance also states that national PF risk assessment should be comprehensive enough to inform national counter-PF strategies—just as the assessment of ML/TF risks should be comprehensive enough to inform national counter ML/TF strategies—and also to enable the implementation of targeted financial sanctions based on a risk-based approach. It also states that national PF risk assessment should help countries and private-sector firms to determine and prioritize the resources necessary to mitigate the different risks.

(2) Approach of the National Risk Assessment

The National Risk Assessment identified and analyzed the threats to Japan and its vulnerabilities and conducted a multi-faceted, comprehensive risk assessment in view of the FATF PF Guidance, and with reference to the FATF Recommendations and their Interpretative Notes (which are collectively referred to by the FATF as the "FATF Standards"), the points mentioned in the FATF Fourth Round Mutual Evaluation Report of Japan, other countries' national risk assessments (prepared by at least 24 countries/regions as of now, including the United States, the United Kingdom, and Australia), and reports by the Panel of Experts and the MSMT. Furthermore, the National Risk Assessment refers to "Complex Proliferation Financing and Sanctions Evasion Schemes" (hereinafter referred to as the "CPFSES Report")[17] published by the FATF in June 2025, which was compiled based on the "FATF PF Guidance" and summarizes the current PF threats and vulnerabilities, typologies and case studies of complex PF and sanctions evasion schemes, as well as enforcement challenges and best practices.

Complex Proliferation Financing and Sanctions Evasion Schemes
(Published in June 2025)

(Source) FATF

(3) Scope of the National Risk Assessment

Regarding CPF, the FATF Recommendation 7 covers compliance with PF-related UNSCRs for North Korea and Iran. On the other hand, the CPFSES Report analyzes PF risks that include not only those related to North Korean WMD proliferation but also those related to relevant actors as well as state actors, individuals, and entities that support or cooperate with North Korea or Iran to evade UNSC sanctions. Based on this, the National Risk Assessment covers a wider scope than the FATF Recommendation 7, including not only North Korea and Iran but also Russia in consideration of its relationship with North Korea.

[17] FATF, *Complex Proliferation Financing and Sanctions Evasion Schemes*, June 20, 2025, https://www.fatf-gafi.org/en/publications/Financingofproliferation/complex-proliferation-financing-sanction-evasion-schemes.html

(4) Framework for Preparing the National Risk Assessment

In preparing the National Risk Assessment, the relevant ministries and agencies indicated below cooperated and exchanged information with each other, and the Policy Council worked out the assessment report. (The relevant ministries and agencies are indicated below in order of establishment.)

National Police Agency (NPA): https://www.npa.go.jp/english/index.html
Financial Services Agency (FSA): https://www.fsa.go.jp/en/
Ministry of Internal Affairs and Communications (MIC): https://www.soumu.go.jp/english/index.html
Ministry of Justice (MOJ): https://www.moj.go.jp/EN/index.html
Ministry of Foreign Affairs (MOFA): https://www.mofa.go.jp/index.html
Ministry of Finance (MOF): https://www.mof.go.jp/english/index.htm
Ministry of Economy, Trade and Industry (METI): https://www.meti.go.jp/english/index.html
Ministry of Land, Infrastructure, Transport and Tourism (MLIT):https://www.mlit.go.jp/en/index.html
Japan Coast Guard (JCG): https://www.kaiho.mlit.go.jp/e/index_e.html
Ministry of Defense/Self-Defense Forces (MOD/SDF): https://www.mod.go.jp/en/

(5) Major Changes

Major changes in the 2025 National Risk Assessment are as follows:

- PF threats, vulnerabilities, and related cases analyzed in the CPFSES Report were added.
- Descriptions on sanctions against Iran that were reapplied in September 2025 under UNSCR 2231 were added.
- Descriptions on the reports by the MSMT containing information on violations and evasions of sanctions under UNSCRs were added.
- Up-to-date information on the activities of North Korean information technology workers and cyber actors was added.
- Related cases were summarized into tabular format at the end of this report.

Reference 1. Major Updates So Far

Publication Date	Major Changes
March 2024	First edition published
December 2024	More details were added regarding overseas changes and related cases

Chapter 2. PF Threats

1. Premises

The FATF PF Guidance defines PF threats as follows:

> *Threat refers to designated persons and entities that have previously caused or with the potential to evade, breach or exploit a failure to implement PF-TFS in the past, present or future. Such threat may also be caused by those individuals or entities acting for or on behalf of individuals or entities that have been subjected to measures such as asset freezing for their involvement in the development, possession and export of and other activities related to WMDs. It can be an actual or a potential threat.*

The Guidance also points out that when identifying PF threats, it is necessary to keep in mind that unlike ML/TF threats, PF threats have the following two characteristics:

I. Financing for the purpose of supporting WMD proliferation activities (e.g., development and trade) constitutes PF regardless of whether the financing is sourced from legitimate or illegitimate activities.
II. Not only threats caused by entities and individuals designated by relevant UNSCRs but also threats caused by global networks created by the designated entities or individuals to conceal their own activities may be equivalent to PF threats. The scope of assets that may be subject to sanctions includes those indirectly owned or controlled by designated entities or individuals.

2. Internationally Analyzed PF Threats

The CPFSES Report assesses the current PF threats as follows:

(1) North Korea

North Korea, though being subject to UNSCRs for nearly 20 years since the adoption of UNSCR 1695 in 2006, has continued to develop nuclear weapons. For example, North Korea launched an ICBM called the “Hwasong-19” in October 2024.

While such activities have continued, those subject to asset freezing measures under UNSCRs have remained almost unchanged in the past decade[18]. Furthermore, the Panel of Experts, established under

[18] MOFA, *Sanctions Against North Korea Based on UN Security Council Resolutions,* November 28, 2025, https://www.mofa.go.jp/mofaj/gaiko/unsc/page3_003268.html

UNSCR 1718 to monitor PF activities related to North Korea, was dissolved in 2024[19]. This has led to a major challenge in monitoring sanctions violations related to North Korea. For the FATF, it has become difficult to obtain information for assessing PF risks related to North Korea, hindering PF risk assessment in each country.

As for North Korea, there are two major factors that contribute to the financing of WMD.

First, there have been various activities to enhance financial cooperation. For example, enhancing economic cooperation and promoting mutual understanding on economic and investment potential was agreed between Russia and North Korea under the Russia-North Korea Partnership Treaty. In addition, North Korean officials of financial institutions based in North Korea's neighboring countries including Russia were facilitating transactions worth hundreds of millions of dollars to support North Korea's trade and revenue as of 2024, despite the fact that UNSCRs require States to expel individuals working on behalf of or at the direction of North Korean financial institutions. The enhancement of such financial cooperation has led to vulnerabilities in the international financial system (see Overseas Case 1).

Second, the means of securing revenue sources have become more diversified. Activities related to sanctions evasion include forgery, fraud, cyber theft, and trafficking of arms, drugs, and wildlife. For example, billions of dollars in virtual assets have been stolen in cyberattacks against crypto-related companies. North Korea has sent thousands of highly skilled IT workers around the world to capitalize on demand for specific IT skills, such as software and mobile application development, to obtain freelance contracts from clients around the world, including Asia, Europe, and North America. North Korean trading companies subject to sanctions are related to North Korea's wig and false eyelash exports that accounted for about 60% of its overall exports to its neighboring countries in the first half of 2024, indicating that revenues from such exports may support North Korea's strategic weapons program. The diversification of revenue sources further increases PF risks and sanctions evasion threats.

(2) Iran

Iran was initially sanctioned by the United Nations (UN) from 2006 to 2010 for its non-compliance with UNSCR 1696 (2006), etc., before the adoption of UNSCR 2231 in 2015. UN financial sanctions imposed on persons and entities related to Iran under the resolution expired in October 2023[20]. However, some countries have implemented their own sanctions due to threats posed by Iran.

---

[19] UNSC, *Security Council fails to extend mandate for Expert Panel Assisting Sanctions Committee on Democratic People's Republic of Korea,* March 28, 2024, https://press.un.org/en/2024/sc15648.doc.htm

[20] As noted in Chapter 1,1(2)(ii) of this report, on September 28, 2025, the sanctions previously adopted against Iran were re-applied pursuant to UNSCR 2231.

Iran has relied on military proxy organizations in the Middle East and international criminal networks that exploit currency exchange offices and banks to evade sanctions. In particular, Hezbollah acts as a proxy for Iran in direct violation of sanctions, carrying out large-scale smuggling oil, weapons, and other goods subject to sanctions.

(3) Russia

The Russia-North Korea Partnership Treaty, as well as other bilateral economic and military cooperation frameworks, has raised concerns that Russia may pose a PF threat and has led to the creation of new revenue sources supporting North Korea's WMD development program. North Korea announced that it had dispatched troops to the Russia-Ukraine conflict under the new treaty. The expansion of economic and military relations between Russia and North Korea has raised concerns in many countries that Russia poses a PF threat, further complicating PF and sanctions evasion.

(4) Other Threats

Many countries remain concerned that, in addition to state actors, non-state actors, such as terrorist groups and criminal organizations, may seek to acquire and procure materials, knowledge, and technologies related to WMD, including biological, chemical, and nuclear weapons. In light of this situation, UNSCR 1540, updated in November 2022, reaffirmed international commitments to prevent the proliferation of WMD by non-state actors. While there have so far been few cases of non-state actors abusing the financial system to support PF or PF-related activities, many countries recognize the importance of continuously monitoring their potential impacts.

3. Threats in Japan

In light of the abovementioned definition of PF threat and internationally analyzed threats, Japan is considered to be exposed to the following threats.

(1) Persons and entities involved in the outflow of funds
  (i) Trade: Sanctions-circumvention trade or remittances with North Korea, Iran, and Russia
  (ii) Persons: Remittances to persons of North Korean nationality
  (iii) Cyberattacks or related activities
(2) Persons and entities involved in the outflow of goods and technologies
  (i) Funds through the provision of dual-use items, and related remittances
  (ii) Earning funds through intangible technology transfers, and related remittances
  (iii) Ship-to-ship transfers, and related remittances
(3) Persons and entities using opaque corporate structures located in Japan or elsewhere, including

those involving persons or entities designated under the UNSCRs

(1) Persons and Entities Involved in the Outflow of Funds

Where funds flow out of Japan for the purpose of WMD development, the following assumptions are made with respect to the three possible types of activities—trade (movement of goods), movement of persons, and cyberattacks—and the persons and entities involved in those activities.

(i) Trade: Persons and Entities That Conduct or Attempt to Conduct Sanctions-circumvention Trade or Remittances with North Korea, Iran, and Russia

With regard to North Korea, Iran, and Russia, which are assessed as PF threats, certain economic sanctions have been imposed domestically and internationally. Accordingly, rather than engaging in direct transactions with these countries, it is considered that trade transactions or remittances for sanctions circumvention may be conducted or attempted via neighboring countries or other third countries, and that persons and entities seeking to engage in such transactions exist as threats.

According to published data, North Korea and Iran actively trade with countries/regions such as China, Southeast Asia, and the Middle East.

North Korea's exports in 2024 totaled 360 million dollars, an increase of 10.8% from the previous year. Major contributors to export growth included caps and wigs (up 13.0%), ores, slags, and ashes (up 40.7%), and clocks (up 294.2%)[21]. North Korea relies on China for approximately 98% of its international trade. According to the General Administration of Customs of China, trade between China and North Korea in the period from January to July 2025 reached 1,465.84 million dollars, representing a 32% increase compared with the same period of the previous year.

According to the Iran Customs Administration, Iran's exports in 2024 totaled 57,844 million dollars, an increase of 15.4% from the previous year. Key drivers of export growth to China, Iran’s largest export destination, included plastics and plastic products (up 6.3%), edible fruits and nuts (up 320%), and aluminum and aluminum products (up 34.2%)[22]. With regard to Russia, while Europe had previously been its major trading partner, trade with countries such as China, India, and Kazakhstan has expanded as a result of economic sanctions imposed following its aggression against Ukraine in 2022.

[21] Bank of Korea, *Gross Domestic Product Estimates for North Korea in 2024*, August 29, 2025, https://www.bok.or.kr/eng/bbs/E0000634/view.do?menuNo=400423&nttId=10093293
[22] Japan External Trade Organization (JETRO), *Iran Trade and Investment Report*, https://www.jetro.go.jp/world/middle_east/ir/gtir.html

Reference 2. North Korea's 10 Major Trade Counterpart Countries (2024)

(Unit: 1 thousand dollars. %)

Ranking	Country/region	Exports by North Korea		Imports by North Korea		Total Trade Value	
		Value	Rate of Change	Value	Rate of Change	Value	Share
1	China	341,819	16.9	2,299,051	△5.3	2,640,870	97.95
2	Argentina	590	168.2	14,535	1,141.2	15,125	0.56
3	Vietnam	4,916	△46.4	7,959	20.9	12,875	0.48
4	Netherlands	186	204.9	7,991	585.9	8,177	0.30
5	Nigeria	1,542	22.3	2,917	224.1	4,459	0.17
6	India	1,404	△49.1	2,055	9.9	3,459	0.13
7	Austria	2,254	△24.7	482	-	2,736	0.10
8	Indonesia	906	39.4	2	△98.7	908	0.03
9	Mozambique	846	△73.3	7	-	853	0.03
10	Senegal	736	16.8	28	△82.8	764	0.03

Reference 3. Top Five Export Products of North Korea (2024) (Unit: 1 thousand dollars. %)

Items	2023	2024			Share of Exports to China
		Value	Rate of Change	Share	
Prepared Feathers and Feather Products	167,664	189,384	13.0	52.5	100.0
Ores, Slag, and Ash	33,115	46,606	40.7	12.9	100.0
Iron and Steel	34,367	23,436	△31.8	6.5	99.7
Mineral Fuels and Mineral Oils	22,395	22,244	△0.7	6.2	99.8
Clocks, Watches, and Their Parts	4,212	16,604	294.2	4.6	100.0

(Source) KOTRA (Korea Trade-Investment Promotion Agency), "*2024 Trends in North Korea's Foreign Trade (KOTRA Report 25-091)*" (published July 28, 2025), compiled by the MOF based on the report.

https://dream.kotra.or.kr/dream/cms/indReport/actionIndReportDetail.do?MENU_ID=4630&CONTENTS_NO=1&pRptNo=14039&pHotClipTyName=DEEP#

(Notes)

1. Since North Korea does not publish official statistics on foreign trade, the figures are estimates based on data from official statistical agencies of various countries.

2.The survey for 2024 covered 85 countries.

3.Russia was not included in the 2024 survey because its official statistics have not been released.

4.Based on HS code classification, "Prepared feathers and feather products" includes items such as false eyelashes and wigs.

Reference 4. Iran's Major Trade Counterpart Countries (FY2024)

(Unit: 1 million dollars. %)

Export					Import				
Country/Region	FY2023	FY2024			Country/Region	FY2023	FY2024		
	Value	Value	Share	Rate of Growth		Value	Value	Share	Rate of Growth
China	14,157	14,854	25.7	4.9	United Arab Emirates	20,987	21,981	30.4	4.7
Iraq	9,351	11,941	20.6	27.7	China	18,682	19,325	26.7	3.4
United Arab Emirates	6,715	7,201	12.4	7.2	Türkiye	7,678	12,474	17.2	62.5
Türkiye	4,211	6,889	11.9	63.6	Germany	2,177	2,430	3.4	11.6
Pakistan	2,111	2,423	4.2	14.8	India	1,933	1,747	2.4	△9.6
Japan	11	10	0.0	△10.9	Japan	99	104	0.1	5.1

(Source) JETRO, "*Table 1-1: Iran`s export to major countries (non-oil sector) (customs base)*" and "*Table 1-2: I Iran`s import from major countries (non-oil sector) (customs base)*", compiled by the MOF based on JETRO data.

https://www.jetro.go.jp/world/middle_east/ir/gtir.html#page02

(Notes)

1. Usually, the period of the fiscal year in Iran is from around March 21 to March 20 in the following year. Fiscal year 2024 covers March 20, 2023 – March 20, 2024; fiscal year 2023 covers March 21, 2022 – March 19, 2023.
2. The value of exports covers only non-oil sectors (oil and gas products are included).
3. The terms of trade include both FOB and CFR with respect to both imports and exports.
4. Based on date from Iranian Customs.

Reference 5. Russia's Major Trade Counterpart Countries (January-September 2024)

(Unit: 1 million dollars. %)

Export				Import			
Country/Region	2023	January-September 2024		Country/Region	2023	January-September 2024	
	Value	Value	Rate of Growth		Value	Value	Rate of Growth
China	129,323	129,882	0.43	China	110,913	115,257	3.92
India	60,612	66,002	8.89	EU	41,063	34,021	△17.15
Türkiye	45,669	43,969	△3.72	Kazakhstan	9,788	9,546	△2.47
EU	48,164	36,496	△24.23	Türkiye	10,907	8,556	△21.55
Kazakhstan	16,192	18,252	12.72	India	4,057	4,922	21.32
Brazil	10,013	10,965	9.51	Brazil	1,343	1,450	7.97
Japan	7,434	5,698	△23.35	Japan	2,850	2,162	△24.14

(Source) JETRO, "*Table 2: Trends in Russia's Export Value by Country/Region (FOB)*" and "*Table 5: Trends in Russia's Import Value by Country/Region (FOB*)," compiled by the MOF based on JETRO data.

https://www.jetro.go.jp/biz/areareports/2025/519c550387fafe33.html

(Notes)

1.Due to inconsistencies in statistical standards (CIF, FOB, etc.) and differences in conversion rates, figures do not match those published by Russia.

2.Russia's export value to each country/region is based on the import value from Russia recorded by the counterpart country.

3.Data is based on sources including the Federal Customs Service of Russia, GAT, TradeMap, the UAE Federal Competitiveness and Statistics Authority, the Statistics Agency under the President of Uzbekistan, the Belarus Statistics Office, and various media reports.

Reference 6. Russia's Exports by Commodity (January- September 2024)

Customs Basis, Exports (FOB)	(Unit: 1 million dollars, %)			
Items	2023	January-September 2024		
	Value	Value	Share	Rate of Growth
Mineral Products	260,127	197,681	62.1	3.1
Precious Stones, Precious Metals and Articles Thereof	60,026	45,118	14.2	△6.2
Foodstuffs and Agricultural Products (Excluding Textiles)	43,058	30,983	9.7	△4.0
Chemicals, Plastics and Rubber	27,205	19,888	6.3	△1.9
Machinery, Equipment, Transport Equipment and Other Articles	22,927	15,179	4.8	△3.7
Wood, Pulp and Paper Products	9,860	7,584	2.4	0.8

(Source) JETRO, *"Table 7: Russia's Exports by Commodity (Customs Basis) for January–September 2022–2024, Exports (FOB),"* compiled by the MOF based on JETRO data,
https://www.jetro.go.jp/biz/areareports/2025/519c550387fafe33.html
(Note) Based on data from the Federal Customs Service of Russia.

Reference 7. Japan's Major Trade Counterpart Country/Regions (2024)

(Unit: 1 thousand dollars. %)

Ranking	Country/Region	In Terms of Export by Japan		Ranking	Country/Region	In Terms of Import by Japan	
		Value	Rate of Change			Value	Rate of Change
1	China	167,809,756	△ 3.7	1	United States	140,948,238	△ 2.2
2	United States	83,883,661	1.6	2	China	124,819,696	△ 1.3
3	Australia	53,132,251	△ 18.7	3	Republic of Korea	46,547,844	△ 1.0
4	United Arab Emirates	36,976,407	△ 0.1	4	Taiwan	45,431,984	5.6
5	Republic of Korea	31,543,006	1.5	5	Hong Kong	36,029,151	10.5
6	Taiwan	30,614,191	△ 14.3	6	Thailand	26,648,088	△ 9.4
7	Saudi Arabia	29,944,219	△ 13.9	7	Singapore	19,870,952	5.4
8	Vietnam	26,857,240	3.9	8	Germany	17,427,478	△ 10.1
9	Thailand	24,772,816	△ 3.9	9	India	17,258,203	8.1
10	Indonesia	23,451,905	△ 4.3	10	Vietnam	17,116,042	△ 0.4
24	India	6,459,130	14.3	11	Australia	16,015,745	△ 4.6

(Source) JETRO, *"Table 1: Overview of Trade by Region (2024, Final Confirmed Figures),"* compiled by the MOF based on JETRO data.
(*) The countries/regions indicated in red are the ones indicated in Reference 2.

While Japan has banned the import of all cargo originating in or shipped from North Korea, illicit imports from North Korea have been identified (see Domestic Case 1 to 5).

In response to the above-mentioned threats, Japan has taken asset-freezing and other measures based on the FEFTA (see Chapter 4). The government needs to continue promoting prudent responses to transactions with countries/regions regarded as PF risks and, based on the latest information and data, to verify sanctions-circumvention transactions with these countries conducted via third countries (see Domestic Case 6 to 8).

It is also useful for private-sector business operators to take appropriate actions in accordance with the risks, while paying particular attention to transactions related to countries/regions and items that require caution.

In recent years, it has been pointed out that countries/regions of concern have continued transfers of goods while evading international surveillance by employing sophisticated means, including document forgery and the diversification of transportation routes, when illicitly exporting WMD-related items.[23] As of now, there have been no arrest cases involving the smuggling of WMD into Japan, however, it is necessary to respond under international cooperation to prevent countries/regions of concern from engaging in indirect imports via third countries.

(ii) Persons: Persons and Entities That Conduct or Attempt to Conduct Remittances to Persons of North Korean Nationality

Making remittances from Japan to North Korea is prohibited in principle. Japan has imposed broad restrictions on the movement of people to and from North Korea, including the prohibition-in-principle of the entry of persons of North Korean nationality into Japan.

In relation to the prohibition-in-principle of payments to North Korea, it is required that special attention be paid to overseas remittances made to the three provinces of China's northeastern region (Liaoning Province, Jilin Province, and Heilongjiang Province) because migrant workers from North Korea have traditionally stayed there (see Domestic Case 9 to 10).

On the other hand, some neighboring countries/regions and other third countries/regions have not prohibited the entry of persons of North Korean nationality, and some of them accept workers from North Korea. Remittances made from Japan to persons of North Korean nationality residing in those countries/regions may include transactions that constitute PF, regardless of whether they are legitimate or illegitimate. From this perspective, persons of North Korean nationality who are dispatched by the North Korean authorities to third countries, including neighboring countries, and earn income there,

[23] MOD/SDF, *Defense of Japan 2025*, https://www.mod.go.jp/en/publ/w_paper/index.html

as well as persons and entities that seek to make remittances to persons contributing to fund-raising related to PF activities conducted by North Korean authorities, are considered to be threats (see Overseas Case 4 to 5).

According to the second report by the MSMT, North Korea is likely to have earned approximately 350 million to 800 million dollars through IT workers in 2024.[24] It has been pointed out that the activities of North Korean IT workers are becoming more sophisticated and are expanding their targets worldwide.[25] Furthermore, it has also been pointed out that North Korean IT workers are likely to be involved in malicious cyber activities, such as information theft, and that the associated threats have been intensifying (see Overseas Case 6).

In Japan, cases have been identified in which North Korean IT workers impersonate Japanese citizens to earn income by using online platforms provided by Japanese and other companies for receiving and placing business orders (see Domestic Case 11 to 14).

The government should continue to verify, based on all available and up-to-date data, whether there are countries/regions that require particularly strict examination.

Private-sector business operators should also conduct strict examination of transactions while paying heed to countries/regions requiring attention.

(iii) Cyber activities: Persons and Entities That Conduct Cyberattacks or Related Activities

North Korea, which is under sanctions of various kinds, uses cyberattacks to acquire foreign currency by taking advantage of sanction loopholes[26] (see Overseas Case 7 to 14). According to the second report by the MSMT, North Korea is reported to have stolen at least 2.8 billion dollars in crypto assets between January 2024 and September 2025. Moreover, North Korean attacks on crypto assets have been increasing in both frequency and scale. An analysis of the average time required to complete successful attacks shows year-on-year decreases across attacks of all sizes, indicating that large-scale attacks are being carried out more skillfully and rapidly. These attacks are reportedly linked to North Korean IT workers, who are said to exploit identity forgery and remote work arrangements in order to attempt access by using advanced tactics, techniques, and procedures.[27]

---

[24] MSMT, *The DPRK's Violation and Evasion of UN Sanctions through Cyber and Information Technology Worker Activities (MSMT/2025/2)*, October 22, 2025, https://msmt.info/Publications/detail/MSMT%20Report/4221

[25] Federal Bureau of Investigation (FBI), *North Korean IT Worker Threats to U.S. Businesses*, July 23, 2025, https://www.ic3.gov/PSA/2025/PSA250723-4

[26] MOD/SDF, *Defense of Japan 2025*, https://www.mod.go.jp/en/publ/w_paper/index.html

[27] Chainalysis, *The 2025 Crypto Crime Report*, January 15, 2025, https://go.chainalysis.com/2025-Crypto-Crime-Report.html

In Japan, the number of cleared cybercrime cases has been steadily on an increasing and reached a record high of 13,164 cases in 2024. This indicates that threats in cyberspace have remained extremely serious in recent years.[28] On October 14, 2022, the relevant agencies issued an alert stating that, for several years, Japan's crypto asset exchange companies had been strongly suspected of having been targeted by the “Lazarus” cyberattack group, which is alleged to be a subordinate organization of the North Korean authorities.[29] On December 24, 2024, the National Police Agency announced that the North Korea-backed cyberattack group “TraderTraitor” stole approximately 48.2 billion yen worth of crypto assets from DMM Bitcoin Co., Ltd., a Japanese crypto asset-related company[30] (see Domestic Case 15).

According to the second report by the MSMT, it has been observed that North Korean cyber actors use various ML tools, such as mixing and bridging, after stealing funds, in order to obscure their sources and evade tracking by regulators.[31] Furthermore, cases have been identified in which ransomware attackers[32] demanded ransom payments in crypto assets and threatened to conduct larger-scale attacks if the demands were not met, as well as cases in which crypto assets were used for ransomware payments (see Overseas Case 15 to16).

[28] NPA, *Police White Paper 2025*, https://www.npa.go.jp/hakusyo/r07/honbun/index.html

[29] FSA, NPA, and National Center of Incident Readiness and Strategy for Cybersecurity (NICS), *Advisory on Cyberattacks Targeting Crypto Asset–Related Businesses by the Cyberattack Group Known as Lazarus, believed to be a subordinate organization of the North Korean authorities*, October 14, 2022, https://www.fsa.go.jp/news/r4/sonota/20221014/20221014.pdf

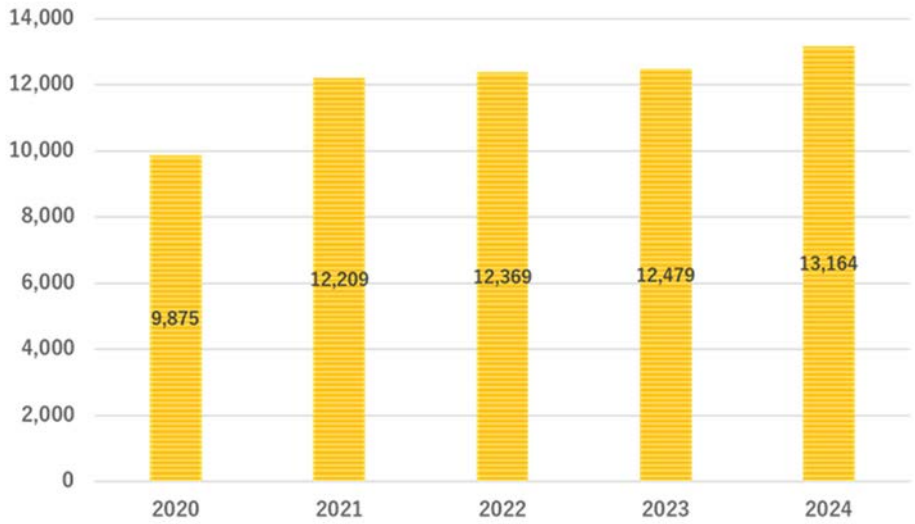
[30] NPA, *On Cyberattacks Targeting Crypto Asset–Related Businesses by TraderTraitor, a Cyberattack Group Linked to North Korea*, December 24, 2024, https://www.npa.go.jp/bureau/cyber/pdf/020241224_pa.pdf

[31] A technique called mixing is used in order to make it difficult for third parties to trace transactions or to identify cases of a single user using multiple accounts by adding to users’ crypto asset transaction data addresses unrelated to them at the time of data input or output. There are also other techniques, such as making it difficult to trace crypto assets by using a “bridge” multiple times for exchange of crypto assets between different blockchains to sever the link between transactions through “chain hopping.” Although technologies and tools for identifying the history of transactions have become widely available with respect to some of those techniques, a tight race is still on between the advance of crime techniques and the progress of technologies to counter the threat.

[32] Ransomware refers to malicious software that, once it infects a computer or other device, encrypts the data stored on it and renders the data unusable, and then demands payment—typically in money or crypto-assets—in exchange for decrypting the data.
NPA, *Measures to Prevent Ransomware Damage*, https://www.npa.go.jp/bureau/cyber/countermeasures/ransom.html

Reference 8. Changes in the Number of Cleared Cybercrime Cases

(Unit: the number of cases)



(Source) NPA, *2025 Edition of the Police White Paper.* Compiled by the MOF.

(2) Persons and Entities Involved in the Outflow of Goods and Technologies

Possible cases are assumed in which goods and technologies flow out of Japan for the purpose of WMD development, and persons who seek to acquire funds through such activities, as well as persons and entities involved therein, are considered to pose PF threats. Japan possesses advanced technologies and goods that utilize such technologies, and if these technologies and goods were to be transferred to countries engaged in WMD development, they could pose an international threat and lead to instability in the international situation.

(i) Persons and Entities That Obtain Funds Through the Provision of Dual-use Items, and Persons and Entities Involved in Related Remittances

In Japan, there are high-quality dual-use items with advanced technologies that can be used for both civilian and military applications. Where such items are procured for the purpose of WMD development through the use of Japanese infrastructure, it becomes difficult to identify the purposes and routes of import and export, while destruction of evidence and the evasion or circumvention of sanctions become easier. Accordingly, trade in dual-use items is considered to constitute one form of PF threat (see Domestic Case 16 to 23).

Under Japan's export control system, licenses are required for the export of dual-use and other items that may be used for WMD development, even if those items are not subject to export controls under international agreements. In order to enhance the effectiveness of this system, METI has published the End User List, which identifies foreign companies and organizations with respect to which concerns

remain regarding possible involvement in WMD development.[33] When exporting goods to companies and organizations listed on the End User List, a license from METI is required, except where it is clear that such goods are not to be used for WMD development or other illicit activities.

Although METI provides information to the public regarding which items require prior export licenses as dual-use items, there have been cases in which private-sector business operators have imported or exported such items without sufficient understanding, resulting in transactions being determined to constitute regulatory violations.

In addition to preventing violations of laws and regulations, METI has long conducted outreach activities targeting small and medium-size enterprises, with the aim of maintaining international peace and preventing the outflow of technologies.

Reference 9. Uses of Concern and Civilian Uses of Dual-use Items

	Uses of concern	Civilian uses
Machine tools	Production of centrifugal separators for uranium enrichment 	Production of Automobiles and machining 
Sodium cyanide	Raw materials of chemical weapons 	Metal plating process 
Filters	Extraction of bacteria for production of bacterial weapons 	Seawater desalination 
Carbon fiber	Structural materials of missiles 	Structural materials of aircraft 

(Source) An extract from a reference material prepared by the METI

[33] As of the amendment on October 9, 2025, a total of 154 entities in North Korea and 257 entities in Iran are listed on the End User List.
METI, *End User List*, October 9, 2025, https://www.meti.go.jp/english/press/2025/0929_003.html

Reference 10. Examples of Goods at High Risk of Being Used for WMD Development

Items	Uses of concern
1. Tributyl phosphate (TBP)	Nuclear weapons
2. Carbon/Glass/Aramid fiber	Nuclear weapons, missile
3. Titanium alloys	
4. Maraging steel	
5. Aluminum alloys tubes with a diameter of more than 75 mm	Nuclear weapons
6. Flow-forming machines	Nuclear weapons, missile
7. Numerically-controlled (N/C) machine tools	
8. Isostatic presses	
9. Filament winding machines	
10. Frequency changers	Nuclear weapons
11. Mass spectrometers or ion sources	
12. Vibration test systems	Nuclear weapons, missile
13. Centrifugal multiplane balancing machines	
14. Corrosion-resistant pressure gauges/sensors	
15. Large-size non-destructive inspection equipment	
16. High frequency oscilloscope and waveform digitizers	Nuclear weapons
17. Stable power/voltage DC power supplies	
18. Large generators	
19. Large vacuum pumps	
20. Radiation-hardened robots	
21. TIG welding units, electron beam welding units	Nuclear weapons, missile
22. Radiation monitoring and detection equipment	Nuclear weapons
23. Mill for fine powder	Missile
24. Karl Fischer moisture equipment	

Items	Uses of concern
25. Equipment designed for producing prepregs	Missile
26. Artificial graphite	Nuclear weapons, missile
27. Gyroscopes	Missile
28. Rotary encoders	
29. Heavy trucks (incl. tractors, trailers, dump trucks)	
30. Crane trucks	
31. Chambers (sealed) for fermentation	Biological weapons
32. Centrifugal separators	
33. Freeze dryers	
34. Corrosion-resistant reactors	Missiles, chemical weapons
35. Corrosion-resistant agitators	
36. Corrosion-resistant heat exchangers or condensers	
37. Corrosion-resistant distillation or absorption columns	
38. Corrosion-resistant filling equipment	
39. Unmanned aerial vehicles (UAVs) that are specially designed for incorporating spray machines (excl. model aircraft for amusement or sport use)	Missiles, biological/chemical weapons
40. Spray machines that are specially designed for installing in UAVs	
41. N-(1-phenethyl-4-piperidyl)propionanilide (also known asfentanyl) (437-38-7), N-[1-[2-(4-ethyl-5-oxo-2-tetrazoline-1-yl)ethyl]-4-(methoxymethyl)-4-piperidyl]propionanilide (also known as alfentanil) (71195-58-9), Methyl=1-phenethyl-4-(N-phenylpropanamide)piperidine-4-carboxylate (also known as carfentanil) (59708-52-0), 1-(2-methoxycarbonylethyl)-4-(phenylpropionylamino)piperidine-4-carboxylic acid methyl ester (also known as remifentanil) (132875-61-7), N-[4-(methoxymethyl)-1-[2-(2-thienyl) ethyl)-4-piperidyl]propionanilide (also known as sufentanil) (56030-54-7)	Chemical weapons

(Source) An extract from the Security Export Guidance (Introduction), METI.

In addition to the possibility that companies may unintentionally violate regulations, there is also the possibility that, with the increasing complexity of distribution structures, persons and entities of

concern may use various techniques to acquire sensitive technologies and goods that can be converted to military applications while concealing the identities of the actual end users. The CPFSES Report cites schemes to circumvent country-specific export controls by using third-country intermediaries, such as front companies or defunct shell companies, as well as falsified documents, to conceal information on transportation routes, final destinations, and countries of origin of dual-use items (see Overseas Case 17 to 18). In addition, there are cases in Japan in which, despite compliance with legitimate procedures, such technologies and goods are resold, through third countries where export controls are not strictly enforced, to countries engaged in the development of WMD or conventional weapons (see Domestic Case 24).

When companies involved in import and export transactions suspect PF-related transactions, in addition to identifying suspicious cases such as those described below, it is useful for them to identify signs of PF by checking risk indicators by categories—such as customer behavior, transactions, and trade activities—described in the CPFSES Report.[34] [35]

- Customers conduct trade transactions involving dual-use items, export-controlled items, or equipment that is not consistent with their technical backgrounds or business activities, including complex equipment. Payments for such items are made using individuals' accounts. Customers affiliated with universities or research institutions handle dual-use items or export-controlled items.
- Customers that are manufacturing or trading companies use cash in transactions involving industrial products or other trade transactions. As an indication of such transactions, the outstanding balances of their deposit accounts increase steeply, followed by cash withdrawals.
- The counterparty to a trade transaction at the final destination of delivery is a transportation company or an entity other than the importer.
- There are inconsistencies or deficiencies in descriptions (such as parties to transaction, quantities of goods, or prices, etc.) across contracts, invoices, and trade-related documents, etc. Instructions are given to make or receive remittances from persons who cannot be identified through letters of credit or similar means.
- The declared price of cargo is low in comparison with transportation costs.
- Items whose quality or specifications are not consistent with the technological level of the country of destination are exported.
- Multiple destinations are designated with no apparent purpose; the flag of registry of a vessel is

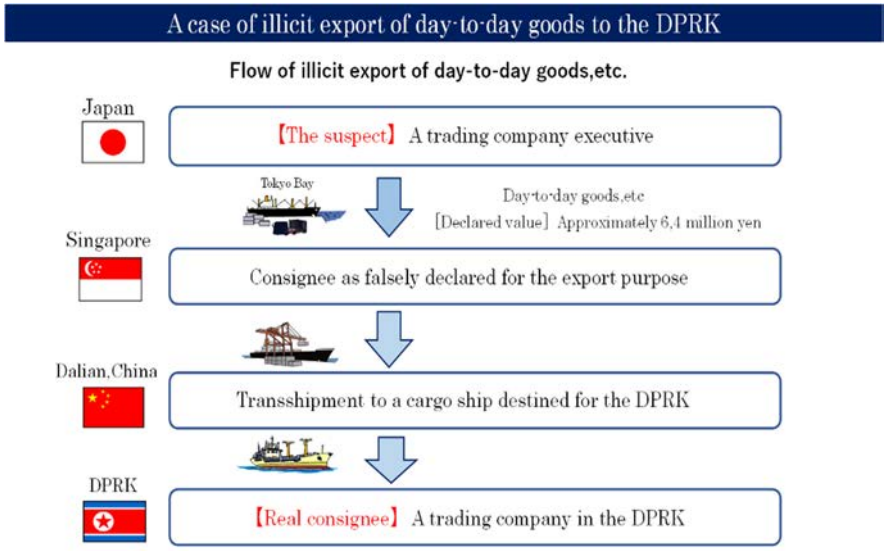
[34] MOF, *Frequently Asked Questions Concerning Guidelines for Foreign Exchange Transactions Service Providers on Compliance with FEFTA and Its Regulations, etc., published in July 2025*, https://www.mof.go.jp/policy/international_policy/gaitame_kawase/inspection/guideline_index.htm
[35] MOF, *CPFSES*, https://www.mof.go.jp/policy/international_policy/convention/fatf/20250704PFreport.html

changed frequently; or goods are transported through roundabout means, including the use of small or obsolete vessels, or are routed via countries/regions of concern.

- Customers request the issuance of letters of credit related to dual-use items or export-controlled items before approval is given for the opening of an account.
- Multiple bank accounts or complex or unusual payment routes, including those using crypto assets, etc. are utilized.
- Sudden changes are instructed with respect to ultimate consignees or destinations for shipments of dual-use equipment or technologies, or other goods unrelated to normal business activities.
- Commercial transactions run counter to normal trade patterns, including cases in which goods are exported or imported by countries that do not usually export or import such goods. Trade transactions lack clear grounds or reasonable explanations for large payments.
- Transactions involve goods transiting through countries/regions of concern, or involve freight-forwarding firms operating in high-risk transshipment areas.
- End users are not specified in invoices or related documents; there is suspicion that false contracts are used to conceal the end user; or there are discrepancies between invoice information and cargo information (such as cargo type, weight, value, or destination).

With regard to North Korea, even for products other than dual-use items, including daily goods such as food and clothing, there are persons and entities that engage in, or attempt to engage in, illicit exports or indirect exports to North Korea via third countries. Such persons and entities, as well as those involved in related remittances, may be considered to pose PF threats. In some cases of illicit exports to North Korea, a method involving multiple transit points has been employed.

Reference 11. A Case of Illicit Export of Day-to-day Goods, etc. to North Korea



(Source: NPA)

Reference 12. Counterpart Countries/Regions in Illicit Exports from Japan and the Industry Categories and Attributes of Legal Persons and Individuals Subjected to Administrative Punishments for Illicit Exports

According to the list of cases of violation of the FEFTA published by the Center for Information on Security Trade Control, and the list of cases related to measures implemented against North Korea published by the NPA, the major counterpart countries/regions (places of destination and transit) in cases subject to administrative punishment for illicit exports are as follows. (The countries/regions underlined indicate places of destination and transit in cases for which administrative punishment was imposed in and after 2018.)

Category	Specific Country/Region
Places of destination	North Korea, China, ROK, Myanmar, Thailand, Singapore, Malaysia, Iran, the Philippines, Indonesia, United States, German Democratic Republic (East Germany), Poland
Places of transit	Hong Kong, China, China (Dalian), ROK, ROK(Busan), Singapore, Malaysia, Taiwan, Iran

The major industry categories and attributes of legal persons and individuals subjected to administrative punishments are as follows (the industry categories and attributes underlined indicate those observed in cases in which administrative punishments were imposed in and after 2018).

Legal Persons

- Trading companies (e.g., chemicals, construction materials, PCs, seafood, day-to-day goods, machinery and equipment, and automobiles)
- Manufacturing companies (e.g., semiconductors, electronic equipment, transportation machinery, and textiles)
- Industrial waste delivery companies
- Transportation companies
- EC site operating companies
- Retail companies
- Travel agencies

Natural Persons

- Company executives
- Former company executives
- Travelers from North Korea
- Unemployed youth
- Officials related to Japan-North Korea friendship associations

As described above, there have been cases in which dual-use items and daily goods have been exported illicitly from Japan to countries/regions of concern, including cases of indirect exports via third countries. The techniques used in such illicit exports have become increasingly sophisticated. Accordingly, persons and entities that generate funds through the provision of dual-use and other goods, etc., as well as those involved in related remittances, may be regarded as potential threats.

(ii) Persons and Entities That Obtain Funds Through Intangible Technology Transfers, and Persons and Entities Involved in Related Remittances

Japan possesses information related to advanced technologies used around the world and manufactures cutting-edge, high-performance products. Some of this technological information and these products may be diverted to military applications depending on how they are used. There are also concerns over intangible technology transfer, a practice whereby countries/regions of concern obtain advanced technologies that may be applied to WMD development and production through researchers and students dispatched to major companies or academic institutions in developed countries. Even if such activities are conducted in a legitimate manner, the technologies thus obtained may be abused for WMD proliferation. In this regard, a deficiency in FEFTA compliance has been pointed out (see Domestic Case 25).

Although there have been few cases of intangible technology transfers being misused to support WMD proliferation, persons and entities seeking to raise funds for WMD development through such transfers are considered to be a threat, given Japan's advanced technologies and related products.

(iii) Persons and Entities That Conduct Ship-to-ship Transfers, and Persons and Entities Involved in Related Remittances

Japan is an island nation surrounded on all sides by the Pacific Ocean, the Sea of Okhotsk, the Sea of Japan, and the East China Sea, and cross-border movement of people and goods is routed via seaports and airports.

According to reports of the Panel of Experts, refined petroleum products have been delivered through illicit ship-to-ship transfers in North Korea's territorial waters and exclusive economic zone.[36] In this respect, under the UNSCRs, all UN Member States are prohibited from facilitating or engaging in the supply, sale, or transfer, including ship-to-ship transfers, of any type of goods or items to or from North Korea (UNSCR 2375, para. 11, etc.). In accordance with this prohibition, as part of monitoring and surveillance activities, the MOD/SDF conduct information-gathering activities on vessels suspected of violating the UNSCRs using Japan Maritime Self-Defense Force (JMSDF) vessels and other assets. The CPFSES Report points out that ship-to-ship transfers carry a risk of being abused to falsify cargo

[36] Cases of ship-to-ship transfers have been pointed out every year in reports by the Panel of Experts.

routes and destinations in order to evade sanctions.

To date (as of the end of October 2025), the MOD has disclosed 24 cases strongly suspected of constituting ship-to-ship transfers.

There have been no cases exposed by the JCG involving ship-to-ship transfers or smuggling of goods or persons related to North Korea's PF activities. Moreover, as of the end of December 2024, there have been no cases in which activities by suspicious vessel or spy vessel[37] from North Korea exposed by the JCG were judged to be related to WMD development. In January 2025, apart from ship-to-ship transfers conducted for sanctions evasion or fund transfers, the JCG blocked drug smuggling activities by clearing multiple cases of smuggling involving ship-to-ship transfers, including the first drug smuggling case using small vessels in five years since 2018.[38]

Reference 13. Illicit Ship-to-ship Transfers of Goods by North Korea-related Vessels [39]

	Names of Tankers of North Korean Nationality	Names of Vessels Transferring Goods to North Korean Tankers	Date of Incident Occurrence
1	Rye Song Gang 1	Yuk Tung, the Dominican-flagged tanker	Jan. 20, 2018
2	Rye Song Gang 1	Wan Heng 11, the Belizean-flagged tanker	Feb. 13, 2018
3	Yu Jong 2	MIN NING DE YOU 078, the North Korean-flagged tanker	Feb. 16, 2018
4	Chon Ma San	Xin Yuan 18, the Maldivian-flagged tanker	Feb. 24, 2018
5	JI SONG 6	An unidentified small vessel	May 19, 2018
6	SAM JONG 2	An unidentified tanker	May 24, 2018
7	YU PHYONG 5	An unidentified small vessel	Jun. 21 and 22, 2018
8	AN SAN 1	An unidentified vessel	Jun. 29, 2018
9	NAM SAN 8	An unidentified vessel	Jul. 31, 2018
10	AN SAN 1	An unidentified small vessel	Jan. 18, 2019
11	SAEBYOL	An unidentified small vessel	Mar. 2, 2019
12	YU SON	An unidentified small vessel	Mar. 20 and 21, 2019
13	AN SAN 1	Two unidentified small vessels	May 13 and 14, 2019
14	MU BONG 1	An unidentified small vessel	Nov. 13, 2019
15	NAM SAN 8	An unidentified small vessel	Dec. 16 and 17, 2019
16	CHON MA SAN	An unidentified vessel	Jan. 12, 2020

[37] According to the JCG, as of the end of December 2024, a total of 21 suspicious ships and spy ships had been identified since its establishment in 1948. These suspicious ships and spy ships are highly likely to have been involved in serious crimes, including the smuggling of illicit drugs and the illegal entry into and exit from Japan by spies, as exemplified by a spy ship incident that occurred in 2001 in the maritime area southwest of Kyushu. Accordingly, preventing the activities of suspicious ships and spy ships that threaten Japan's public safety and national security remains an important task. JCG, *Maritime Safety Report 2025*, https://www.kaiho.mlit.go.jp/info/books/report2025/html/honpen/2_11_chap6.html

[38] JCG, *FY2024 Enforcement Status on Smuggling and Illegal Entry (Preliminary): Multiple Smuggling Cases via Ship-to-Ship Transfers Using Small Vessels*, https://www.kaiho.mlit.go.jp/info/kouhou/post-1173.html

[39] MOD/SDF, *Suspicion of Illicit Ship-to-Ship Transfer of Cargo on the High Seas by North Korea–Related Vessels*, https://www.mod.go.jp/j/approach/defense/sedori/index.html

The number of cruise ship calls to Japanese ports in 2024 rose to approximately 85% of the pre-COVID-19 peak level of 2018. [40]Amid the gradual recovery in cross-border movements of goods and people, the rising risk of smuggling through ship-to-ship transfers concealed by increasing vessel traffic poses a significant threat.

When illicit ship-to-ship transfer operations are conducted, payments are highly likely to be made through cash transactions that do not involve financial institutions[41] as intermediaries, making it extremely difficult for financial institutions to conduct thorough due diligence. However, financial institutions, etc., may conduct intensified verification in cases where the use of cash by a customer, such as a manufacturing or trading company, for transactions involving industrial products and other goods is detected, or where a rapid increase in the balance of a deposit account followed by cash withdrawals is observed as an indication of such activities.

(3) Persons and Entities Using Opaque Corporate Structures Located in Japan or Elsewhere, Including Those Involving Persons or Entities Designated Under the UNSCRs

With regard to the means of fund transfer used for the provision of funds for WMD proliferation, the use of front companies, joint ventures, etc., has been pointed out, and in this respect, PF is not different from ML/TF. Indeed, the UNSCR 2270 (Paragraph 16) notes that North Korea frequently uses front companies, shell companies, joint ventures, and complex and opaque ownership structures for the purpose of violating sanctions (see Overseas Case 19). The CPFSES Report also notes that North Korea frequently uses methods to conceal beneficial owners in order to gain access to the international financial system, and exploits foreign-based front companies, etc., to conceal real customers, beneficiaries, and the purpose of transaction (see Overseas Case 20).

Although there have been no cleared PF cases in Japan involving persons and entities designated under the UNSCRs, persons and entities that use opaque firms—such as front or subordinate companies, etc., —and those involved in related remittances are considered to pose a threat.

It has also been pointed out that the situation has been worsening due to countries inadequately addressing domestic corporate registration rules, and that such loopholes make compliance with sanctions and “know your customer” onboarding processes and procedures at financial institutions practically impossible.[42]

---

[40] MLIT, *Number of Cruise Passengers Visiting Japan and Cruise Ship Port Calls (2024 Preliminary Figures)*, February 28, 2025, https://www.mlit.go.jp/report/press/port04_hh_000500.html

[41] The FATF defines “financial institutions, etc.” as banks, life and non-life insurance companies, financial instruments business operators, moneylenders, money or value transfer services providers, virtual assets service providers, currency exchange operators, finance lease companies, credit card companies, trust companies, etc.

[42] UNSC, *Midterm report of the Panel of Experts submitted pursuant to resolution 2515 (2020)*, August 28, 2020, https://main.un.org/securitycouncil/en/sanctions/1718/panel_experts/reports

Chapter 3. PF Vulnerabilities and Risks

1. Premises

The FATF PF Guidance defines PF vulnerability as follows:

> *Vulnerability refers to matters that can be exploited by the threat or that may support or facilitate the breach, non-implementation or evasion of PF-TFS* (targeted financial sanctions related to PF).

As described in Chapter 2, PF threats are not limited to those related to persons and entities designated under the relevant UNSCRs. With regard to vulnerabilities, countries are required to conduct evaluations of the weaknesses in the set of measures they have implemented, as well as of the types of financial services and trade transactions that are liable to be exploited for the purpose of PF.

The FATF Fourth Round Mutual Evaluation Report of Japan, published in August 2021, [43] states that Japan is exposed to significant PF vulnerabilities due to factors such as its geographical proximity to North Korea, its major role as an international financial center, and its importance in international trade.

> **—FATF Fourth Round Mutual Evaluation Report of Japan (Extract)—**
>
> 300. The proliferation of DPRK's weapons-of-mass-destruction (WMD) is an existential threat to Japan. In addition, historic illicit activities by DPRK—particularly the abductions of at least 17 Japanese citizens in the late 1970s and early 1980s— continue to buoy public sensitivity toward DPRK-related threats. Consequently, Japan has taken legislative measures and dedicated significant resources to countering DPRK WMD proliferation, including through implementation of PF-related TFS. **Japan is nonetheless exposed to significant vulnerabilities for PF that flow directly or indirectly from its geographic proximity to DPRK (such as maritime trade with other neighboring jurisdictions) and Japan's role as a regional and global financial center, with an important role in international trade.**

2. Internationally Assessed PF Vulnerabilities

The CPFSES Report assesses current PF vulnerabilities as follows:

[43] FATF, *Japan's measures to combat money laundering and terrorist financing*, Aug 30, 2021, https://www.fatf-gafi.org/en/publications/mutualevaluations/documents/mer-japan-2021.html

(1) Analysis of National-level Vulnerabilities

(i) Geographical and Demographic Factors

Geographical proximity to countries subject to UN and national sanctions may create opportunities for illicit networks to transfer funds across borders. Neighboring countries of sanctioned states increase their vulnerabilities by providing vital shipping lanes and trade routes. Countries in East Asia may create illicit financial pathways for North Korea, while countries in the Middle East may do so for Iran. In addition, there are reported cases in which diplomatic personnel and other relevant representatives from countries subject to UN sanctions are involved in sanctions evasion.

(ii) Economic and Trade Factors

PF and sanctions-evasion threat actors target countries that function as international financial centers, as well as those with major ports and logistics infrastructure. Such countries are highly vulnerable to financial abuse and the transportation of dual-use items due to the wide range of services offered by international financial hubs, the scale of global fund flows, and open transportation activities associated with open economies.

(iii) Regulatory Factors

While many countries are developing regulatory frameworks for AML/CFT/CPF, some countries lack regulatory or legal frameworks to apply sanctions obligations and export controls. In unregulated sectors, or sectors with inadequate oversight, such as crypto asset-related entities, complex sanctions evasion is difficult to detect, and where regulations regarding the transparency of beneficial owners are weak, PF risks increase further.

(iv) Other Factors

Countries that produce technologies and goods related to WMD development tend to be vulnerable to PF risks related to the transfer of dual-use items. In addition, countries with large defense sectors require a significant number of organizations to provide materials, products, and services for defense equipment, indicating the possibility that such complex supply chains may be abused

(2) Analysis of Sectoral-level Vulnerabilities

(i) Banking and Other Financial Sectors

Sectors most exposed to PF threats include banking and other financial sectors, including insurers, that engage in cross-border transactions. Threat actors conceal the nature and purposes of fund flows by using various techniques that make transactions difficult to identify, such as the use of multiple accounts, falsified trade documents, and layering of transactions.

(ii) Virtual Assets and Virtual Asset Service Providers

In many countries, virtual assets are used for cross-border fund transfers, including for the purpose of circumventing traditional financial oversight. PF actors are considered to take advantage of the lack of uniform AML/CFT/CPF regulations related to virtual assets and virtual asset service providers across countries. For example, in the laundering of proceeds derived from large-scale virtual asset theft, the combined use of various services and anonymity-enhancing cryptocurrencies (AECs) to further increase the anonymity of transactions has been observed. The use of these new and complex forms of virtual assets makes it extremely difficult to trace transactions and identify the true sources and destinations of remittance.[44]

(iii) New Alternative Payment Infrastructure and Other Sectors

In order to circumvent traditional financial channels related to sanctions enforcement, some state and non-state actors use new alternative payment infrastructure, including the promotion of local- currency payments, alternatives to the Society for Worldwide Interbank Financial Telecommunication (SWIFT) for international payments, and peer-to-peer transactions.

Precious metals and stones traders also represent sectors that can provide means of transferring funds across borders and are vulnerable to PF risks. In addition, sectors such as aviation, IT, maritime, nuclear power, and shipbuilding are analyzed as being likely to be abused for PF due to their relationship with dual-use products and technologies.

3. Japan's Vulnerabilities

In light of the above, Japan's vulnerabilities are overviewed as classified below.

(1) Geographical proximity to North Korea
(2) A major and open financial system in Asia
(3) Concentration of high-technology enterprises and an open economic system

(1) Geographical Proximity to North Korea

Japan's geographical proximity to North Korea is considered to make Japan more vulnerable than other countries to PF risks associated with the flows of goods and people. As Japan is an island nation, cross-border movements of people and goods are conducted through seaports and airports, and

[44] In a report published by the UN Panel of Experts, the panel recommended that UN member countries should implement the guidance concerning crypto assets prepared by the FATF as promptly as possible in order to prevent the provision of funds for WMD proliferation.
UNSC, *Midterm report of the Panel of Experts submitted pursuant to resolution 2627 (2022)*, September 7, 2022, https://main.un.org/securitycouncil/en/sanctions/1718/panel_experts/reports

maintaining trade with other countries, in terms of both quality and quantity, is essential given the scarcity of domestic energy resources. Due to its geographical proximity to North Korea, together with the fact that there have historically been extensive flows of people and goods to and from the Korean Peninsula, Japan is exposed to the risk that PF-related trade and associated fund transfers may be conducted via neighboring countries with close ties to North Korea. In addition, as mentioned in the previous chapter, persons and entities seeking to engage in indirect trade or remittance transactions with North Korea, as well as those seeking to conduct illicit ship-to-ship transfer of goods, may exploit this situation.

(2) A Major and Open Financial System in Asia

As a major global financial center, Japan has a highly developed financial sector in which considerable volumes of financial transactions are conducted. For example, the Tokyo Stock Exchange is one of the major global exchanges in terms of the market capitalization of listed companies.[45] In addition, Japan's financial system, with its extensive nationwide network, provides easy access and enables the rapid and secure transfers of funds.[46] Of the 29 global systemically important banks (G-SIBs) designated by the FSB in 2025, three are Japanese megabanks. Moreover, the total outstanding amount of investment assets in Japan has increased considerably,[47] and, in particular, there is an abundance of financial assets held by individuals.[48]

On the other hand, Japan's globalized and highly advanced economic environment provides persons and entities aiming to engage in PF with a variety of means and methods, as in the case of ML/TF, which may constitute a vulnerability. Among the wide range of transactions, products, and services that exist globally, such persons and entities select those best suited to their purposes. While funds used for PF may originate from either legitimate or illegitimate activities, Japan's position as one of

---

[45] As of the end of October 2025, the total market capitalization of stocks in Japan was approximately 1,168 trillion yen. Japan Exchange Group, Inc., *Month-End Market Capitalization (October 2025)*, https://www.jpx.co.jp/english/markets/statistics-equities/misc/02.html

[46] The number of branches operated by major financial institutions as of the end of March 2024 was 37,181 (including 172 foreign branches), while the number of ATMs installed was approximately 83,000. As a result, access to the financial system is easy. National Public Safety Commission, *the National Risk Assessment-Follow-up Report*, November 2025, https://www.npa.go.jp/sosikihanzai/jafic/nenzihokoku/nenzihokoku.htm

[47] FSA, *Business Opportunities*, https://www.fsa.go.jp/internationalfinancialcenter/en/why-japan/business-opportunities/

[48] As of the end of June 2025, the assets under management (AUM) of asset management companies in Japan increased to approximately 1,059 trillion yen. At the same time, Japan's household financial assets grew to approximately 2,239 trillion yen. The figures for domestic asset management companies' AUM are based on statistics published on the websites of the Investment Management Association of Japan, while the household financial assets figures are calculated by the FSA based on the Bank of Japan's Flow of Funds Statistics.
Investment Management Association of Japan, *Statistics*, https://www.imaj.or.jp/en/statistics/jiaa/, https://www.toushin.or.jp/statistics/statistics/index.html,

Asia's leading international financial centers suggests the possibility that PF-related transactions may be conducted through the Japanese financial system.[49]

(3) Concentration of High-technology Enterprises and an Open Economic System

As Japan is the world's fourth-largest trading nation, it actively conducts trade with Asia, region that is vulnerable to PF activities by North Korea. Accordingly, there is a risk that, under the cover of trade transactions involving Japan, North Korean products may be procured indirectly by other countries, or foreign products may be exported to North Korea via third countries. In addition, as such procurement activities have become increasingly complex and sophisticated, indirect exports via third countries have emerged as a challenge.

Furthermore, as Japan is an industrial center in which companies possessing advanced technologies are concentrated,[50] it has a comparative advantage, relative to other major countries, in the manufacture of finished products—such as transportation equipment and general machinery— the production of which involves highly diverse is limited to a small number of countries.[51] As a result, Japan functions as a trade hub in which parts and semi-finished products (intermediate goods) from various countries are concentrated, giving rise to a vulnerability whereby Japan may be targeted by persons and entities seeking to exploit Japanese companies' high-level technologies and products for WMD development.

Japan engaged in substantial trade with Iran until around 2010. On the import side, the main items traded were oil, gas, and petrochemical products procured from Iranian state-owned companies, while on the export side, the main items were automobiles and electric products. Since 2019, exports to Japan have decreased sharply, and exports of oil and gas from Iran to Japan have been suspended. On the other hand, a certain level of trade relations has been maintained, raising concerns that Japan may continue to be exposed to the risk of PF-related trade and capital transactions conducted via

---

[49] The FSA provides overviews of responses made by business operators under the FSA's jurisdiction as of the end of June 2023, the FATF Fourth Round Mutual Evaluation Report of Japan and the FSA's initiatives related to the report. While it is necessary to keep in mind that the main focus of the report's analysis is ML/TF-related measures, it also points out the risks and challenges by business type, so the analysis is also useful.
FSA, *Announcement of the Publication of "Current Situation and Issues regarding Anti-Money Laundering, Countering the Financing of Terrorism, and Counter-Proliferation Financing Measures" (June 2023)*, June 30, 2023, https://www.fsa.go.jp/news/r4/20230630/20230630.html

[50] The Atlas of Economic Complexity, developed and published by the Growth Lab at Harvard University, is an index that assesses countries' accumulated economic knowledge and capabilities from the perspective of their ability to export diverse, high value-added products. According to this index, Japan ranked between first and third globally throughout the period from 1995 to 2023.
Growth Lab at Harvard University, *The Atlas of Economic Complexity*, https://atlas.hks.harvard.edu

[51] Cabinet Office, *Annual Report on the Japanese Economy and Public Finance*, Chapter 3, Section 1, "Changes in Japan's trade and investment structures."
https://www5.cao.go.jp/j-j/wp/wp-je19/index_pdf.html

neighboring countries that have close relationships with Iran.

Reference 14. Total Value of Iran's Trade with Japan

(Unit: 1 million yen)

		2017	2018	2019	2020	2021	2022	2023	2024
Exports to Japan		400,866	381,068	126,925	3,618	4,178	4,626	4,336	4,378
Item-by-item Breakdown	Petroleum	392,539	370,966	121,658	-	-	-	-	-
	Textile Yarn, Fabrics	2,837	3,229	3,140	2,275	3,118	3,281	2,423	2,264
Imports from Japan		98,468	76,958	7,246	8,561	7,687	6,559	9,062	13,387
Item-by-item Breakdown	Electrical Machinery	13,876	5,066	606	2,871	1,732	1,471	3,213	2,693
	Transport Equipment	34,797	19,017	185	98	44	77	179	156

(Source) MOF, Trade Statistics

4. Complex PF and Sanctions Evasion Typologies

The CPFSES Report lists the following four typologies of complex PF and sanctions evasion schemes and their specific cases.

(1) Use of Intermediaries

PF and sanctions evasion actors abuse multiple intermediaries, such as shell and front companies, financial facilitators, bank accounts, and transshipment through third countries, to conceal real customers, sources of funds, destinations, and purposes (see Overseas Case 21 to 22).

(2) Concealment of BO Information

In order to evade sanctions and access the international financial system, PF and sanctions evasion actors abuse foreign-based front companies, foreigners, unlicensed financial intermediaries, and subsidiaries in regions with loose AML/CFT/CPF regulations to obscure BO information (see Overseas Case 23 to 25).

(3) Use of New Technologies such as Virtual Assets

PF and sanctions evasion actors use anonymity-enhancing technologies, such as mixers, so-called

decentralized finance (DeFi) arrangements, and cross-chain bridges, to conceal the sources and destinations of funds. In addition, funds for WMD programs are being raised through North Korea's unlawful dispatch of IT workers and cyberattacks by entities designated under sanctions (see Overseas Case 13 to 14).

(4) Exploitation of Maritime and Shipping Sectors

Cargo origins and destinations are disguised by the concealment of vessel ID, the manipulation of the Automatic Identification System (AIS), the forging of documents reviewed by customs authorities, and ship-to-ship (STS) transfers (see Overseas Case 26 to 29).

In addition to cases described in this report, the CPFSES Report provides other cases that should also be used for reference.

5. Transactions with High PF Risk

In light of the abovementioned vulnerabilities and the threats explained in the previous chapter, the six types of high-risk transactions that require particular attention in the context of PF are outlined below.

(1) Crypto asset transactions, (2) Non-face-to-face transactions, (3) Overseas remittances, (4) Export transactions related to dual-use items, (5) Transactions related to technology transfers that contribute to the development of WMD, (6) Transactions involving North Korean IT workers

(1) Crypto Asset Transactions

Crypto asset transactions pose relatively higher risks than other transactions due to the difficulty of tracing crypto assets, the existence of technologies that enhance the anonymity of such transactions, and the absence of a global regulatory mechanism for crypto assets. Moreover, as technologies continue to evolve on a daily basis, including the development of new crypto assets and trading methods, supervisors and regulators are likely to be engaged in a “cat-and-mouse game” in catching up with the technology.

(2) Non-face-to-face Transactions

Non-face-to-face transactions pose relatively higher risks than face-to-face transactions, as the absence of direct contact with transaction counterparts limits the availability of information on the counterparts and makes it impossible to assess suspicious aspects of transactions through direct checks of the counterparts’ identification documents, gender, facial features, verbal and physical behavior, etc.

(3) Overseas Remittances

Remittances to countries/regions where persons and entities subject to asset freezing and other measures for their involvement in the development, possession, export, and other activities related to WMDs (nuclear, chemical and biological weapons), as well as to neighboring countries, may include transactions that are equivalent to PF regardless of whether the funds originate from legitimate or illegitimate activities. Accordingly, overseas remittances involve relatively higher risk than other transactions.

(4) Export Transactions Related to Dual-use Items

In Japan, there are high-quality, technologically advanced dual-use items that can be used for both civilian and military applications. When such items are procured for the purpose of WMD development through the use of Japanese infrastructure, it becomes difficult to identify the purposes and routes of import and export, while the destruction of evidence, sanctions evasion, and circumvention become easier. Accordingly, trade in dual-use items is considered to be a PF threat.

(5) Transactions Related to Technology Transfers That Contribute to WMD Development

Japan also possesses a significant amount of information related to advanced technologies used around the world and manufactures cutting-edge, high-performance products. Some of such technological information and products may be diverted to military applications, depending on the method of use.

(6) Transactions Involving North Korean IT Workers

North Korea has reportedly dispatched skilled IT workers around the world to take advantage of demand for specific IT skills and earn large amounts of money through freelance contracts. In Japan, there have been cases in which North Korean IT workers impersonated Japanese nationals, indicating PF risks.

While it is necessary to respond to transactions with high PF risks appropriately according to their risks, the following challenges exist in regard to the confirmation of such transactions.

First, when financial institutions, etc. handle transactions on behalf of persons and entities, they need to implement appropriate confirmation measures to ensure that the beneficiaries of remittance and other transactions are not persons subject to asset freezing or other measures for their involvement in the development, possession, and export of WMD. However, persons who effectively receive the benefits of remittance and other transactions (so-called “ultimate originator” and “ultimate beneficiary”) are not necessarily direct customers of financial institutions, etc. In some cases, such persons may be beneficial owners of customer companies, relatives of customers, or other associated

persons.

In other cases, in order to identify the “ultimate originator”, it may be necessary for financial institutions, etc. to grasp the full details of the transactions that constitute the cause of the remittance transaction in question (e.g., commercial transactions and transfer of liabilities).[52]

Financial institutions, etc. confirm information on the “ultimate originator” by sending inquiries to customers or requiring the submission of documents. However, due to information asymmetry between financial institutions, etc. and customers with respect to the cause of transactions, it is generally difficult to identify the related persons and entities behind complex transaction structures.

[52] For example, in remittance transactions for which receiving agent service providers act as intermediaries, the service providers are direct customers of banks, etc. (persons who request to make remittances). However, if banks, etc. are to identify the ultimate originator, it is necessary to find out multiple debtors hidden behind the presence of the receiving agent service providers in some cases.

Chapter 4. Japan's Initiatives Regarding PF

Japan's major initiatives in response to the abovementioned PF-related threats and vulnerabilities are as described below.

1. Initiatives Regarding Financial Transactions

(1) Economic Sanctions under the FEFTA

The FEFTA is a law intended to contribute to the sound development of the Japanese economy by implementing the minimum necessary controls and coordination for international transactions. Based on UNSCRs and measures taken by major countries, such as the G7, Japan imposes asset-freezing and other measures under the FEFTA on entities and individuals designated as sanctions targets by notifications issued by the MOFA. Specifically, Japan designates persons and entities subject to asset-freezing measures and regulates fund transfers by subjecting payments to, and capital transactions (including deposit contracts, trust contracts, and loan contracts) with, such persons and entities to a licensing requirement.

From the perspective of further enhancing the effectiveness of asset-freezing and other measures with respect to crypto assets and electronic payment instruments, the FEFTA was amended in April and December 2022 to expand the scope of regulation to include transactions involving the transfer of crypto assets and electronic payment instruments from designated persons and entities to third parties.[53]

In addition, in June 2023, in order to ensure the effectiveness of the notices concerning payment and capital transactions regulations, the relevant notices were revised and related FAQs were published to clarify that payments, etc. to entities effectively controlled by designated persons or entities, as well as to persons acting on behalf of, or under the direction of, designated persons and entities, are also comprehensively subject to regulation, thereby clearly preventing transfers of such designated persons and entities.[54]

---

[53] MOF, *Recent Amendments to the FEFTA*, https://www.mof.go.jp/policy/international_policy/gaitame_kawase/gaitame/recent_revised/index.html

[54] Regardless of whether or not the activities of those legal persons and other entities are conducted on behalf of the designated persons or entities via agents, payments to them are subject to the restriction. MOF, *FAQs regarding the Payment and Capital Transaction Notifications Put into Effect on June 1, 2023*, https://www.mof.go.jp/policy/international_policy/gaitame_kawase/gaitame/economic_sanctions/gaiyou.html

Reference 15. Purpose (Article 1 of FEFTA) and Overview of the FEFTA

- The purpose of this Act is to ensure that international transactions develop normally and that peace and security are maintained in Japan and the international community through the implementation of the minimum necessary controls and coordination for international transactions, under the basic principle of free engagement in foreign exchange, foreign trade, and other such international transactions; and in doing so, to help achieve balance of payments equilibrium and currency stability and also to contribute to the sound development of the Japanese economy (Article 1 of the FEFTA).
- The FEFTA is a basic law concerning international transactions (international payments and transactions of various sorts). It also functions as a law for the enforcement of asset-freezing measures for economic sanctions to prevent the abuse of global financial systems and also as a tool to control international transactions for the purpose of ensuring national security or when dealing with economic emergencies.

With regard to North Korea, in December 2022, Japan designated the Lazarus Group as subject to asset-freezing measures for its involvement in North Korea's WMD-related and ballistic missile programs, making the first designation of a cyber-related organization. Subsequently, Japan has designated other North Korean cyber-related organizations, such as Andariel, Bluenoroff, and Kimsuky, as subject to asset-freezing measures. In addition to sanctions based on the UNSCRs, Japan has imposed its own measures against North Korea. These include, for example, the principle-based prohibition of payments to North Korea, as well as the lowering of the notification threshold for the carrying-out of cash, etc. destined for North Korea from amounts exceeding 1 million yen to amounts exceeding 100,000 yen, in order to grasp the actual flows of funds in greater detail. Furthermore, in order to further strengthen measures to prevent transfers of funds to and from North Korea, Japan has prohibited payments and receipt of payments conducted for the purpose of contributing to activities that could facilitate North Korea's nuclear-related programs, and, as measures other than those under FEFTA, has comprehensively prohibited the establishment of branches by Japanese financial institutions, etc. in North Korea, the establishment of correspondent relationships with North Korean financial institutions, etc., and the establishment of branches, etc. by North Korean financial institutions in Japan.

Reference 16. UNSCRs against North Korea and Their Outlines[55]

UNSCRs	Sanctions
(1) Resolution 1695: July 15, 2006 (launch of ballistic missiles on July 5) (2) Resolution 1718: October 14, 2006 (nuclear test on October 9) (3) Resolution 1874: June 12, 2009 (nuclear test on May 25 (2nd time)) (4) Resolution 2087: January 22, 2013 (launch of ballistic missiles on December 12, 2012) (5) Resolution 2094: March 7, 2013 (nuclear test (3rd time)) (6) Resolution 2270: March 2, 2016 (nuclear test on January 6 (4th time) and launch of ballistic missiles on February 7) (7) Resolution 2321: November 30, 2016 (nuclear test (5th time) on September 9) (8) Resolution 2356: June 2, 2017 (launches of ballistic missiles, etc.) (9) Resolution 2371: August 5, 2017 (launches of ICBMs on July 4 and 28) (10) Resolution 2375: September 11, 2017 (nuclear test (6th time) on September 3) (11) Resolution 2397: December 22, 2017 (launch of ICBMs on November 29)	1. Persons ○ Prohibition of persons designated by the UNSC or Sanctions Committee and their family members from entering Japan or transiting through Japan ○ Obligation to repatriate to North Korea any North Korean national who obtains proceeds within a member jurisdiction 2. Goods (trade) ○ Prohibition of imports from North Korea: all weapons, specified natural resources (including coal, iron, iron ore, copper, nickel, silver, zinc, lead, and lead ore), seafood (including fishery rights), textile products, agricultural products, machinery, electrical equipment, earth and stone, wood, vessels, etc. ○ Prohibition of exports to North Korea: all weapons, luxury goods, aviation fuel, new helicopters and vessels, crude oil (upper limit: 4 million barrels or 525,000 tons per year), refined petroleum products (upper limit: 500,000 barrels per year), machinery, electrical equipment, transportation vehicles, iron, steel, and other metals 3. Money (finance) ○ Asset freezing of persons or entities designated by the UNSC or Sanctions Committee ○ Prohibition-in-principle of Japanese financial institutions, etc. opening a branch in North Korea and establishing correspondent relationships with North Korean financial institutions, and of North Korean financial institutions opening a branch in Japan, etc. ○ Prohibition on establishment, maintenance, and operation of joint ventures, etc. with North Korean persons or entities 4. Maritime/air transportation ○ Inspection of North Korea-related cargo in the territory of the Member State, and seizure/disposal of prohibited items ○ Prohibition of aircraft from landing, taking off, or overflying territory if there are reasonable grounds to believe that the aircraft is carrying prohibited items ○ Prohibition of designated vessels, vessels for which there are reasonable grounds to believe that they are owned and managed by designated persons or entities, and vessels for which there are reasonable grounds to believe that they transport prohibited items from North Korea from entering the ports of Member States ○ Prohibition of facilitating or being involved in transshipment to or from North Korean-flagged vessels (“illicit ship-to-ship transfers”)

In September 2025, in line with UNSCR 2231, measures based on past UNSCRs 1737, 1747, 1803, and 1929 concerning sanctions on Iran were announced without delay in Japan. Specifically, the government designated Iran's proliferation-sensitive nuclear activities and activities related to the development of nuclear weapons delivery system as subject to fund transfer prevention measures; designated persons involved in Iran's proliferation-sensitive nuclear activities and nuclear weapons

[55] During the 11 years from 2006 to 2017, 11 UNSCRs imposing sanctions against North Korea were adopted unanimously. In the two years of 2016 and 2017, when the frequency of provocative acts by North Korea, such as nuclear tests and ballistic missile launches, increased, six resolutions were adopted, with the terms of the sanctions tightened.
MOFA, *Sanctions against North Korea Based on UNSC Resolutions*, May 30, 2025, https://www.mofa.go.jp/mofaj/gaiko/unsc/page3_003268.html

development as subject to asset-freezing and other measures; designated industries as subject to measures prohibiting Iranian investment in nuclear and other technologies; and designated activities related to the supply of large conventional weapons to Iran as subject to fund transfer prevention measures, thereby regulating relevant fund transfers under the FEFTA.

Reference 17. Major UNSCRs against Iran and Their Outlines

UNSCRs (History of resolutions up to Resolution 2231)	Details of Sanctions (Measures Taken Before Resolution 2231)
(1) Resolution 1696: July 31, 2006 (Requesting Iran to cease all uranium enrichment-related and spent nuclear fuel reprocessing activities and accept IAEA verification) (2) Resolution 1737: December 23, 2006 (Requiring Iran to cease its proliferation-sensitive nuclear activities and all UN members to prohibit the supply of goods that may contribute to Iran's uranium enrichment, spent nuclear fuel reprocessing, and heavy water-related activities, and to the development of nuclear weapons delivery systems, and to take asset freezing, fund transfer prevention, and other measures against certain persons and entities) (3) Resolution 1747: March 24, 2007 (Adding new persons and entities to the scope of those subject to asset freezing and other measures stipulated in Resolution 1737 and mandating measures such as prohibiting the procurement of weapons and related materials from Iran) (4) Resolution 1803: March 3, 2008 (Adding 12 new entities and 13 persons to the scope of those subject to asset freezing and other measures stipulated in Resolution 1737, designating additional materials and technologies that may contribute to Iran's nuclear activities and missile development and that should be subjected to the prevention of supply to Iran, and mandating the prevention of designated persons' entry and transit) (5) Resolution 1835: September 27, 2008 (Calling on Iran to comply with relevant UNSCRs) (6) Resolution 1929: June 9, 2010 (Adding 40 new entities and one person to the scope of those subject to asset freezing and other measures stipulated in Resolution 1737, prohibiting Iran's investment in nuclear materials, technologies etc., and mandating measures to prevent fund transfers related to the supply of large conventional weapons, etc. to Iran) (7) Resolution 2231: July 20, 2015 (Ending sanctions against Iran based on resolutions including (1) to (6) above, requiring all UN members to prevent the transfer of materials and technologies related to Iran's nuclear activities, prohibit Iran's investment in nuclear materials and technologies, and prevent the supply of large conventional weapons to Iran, allowing them to permit these activities if prior UNSC approval is given, and mandating asset freezing, fund transfer prevention, and other measures for certain persons and entities.)	1. Persons Obligation to prevent entry or transit of persons involved in support for Iran's proliferation-sensitive nuclear activities and development of nuclear weapons delivery systems 2. Goods (trade) ○ Prohibition of the supply, sale, or transfer to Iran of all products, materials, equipment, and technologies that may contribute to uranium enrichment, spent nuclear fuel reprocessing, heavy water-related activities, and the development of nuclear weapons delivery systems ○ Compliance with notification to the Sanctions Committee within 10 days after the transfer of nuclear and ballistic missile-related goods that are not subject to embargo ○ Prohibition on the procurement of nuclear and ballistic missile-related goods, weapons, and related materials from Iran ○ Prohibition on the supply, sale or transfer to Iran of tanks, armored fighting vehicles, large artillery systems, combat aircraft, attack helicopters, warships, missiles or missile systems ○ Confiscation and disposal of goods subject to the prohibition of supply, sale, transfer, and export 3 Finance ○ Prevention of the supply of technical support, training, financial support, investment, mediation and other services and the transfer of financial resources and services to Iran regarding the supply, sale, transfer, production, and use of prohibited products, materials, goods, and technologies ○ Freezing the assets of persons and entities involved in Iran's nuclear and ballistic missile-related activities ○ Request for monitoring of public financial assistance for trade with Iran ○ Request for monitoring of transactions with Iranian financial institutions ○ Prohibition of Iran's investment in any commercial activities related to uranium mining and the production and use of nuclear materials and technologies ○ Request for a ban on Iranian banks' opening of new branches, subsidiaries, and representative offices, establishment of joint ventures, and maintenance of ownership and correspondent relationships. ○ Request for a ban on financial institutions' opening of representative offices, subsidiaries, and bank accounts in Iran 4 Others ○ Request for the monitoring and prevention of special education and training that may contribute to Iran's proliferation-sensitive nuclear activities and nuclear weapons delivery system development ○ Cessation of Iran's activities related to ballistic missiles capable of delivering nuclear weapons (including launches using ballistic missile technology) and prevention of technology transfer and technical assistance for such activities to Iran ○ Request for inspection on vessels entering and leaving Iran ○ Prohibition on the provision of refueling services to Iranian-owned or Iranian-contracted vessels suspected of transporting goods subject to embargoes or procurement bans. ○ Duty of care regarding business with Iranian organizations suspected of contributing to nuclear or missile activities, etc.

In response to Russia's aggression against Ukraine that began in 2022, Japan, along with other G7 countries, has implemented asset-freezing measures and strictly regulated direct investment in, and services transactions with, the Government of the Russian Federation and Russian companies under

the FEFTA.

In order to ensure the effectiveness of asset-freezing and other measures under the FEFTA, financial institutions, funds transfer service providers, electronic payment instruments service providers, etc. that handle overseas remittances and cross-border transactions are required to confirm whether foreign exchange transactions related to customer payments, etc. are in compliance with the FEFTA (hereinafter referred to as the "obligation to implement confirmations") and to verify the identities of customers (hereinafter referred to as the "obligation to verify customer identities").

In addition, based on the FEFTA, Japan conducts inspections of financial institutions, etc. that provide foreign exchange services with respect to their compliance with laws and regulations related to asset-freezing and other economic sanctions.

Furthermore, on April 1, 2024, the "Requirements for Financial Sanction Compliance for Foreign Exchange Transactions Service Providers", which obligate banks, etc., funds transfer service providers, electronic payment instruments service providers, etc., and currency exchange operators, etc. to develop systems for implementing asset-freezing and other measures, entered into force. As a result, financial institutions and other entities subject to these requirements are required to conduct risk management activities to ensure the appropriate implementation of asset-freezing and other measures, including appropriate risk assessments related to such measures and the development and implementation of procedural manuals for risk mitigation.

In response, it was decided that the Foreign Exchange Inspection Guidelines would be reorganized to present the concepts and interpretations of the FEFTA and its related regulations, including the Requirements for Financial Sanction Compliance on Foreign Exchange Transaction Service Providers, and to present the guidelines for inspectors conducting foreign exchange inspections. These reorganized guidelines are published as the "Guidelines for Foreign Exchange Transaction Service Providers on Compliance with the FEFTA and Its Regulations, etc." (hereinafter referred to as the "Foreign Exchange Guidelines")[56], in order to ensure that foreign exchange transaction service providers comply with their various obligations. Since April 2024, when the Foreign Exchange Guidelines came into effect, the government has launched new foreign exchange inspections to assess the development of frameworks for governance and internal controls related to economic sanctions compliance. Since then, the government has conducted a total of 17 outreach sessions on the Foreign Exchange Guidelines to promote a better understanding of Guidelines among foreign exchange transaction service providers.

[56] MOF, *Guidelines for Foreign Exchange Transaction Service Providers on Compliance with the FEFTA and Its Regulations, etc., July 2024*, https://www.mof.go.jp/policy/international_policy/gaitame_kawase/inspection/20240718_0.pdf

Reference 18. Number of Entities on Which Foreign Exchange Inspection Was Conducted in Recent Years

Program year[57]2024:123; program year 2023: 105; program year 2022: 110;
program year 2021: 106; program year 2020: 24; program year 2019: 78

"Frequently Asked Questions Concerning Guidelines for Foreign Exchange Transactions Service Providers on Compliance with the FEFTA and Its Regulations, etc.," published by the MOF in July 2025, indicated the following situations as possible cases of violation, evasion, and circumvention of the economic sanctions. It is useful to conduct intensive checks, as appropriate to the risk, from the viewpoint of whether the transaction under examination corresponds to any of these situations.

- The customer is reluctant to provide necessary information, or provides vague or inconsistent information.
- Customers, remittance destinations, business partners, and their beneficial owners are subject to sanctions in other countries. Negative information concerning these persons and entities is reported (e.g., violation of import or export regulations, ML, fraud or other criminal records).
- The customer is located in, or has connections with, a country/region of concern or a high-risk country/region.
- A customer or counterparty appears to be operating as a fund-remittance business or a payable-through account. In particular, such accounts involve rapid movements of high-value transactions with small end-of-day balances without clear business reasons.
- Accounts or transactions involve companies with potentially opaque ownership structures, front companies, or shell companies, etc., such as companies with insufficient capitalization or other indicators of shell companies. There are long periods of account dormancy followed by a sudden surge in activity.
- A trade entity is registered at an address that is likely to be a mass registration address, such as high-density residential buildings, post office box addresses, commercial buildings, or industrial complexes, especially where there is no reference to a specific unit.
- A transaction request is made by a customer who has the same telephone number or IP address as another customer whose transaction request was previously declined.
- The customer's website is extremely simple, and the actual status of the business described therein is unclear.
- Funds are transferred through tax haven countries or special purpose companies (SPCs), making it unclear who the beneficiaries are.
- The transaction counterpart differs from the settlement counterparty without a rational reason.

[57] The period of the program year is from July to June in the following year.

Payment for imported commodities is made by an entity other than the consignee, without clear economic justification, such as by a shell or front company not involved in the trade transaction.

- With respect to payments between a corporation and an individual, there is no rationality between the relationship of the parties and the nature of the payments (e.g., a remittance from a corporation to an individual for the purpose of providing living expenses).
- A customer engages in complex trade transactions involving numerous third-party intermediaries in lines of business that do not accord with the customer's business profile. Goods are shipped in a complex or circuitous manner without economic rationality.
- A company and its affiliates use internal ledgers to clear payment balances among themselves in order to eliminate the need for frequent remittances.
- A person clears payments with multiple parties through accounts within a short period of time, or repeatedly clears payments with the same parties for unclear purposes.
- A customer withdraws funds in a manner inconsistent with the stated purpose of the business relationship identified by the financial institution in relation to an inbound remittance or other transaction. Immediately prior to settlement, there is a deposit suspected to have been made on behalf of a third party.
- A customer modifies some information related to a rejected remittance and attempts to make the remittance again. Payments are made via routes other than the banks or remittance routes normally used.
- A company clears payments of an unusual amount or for purposes that are inconsistent with the customer's industry category or ordinary transactions.

Finally, financial institutions, etc. need to pay attention to the risk of secondary sanctions imposed by the United States in relation to PF. Secondary sanctions are, in principle, targeted at transactions conducted directly or indirectly between non-U.S. persons and designated persons or entities and that have no nexus with the United States, and are intended to effectively deter such transactions by indicating the risk of being subject to the same disadvantage as designated persons or entities if such transactions are conducted. It is also necessary to appropriately keep track of the specifics of the sanctions imposed by the United States.

The government should continue its efforts to publish cases of violation and issue alerts, and, while receiving feedback from private-sector business operators, continuously update the methods of disseminating such information and consider further measures that may be taken.

(2) Regulation of Domestic Transactions under the Terrorist, etc. Assets Freezing Act

International terrorist organizations and persons involved in WMD-related programs conduct activities across national borders, and if adequate measures are not implemented in a particular country, that

country may become a “loophole” in CTF measures.

Based on this concept, Japan has regulated international flows of funds, etc. between residents (persons who have an address, etc. in Japan) and non-residents under the FEFTA as part of its CTF measures. On the other hand, domestic transactions between residents had not previously been subject to regulation. However, in November 2014, the (former) Terrorist, etc. Assets Freezing Act (which entered into force on October 5, 2015) was enacted, thereby bringing domestic transactions within the scope of regulation.

With regard to CPF measures as well, while cross-border transactions between residents and non-residents had been regulated under the FEFTA, domestic transactions between residents had not been subject to regulation, including under the former Terrorist, etc. Assets Freezing Act.[58] Accordingly, in December 2022, the Act to Partially Amend the Act on Special Measures Concerning the Asset-Freezing of International Terrorists Conducted by Japan Based on United Nations Security Council Resolution 1267, etc., to Deal with International Transfers of Unlawful Funds (Act No. 97 of 2022) (the Act to address the FATF Recommendations) was passed, and PF-related domestic flows of funds between residents were brought within the scope of regulation.

2. Import and Export Controls

(1) Prohibition of Imports and Exports Under the FEFTA, etc.

With regard to North Korea, in addition to prohibitions on the import and export of specified goods based on the UNSCRs, Japan has implemented the following three measures as its own measures, similar to financial measures:

(i) Prohibiting of the import of all goods originating in or shipped from North Korea
(ii) Prohibiting of the export of all goods destined for North Korea
(iii) Sanctions measures, including restrictions on the import and export of payment instruments, etc.

In addition, in order to prevent the evasion of sanctions related to import and export controls prescribed under the FEFTA, strict law enforcement is carried out by customs authorities pursuant to the Customs Act (Act No. 61 of 1954).

Furthermore, from the perspective of preventing indirect exports to North Korea or indirect imports

[58] In this respect, the FATF Fourth Round Mutual Evaluation Report of Japan pointed out the following deficiency: measures have not been put in place with respect to domestic transactions conducted by residents in Japan who are involved in PF and who have been designated by the UNSCRs, and as a result, if residents in Japan are designated in the future, Japan will not be able to deal with PF.

into Japan via third countries, Japan implements the following measures:

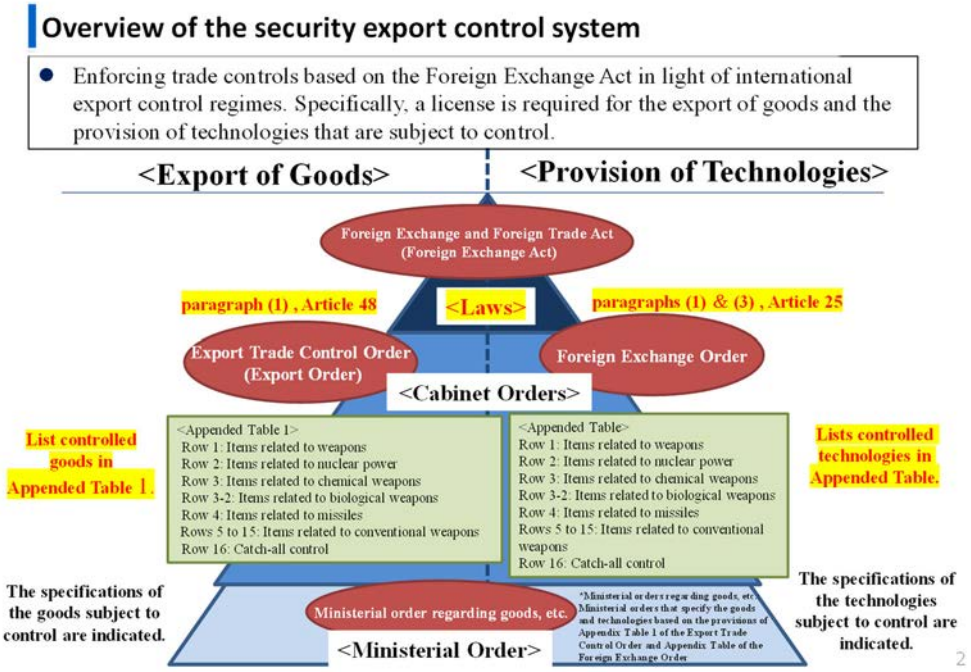
(i) Strict examination and inspection of the origins of goods imported from neighboring countries by means of certificates of origin, etc.
(ii) Strict examination and inspection of final destinations of goods exported to neighboring countries through the review of contracts and other related documents.

In addition to these measures, close information sharing and cooperation are carried out among relevant government agencies and organizations, and efforts are made to enhance information gathering from related business operators, such as customs brokers and shipping agents.

(2) Security Export Control under the FEFTA

With regard to dual-use items and technologies, export controls are being promoted under international frameworks (international export control regimes), mainly by developed countries [59], and Japan controls the export of goods and the provision of technologies under the FEFTA.

Reference 19. Overview of the Security Export Control System



(Source) METI

[59] The countries that are participating in international export control regimes and that are enforcing export controls strictly are as follows [a total of 27 countries]
Argentina, Australia, Austria, Belgium, Bulgaria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Ireland, Italy, the ROK, Luxemburg, Netherlands, New Zealand, Norway, Poland, Portugal, Spain, Sweden, Switzerland, the United Kingdom, and the United States.

Dual-use items and technologies that pose a particularly high risk of being used for the development of WMD are subject to "list control." Specifically, goods are specified in Appended Table 1 (Items 1 to 15) of the Export Trade Control Order, and technologies are specified in the Appended Table (Item 1 to 15) of the Foreign Exchange Order. When exporting goods or providing technologies that fall under these categories, a license must be obtained. In addition, even where goods or technologies do not fall under list control, if there is a risk that may be used for the development of WMD, such transactions are subjected to "catch-all control"[60] and require a license from METI.

Furthermore, as of October 9, 2025, a review of complementary export controls (including the implementation of the catch-all control for conventional weapons) was conducted. As a result, even exports to destinations other than Group A countries[61] or UN arms embargo countries[62] now require a license, limited to specific items, where there is a risk that they may be used for the development of conventional weapons. In addition, even for exports to Group A countries, a license is required where there is a risk of diversion to countries/regions of concern and where the exporter has received a notification from METI.

Moreover, control measures regarding the provision of technologies have been strengthened. METI has traditionally controlled not only the provision of technologies subject to FEFTA regulations to foreign countries, but also the provision of such technologies from residents to non-residents within Japan by treating such provision as an "export" (so-called "deemed export" control), given the high likelihood that such non-residents would ultimately depart from Japan. Since May 2022, METI has clarified that the provision of such technologies to residents who fall under specified categories—namely, those deemed to be under strong influence from non-residents[63]—also falls within the scope of deemed export control.

---

60 "Catch-all control" refers to a system that requires exporters to obtain permission for exporting goods or providing technologies from the METI when they have learned of the risk that the goods that they plan to export or the technologies that they plan to provide may be used for the development, production, use or storage of WMD or for the development, production, or use of conventional weapons, or when they have been informed by the Minister of a notification of the requirement for application for permission. METI, *Catch-all Control*, https://www.meti.go.jp/policy/anpo/catchall.html

61 The countries that are participating in international export control regimes and that are enforcing export controls strictly are as follows [a total of 27 countries]
Argentina, Australia, Austria, Belgium, Bulgaria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Ireland, Italy, the ROK, Luxemburg, Netherlands, New Zealand, Norway, Poland, Portugal, Spain, Sweden, Switzerland, the United Kingdom, and the United States.

62 "The UN arms embargo countries" refer to Afghanistan, the Central African Republic, the Democratic Republic of the Congo, Iraq, Lebanon, Libya, North Korea, Somalia, South Sudan, and Sudan.

63 Specifically, the specified categories include the following persons:(i) persons who are under the control of foreign governments and foreign legal persons based on employment or other contracts; (ii) persons who are under the effective control of foreign governments based on economic interests; (iii) persons who are in Japan under instructions from foreign governments.

3. Other Related Legal Frameworks

(1) Act on Prevention of Transfer of Criminal Proceeds (Verification at the Time of Transaction and Reporting of Suspicious Transactions, Notification Obligation)

The Act on Prevention of Transfer of Criminal Proceeds (Act No. 22 of 2007) was enacted in light of the FATF's "40 Recommendations" in 2003[64] and changes in ML methods. The Act was established based on the entirety of the former Act on Identity Verification of Customers by Financial Institutions, etc. and Prevention of Unauthorized Use of Deposit Accounts (Act No. 32 of 2002), as well as parts of the Act on Punishment of Organized Crimes and Control of Proceeds of Crime (Act No. 136 of 1999). By ensuring that specified business operators appropriately implement measures such as verification at the time of transaction, preparing and preserving records, and reporting of suspicious transactions in accordance with the Act on Prevention of Transfer of Criminal Proceeds, some effects of deterring or countering PF has emerged as a secondary consequence.

(i) Verification at the Time of Transaction and Reporting of Suspicious Transactions

As AML/CFT measures, basic requirements concerning verification at the time of transaction and related obligations are prescribed under relevant laws and regulations, including the Act on Prevention of Transfer of Criminal Proceeds and the FEFTA. Specifically, under the Act on Prevention of Transfer of Criminal Proceeds, business operators such as financial institutions that are designated as "specified business operators" are obligated to conduct identity verification, etc. (including verification of beneficial owners in the case of legal persons) when conducting specified transactions.[65]

[64] The "40 Recommendations" were further revised in February 2012 into the new "40 Recommendations" with the aim of more effectively addressing threats such as the proliferation of WMDs.

[65] Transactions subject to the obligation of verification at the time of transaction prescribed in Article 4, paragraph (1) of the Act on Prevention of Transfer of Criminal Proceeds.

Reference 20. Examples of Specified Business Operators and Specified Transactions Requiring Identity Verification

Specified Business Operator	Specified Transactions
Financial institutions, etc.	Opening of a deposit or savings account Large cash transactions exceeding 2 million yen Cash remittance exceeding 100,000 yen
Credit card companies	Conclusion of a credit card contract
Finance lease companies	Conclusion of a finance lease contract in which the lease payment per occasion exceeds 100,000 yen * Excluding contracts under which a lease company leases goods it already possesses to its customer
Real estate brokers	Conclusion of a real estate sales contract, or provision of intermediary or agency services therefor
Dealers in precious metals and stones	Conclusion of a sales contract for jewelry or precious metals where payment exceeds 2 million yen in cash
Judicial scriveners Certified administrative procedures legal specialists Certified public accountants Tax accountants	Conclusion of a contract to act as agent for the following specified entrusted acts -Acts or procedures related to the sale and purchase of residential land or buildings -Acts or procedures related to the incorporation or merger of companies, etc. -Management or disposal of cash, deposits, securities, or other assets exceeding 2 million yen * Excluding the conclusion of a voluntary guardianship contract

(Reference) Website of the Public Relations Office, Government of Japan.
https://www.gov-online.go.jp/useful/article/201610/1.html

Under the Act on Prevention of Transfer of Criminal Proceeds, specified business operator is obligated to promptly file a with the administrative authority if they find that assets received from a customer are suspected of being criminal proceeds, or that a customer is suspected of engaging in ML in the relevant transaction (the “suspicious transaction reporting system”). Information on suspicious transactions is aggregated at the National Public Safety Commission through administrative authorities or competent ministers, then organized and analyzed, and information deemed useful for investigation, etc. of ML-related crime is provided to investigative authorities.

(ii) Notification Obligation (Travel Rule)

FATF Recommendation 16 (Payment Transparency) and its Interpretative Note provide for a rule whereby financial institutions engaged in wire transfers are required to provide notification of originator and beneficiary information (the so-called travel rule) in order to prevent persons who have obtained criminal proceeds and terrorists, etc. from moving their funds freely, and to make it possible to trace the assets involved in transactions when the assets are suspected of being criminal proceeds. In June 2025, Recommendation 16 and its Interpretative Note were revised with a focus on technology neutrality, etc., in light of the structural development of the payment market through the emergence of new technologies.

Traditionally, Recommendation 16 required the ordering financial institution to provide the originator and beneficiary information to the beneficiary financial institution. However, as part of measures addressing crypto asset transactions, FATF Recommendation 15 was revised in October 2018 and its Interpretive Note was amended in June 2019, following which countries were required to introduce and implement the travel rule, obliging crypto asset exchange service providers to transmit originator and beneficiary information for transfers of crypto asset and stablecoins.

In Japan, following a request from FSA, the travel rule for crypto asset transactions was first introduced in April 2022 as a form of self-regulation by an industry association, the Japan Virtual and Crypto Assets Exchange Association (JVCEA). Subsequently, in December 2022, the Act on Prevention of Transfer of Criminal Proceeds was amended to impose the travel rule obligations on crypto asset exchange service providers, etc.[66] and the amendment entered into force in June 2023. Specifically, crypto asset exchange service providers, etc. are required to transmit originator and beneficiary information upon transfers of crypto assets and electronic payment instruments (stablecoins), and to prepare and retain records of the information transmitted and the information received. Based on the principle of reciprocity, 20 jurisdictions were initially designated[67] and as of August 2025, 58 jurisdictions were covered[68].

[66] The obligation also applies to electronic payment instruments service providers.
[67] The United States, Albania, Israel, Canada, Cayman Islands, Singapore, Gibraltar, Serbia, Germany, Bahamas, Bermuda, the Philippines, Venezuela, Malaysia, Mauritius, Liechtenstein, Luxembourg, the ROK, Hong Kong, and Switzerland.
[68] Public Notice No. 1 of April 2024 issued by the FSA and the MOF (adding eight jurisdictions), and Public Notice No. 1 of June 2025 issued by the FSA and the MOF (adding thirty jurisdictions).

Reference 21. Anti-cybercrime Measures and Regulations on Crypto Asset Transactions
➢ With regard to countermeasures against cyberattacks, in April 2022, the National Cyber Unit was established as a governmental investigative organization responsible for responding to serious cyber incidents, in light of the extremely serious threats existing in cyberspace. In April 2024, it was upgraded and reorganized as the National Cyber Department.[69] The National Cyber Department steadily conducts investigations in cooperation with prefectural police and foreign investigative agencies. In addition, the police cooperates with companies possessing cutting-edge technologies to comprehensively analyze information provided by business operators and share the results with those operators. Efforts are also underway to enhance the overall level of security for IT users through public-private cooperation. ➢ When the police identifies a crypto asset transaction account that is used, or suspected of being used, for unlawful fund transfers related to internet banking fraud, communications fraud, ransomware incidents, crypto asset-related unlawful fund transfers, or SNS-based investment or romance fraud, they promptly contact the relevant crypto asset exchange service provider and requests the provider to consider freezing the account.

(2) Schemes for Increasing the Transparency of Legal Persons

Reports of the Panel of Experts have recommended tightening regulation on the registration of companies with opaque activities in order to increase the transparency of legal persons.[70] In addition, the FATF Recommendations and requests from financial institutions, etc. call for initiatives to enhance the transparency of legal persons from the perspective of preventing their abuse for ML/TF purposes. In response to these requests, Japan has developed institutional frameworks to verify beneficial ownership information of legal persons as follows:

- Beneficial owners are defined, and specified business operators are obligated to verify the identity information of beneficial owners when their customers, etc. are legal persons.
- Specified business operators that provide services such as business address or facilities, communication means, or administrative addresses for legal persons, etc. are obligated, upon concluding service contracts, to conduct verification at the time of transaction and to prepare and retain verification records and transaction records, etc.
- When certifying articles of incorporation upon the incorporation of a stock company, a general incorporated association, or general incorporated foundation, notaries are obligated to have applicants report details including the name of the person who will become the beneficial owner

[69] NPA, *Overview of the Threat Landscape in Cyberspace in the First Half of FY* 2025, https://www.npa.go.jp/publications/statistics/cybersecurity/data/R7kami/R07_kami_cyber_jyosei.pdf
[70] UNSC, *Final report of the Panel of Experts submitted pursuant to resolution 2515(2020)*, March 4, 2021, https://main.un.org/securitycouncil/en/sanctions/1718/panel_experts/reports

and whether that person is a member of an organized crime group, an international terrorist, or a person involved in a WMD-related program.

- In order to enable the continuous identification of beneficial owners after incorporation, a scheme is stipulated whereby a commercial registry office, upon request from a stock company, keeps a document containing information on the beneficial owner of the stock company and delivers a copy of that document.

As a recent development, as part of efforts to continuously identify beneficial owners after incorporation, the MOJ introduced the beneficial ownership of legal persons list system, under which a commercial registry office keeps a document prepared by a stock company (including a special limited liability company) containing information on its beneficial owner and delivers a copy thereof, and began operating the system in January 2022. The Strategic Policy also states that "the Government will promote the use of 'the beneficial ownership of legal persons list system' ... and consider developing a framework that enables centralized, continuous, and accurate identification of beneficial owners of legal persons," and the government is promoting initiatives to enhance the transparency of legal persons in Japan. Furthermore, while the incorporation of certain legal person, such as stock companies, in Japan requires notarization of the articles of incorporation, the MOJ introduced a new mechanism in June 2023 whereby in the notarization procedure, a notary examines whether the person who will become the beneficial owner of the legal person is not a person involved in a WMD-related program.

(3) Immigration Control and Refugee Recognition Act (Cabinet Order No. 319 of 1951)

Japan has imposed broad restrictions on the movement of people to and from North Korea. The specific measures are as follows:

- Principle-based prohibition on the entry of persons of North Korean nationality into Japan
- Principle-based prohibition on re-entry into Japan, with North Korea as the destination, by officials of the North Korean authorities and others residing in Japan
- Request for self-restraint from traveling to North Korea
- Principle-based suspension of travel to North Korea by Japanese national public officials
- Principle-based prohibition on the landing of crew members, etc. of North Korean-flagged vessels, and principle-based prohibition on re-entry into Japan, with North Korea as the destination, by foreign residents in Japan whose sentences for violations of measures against North Korea have become final
- Prohibition on re-entry into Japan, with North Korea as destination, by foreign nationals residing in Japan who are nuclear or missile technology experts

(4) Act on Prohibition of Entry of Specified Ships into Ports / Act on Cargo Inspections

Based on the Act on Special Measures Concerning Prohibition of Entry of Specified Ships into Ports (Act No. 125 of 2004), Japan implements measures to prohibit the entry into Japanese ports of all North Korean-flagged vessels (including those for humanitarian purposes), all vessels that have called at ports in North Korea (including Japan-flagged vessels), and vessels designated as subject to sanctions based on UNSCRs, etc. In addition, Japan prohibits chartered flights to and from North Korea and denies permission for aircraft suspected of carrying prohibited items to take off from, land on, or overfly Japanese territory.

With regard to cargo, Japan implements inspection measures for specified cargo related to North Korea based on the Act on Special Measures Concerning Cargo Inspections Conducted by the Government Taking into Consideration United Nations Security Council Resolution 1874 (Act No. 43 of 2010) and other relevant laws and regulations, in order to ensure inspections required under the relevant UNSCRs.

The MOFA, together with the G7 and other like-minded countries, has been engaged with China regarding the issue of oil tankers suspected of transporting oil to North Korea operating in China's territorial waters.[71] In addition, at the Japan-China High-Level Consultation on Maritime Affairs held in October 2024,[72] Japan once again strongly requested China to address illegal operations by Chinese fishing vessels in the waters around the Yamato Bank in the Sea of Japan and emphasized the importance of the full implementation of UNSCRs related to sanctions against North Korea, including measures to address illicit maritime activities, such as ship-to-ship transfers.

(5) Other AML/CFT-related Laws and Regulations

Other laws and regulations related to AML/CFT measures include the following. While these laws primarily address ML and TF, their risk-mitigation measures are also considered useful as reference for mitigating PF risks.

- Act on Punishment of Organized Crimes and Control of Proceeds of Crime (Act on Punishment of Organized Crimes):

  This Act specifies instances of serious crime, etc. as predicate offences of the crime of concealment of proceeds of crime, etc., and provides for the confiscation of proceeds of crime, etc. and the collection of a sum of equivalent value that may be performed in lieu of the

[71] Reports by the Panel of Experts have indicated that multiple oil tankers often withdraw to waters near Sansha Bay between instances of illegal navigation.
UNSC, *Final report of the Panel of Experts submitted pursuant to resolution 2680 (2023)*, March 7, 2024, https://main.un.org/securitycouncil/en/sanctions/1718/panel_experts/reports

[72] MOFA, *The 17th Japan–China High-Level Consultation on Maritime Affairs (Outcome)*, October 23, 2024, https://www.mofa.go.jp/mofaj/press/release/pressit_000001_01303.html

confiscation. The Act was amended in 2025 to develop procedures for the execution of judicial decisions on the confiscation of crypto assets as criminal proceeds and direct freezing of such assets.

- Act Concerning Special Provisions for the Narcotics and Psychotropics Control Act, etc. and Other Matters for the Prevention of Activities Encouraging Illicit Conducts and Other Activities Involving Controlled Substances through International Cooperation (Act No. 94 of 1991) (Anti-Drug Special Provisions Act):
  This Act designates certain drug-related crime as predicate offences for crimes such as concealment of proceeds of drug-related crime, etc., and provides for the confiscation of such proceeds of drug-related crime, etc. and the collection of a sum of equivalent value that may be performed in lieu of the confiscation.
- Act on Punishment of Financing of Offences of Public Intimidation (Act No. 67 of 2002)" (Act on Publishment of Terrorist Financing):
  This Act provides for the punishment of the collection, provision, etc. of terrorist funds.

4. Major Initiatives Relating to Coordination among Ministries and the Private Sector

(1) Major Initiatives Relating to Inter-ministerial Coordination

CPF measures span, and are interrelated with, fields such as finance and trade that fall under the jurisdictions of multiple ministries and agencies. Accordingly, close cooperation among ministries and agencies in implementing CPF measures is extremely important. Specific examples of such coordination are described below.

(i) Initiatives Regarding UNSCRs and the FATF

- The MOFA shares information necessary for implementing measures such as asset-freezing prescribed in the UNSCRs regarding North Korea with relevant ministries and agencies that implement measures under the FEFTA and the Terrorist, etc. Assets Freezing Act.
- In order to implement measures such as asset-freezing under the FEFTA without delay, the MOF, METI, and MOFA prepared an agreement among the relevant ministries and agencies stipulating that, when persons or entities are additionally designated under the UNSCRs, the necessary measures will be implemented within 24 hours from the time of designation (including advance notification to financial institutions, etc.). This framework has been in operation since May 31, 2021. (Since the start of the operation, there have been no additional designations under UNSCR 1718. In September 2025, with the reapplication under UNSCR 2231 of past UNSCRs concerning Iran, including UNSCR 1737, the MOFA issued a public notice on the same day designating 78 entities and 43 individuals.)

- Taking into account the findings of the FATF Fourth Round Mutual Evaluation Report of Japan, the MOF and the FSA conduct "joint inspections," under which the MOF's foreign exchange inspections and the FSA' AML inspections are conducted jointly, with a view to sharing inspection officials' expertise and inspection information and ensuring compliance with relevant related laws and regulations by financial institutions in an effective and efficient manner while reducing their burden. In addition, since December 2018, the MOF has introduced off-site monitoring in order to regularly and continuously understand the status of financial institutions' foreign exchange operations and internal control frameworks and to utilize such information for inspection planning (selection of institutions to be inspected), by annually collecting reports pursuant to Article 55-8 of the FEFTA and Article 15 of the Act on Prevention of Transfer Criminal Proceeds.

(ii) Initiatives Regarding North Korean IT Workers and Cyberattacks

- With regard to the activities by North Korean IT workers, the MOFA, the NPA, the MOF, and the METI issued the "Alert for Companies on North Korean Information Technology Workers" in March 2024. In light of the increasing sophistication of their methods and the expansion of their activities, the alert was updated in August 2025 to inform relevant companies and organizations of specific tactics used by North Korean IT workers, such as forgery of identification documents and impersonation of third parties, and to call for measures including the strengthening of identity verification procedures.[73]
- In response to cyberattacks targeting crypto asset-related companies by the cyberattack group known as Lazarus, which is considered to be subordinate to the North Korean authorities, as well as by the North Korea-backed cyberattack group "TraderTraitor," the NPA, the NISC, and the FSA issued an alert, providing specific tactics and mitigation measures so that organizations and companies that may become targets can implement appropriate security measures.[74]

(iii) Other Initiatives

- As part of monitoring and surveillance activities, the MOD/SDF collect information on vessels suspected of violating the UNSCRs by using JMSDF vessels and other assets. The collected and analyzed information is shared in a timely and appropriate manner with relevant ministries and agencies through Japan Joint Staff. In addition, when activities

[73] NPA, the MOFA, the MOF, and the METI, *Alert on North Korean IT workers for Companies and Other Organizations*, August 27, 2025, https://www.mof.go.jp/policy/international_policy/gaitame_kawase/press_release/2statement.pdf

[74] NPA, NISC, and FSA, *Alert: Cyberattack by TraderTraitor, a cyberattack group linked to North Korea*, December 24, 2024, https://www.npa.go.jp/bureau/cyber/koho/caution/caution20241224.html

suspected of illicit maritime activities, including ship-to-ship transfers prohibited under the UNSCRs, are detected by JMSDF vessels or other assets, the MOD provides such information to relevant ministries and agencies.

(2) Major Initiatives Relating to Coordination with the Private Sector and Information Dissemination

As described above, banks, etc., funds transfer service providers, electronic payment instruments service providers, and currency exchange operators are required to conduct their own risk assessments and take measures based on the identified risks. In addition, other private-sector business operators, including DNFBPs, are expected to take risk-based measures. Furthermore, in order to reduce the risk that business operators may become unintentionally involved in PF, close coordination between the government and private-sector business operators, as well as information dissemination, is important. Accordingly, the following initiatives are currently being implemented. In practice, business operators encounter transactions such as those shown in Table 3 and take responses commensurate with the risks (see Table 3).

- Ministries and agencies with jurisdiction over financial institutions, etc. publish reference case examples of transactions that may constitute suspicious transactions and to which financial institutions, etc. should pay particular attention when fulfilling their obligation to report suspicious transactions. In addition, by taking advantage of various opportunities, such as the issuance of FATF statements, these ministries and agencies repeatedly request financial institutions, etc. to: promptly update sanction lists following the designation and publication of sanctions targets; conduct strict customer due diligence in accordance with the Act on Prevention of Transfer of Criminal Proceeds and relevant guidelines; thoroughly fulfill the obligation to report suspicious transactions; appropriately implement measures under the FEFTA; and comply with the provisions of the Terrorist etc. Assets Freezing Act.
- The NPA and the FSA jointly hold annual workshops for personnel financial institutions, etc. to deepen their understanding on the suspicious transaction reporting system.
- Ministries and agencies with jurisdiction over DNFBPs publish reference cases examples of transactions that may constitute suspicious transactions and to which specified business operators should pay particular attention. In addition, through AML/CFT/CPF guidelines formulated by the respective ministries and agencies, required responses related to asset-freezing measures under the FEFTA, etc. are set out, and information on persons and entities subject to asset-freezing measures is provided to business operators under their jurisdiction. The Japan Federation of Bar Associations, upon receiving notifications from the MOJ, disseminates information on persons and entities subject to asset-freezing measures to its members.
- Customs authorities endeavors to disseminate information to customs brokers, etc. regarding

prohibitions on imports from and exports to North Korea, and request their cooperation in ensuring the effectiveness of such measures.

- While passengers' personal effects carried into or out of Japan are generally treated as exceptions to import and exempt prohibitions, customs authorities conduct strict enforcement by closely exchanging information with relevant government agencies, shipping companies, and airlines, etc., in order to respond to cases in which illicit imports or exports are conducted by disguising goods as personal effects, as well as cases in which ship or aircraft crew members attempt to export luxury goods to North Korea by concealing them among items deemed for personal use.
- In August 2025, the MOFA, the U.S. Department of State, and the Ministry of Foreign Affairs of the Republic of Korea, in partnership with Mandiant, co-hosted the Japan-U.S.-ROK Public-Private Event to counter North Korean IT worker Threats in Tokyo, providing discussions for public and private sector to bolster their collective protection against North Korean IT worker activities..[75]

5. Promotion of International Cooperation

(1) G7-related Initiatives

- The G7 foreign ministers at their meeting in Charlevoix, Canada, in March 2025 expressed their concerns over, and the need to address together, the DPRK's cryptocurrency thefts. Furthermore, Japan has held talks with the United States and the ROK, issued joint statements with like-minded countries including G7 members, and proposed urgent consultations at the UNSC depending on the intensity of North Korea's provocative actions.
- The G7 finance ministers and central bank governors at their meeting in Banff, Canada, in May 2025, issued the "G7 Financial Crime Call to Action" as an annex to their joint statement.[76] The document emphasized serious concerns about North Korea's theft and fraud of crypto assets as the PF risks, as well as the need to stay updated on new risks and deepen responsible information exchange through the enhancement of international cooperation in AML/CTF/CPF measures. The G7 finance ministers and central bank governors reaffirmed their strong commitment to combating financial crime, including financing for WMD proliferation.
- At the G7 Leaders' Meeting in Kananaskis, Canada, in June 2025, Japan expressed concern over cryptocurrency thefts, which is suspected to be one of the funding sources for North Korea's nuclear and missile development. The Chair's Summary for the G7 summit stated that the leaders

[75] MOFA, *Japan-U.S.-ROK Public-Private Event to Counter North Korean IT Worker Threats*, August 26, 2025, https://www.mofa.go.jp/press/release/pressite_000001_01601.html
[76] MOF, *G7 FINANCE MINISTERS AND CENTRAL BANK GOVERNORS' COMMUNIQUÉ*, May 20-22, 2025, https://www.mof.go.jp/english/policy/international_policy/convention/g7/g7_20250522_1.pdf

"expressed concern about DPRK's nuclear weapons and ballistic missile programs and the need to jointly address DPRK cryptocurrency thefts fueling these programs."[77]

(2) Cooperation with Other Countries

- The MOFA, the United States and the ROK, has held the Japan-U.S.-ROK Trilateral Diplomatic Working Group on North Korea's Cyber Threats in December 2023, March and September 2024, and August 2025. Through these meetings, the three countries have reaffirmed their commitment to advancing tangible efforts against North Korea's malicious cyber activities, including crypto asset thefts and North Korean IT workers' activities.[78]
- In December 2024, the NPA, the Federal Bureau of Investigation (FBI), and the Department of Defense Cyber Crime Center (DC3) jointly announced that they had identified a North Korea-backed cyberattack group, "TraderTraitor," as having stolen about 48.2 billion yen in crypto assets from DMM Bitcoin Co., Ltd., a Japan-based crypto asset exchange service provider. The NPA stated that it would continue to work with the FBI, other U.S. government agencies, and international partners to identify and take strict action against illicit activities that benefit North Korea, including cybercrime and crypto asset theft.
- In January 2025, Japan, the United States, and the ROK issued the "Joint Statement on Cryptocurrency Thefts by the Democratic People's Republic of Korea and Public-Private Collaboration," pointing out crypto asset theft by North Korea and reaffirming their commitment to combatting cyber threats posed by the DPRK and enhancing their coordination.[79] In August, the three countries also issued the "Joint Statement on North Korean Information Technology Workers," pointing out the increasing sophistication of North Korean IT workers' tactics and the expanding number of their target clients and reaffirming their commitment enhancing their coordination among the three countries and collaboration between the public and private sector.[80]
- In May 2025, the MSMT released its first report on unlawful military cooperation between North Korea and Russia, including arms transfers. In October, it published its second report on North Korea's malicious cyber activities and North Korean IT workers' activities in violation of the UNSCRs.

---

[77] MOFA, *CHAIR'S SUMMARY,* June 17, 2025, https://www.mofa.go.jp/mofaj/files/100864611.pdf
[78] MOFA, *The 4th Japan-U.S.-ROK Trilateral Diplomatic Working Group on North Korea's Cyber Threats*, August 28, 2025, https://www.mofa.go.jp/press/release/pressite_000001_01606.html
[79] MOFA, *Joint Statement on Cryptocurrency Thefts by the Democratic People's Republic of Korea and Public-Private Collaboration*, January 14, 2025, https://www.mofa.go.jp/press/release/pressite_000001_00914.html
[80] MOFA, *Japan-U.S.-ROK "Joint Statement on North Korean Information Technology Workers" and "Alert for Companies on North Korean Information Technology Workers"*, August 27, 2025, https://www.mofa.go.jp/press/release/pressite_000001_01605.html

(3) FATF

- Under Japan's G7 Presidency, the FATF Virtual Asset Contact Group (VACG) meeting, co-chaired by the FSA, was held in Tokyo in April 2023.[81] Officials from 19 jurisdictions, including Japan, and international organizations attended the meeting. The group discussed challenges for the effective implementation of AML/CFT/CPF measures on virtual assets while bearing in mind the growing risks, such as theft and misuse of virtual assets by North Korea.
- The FATF/VACG has continued outreach activities and technical assistance for global compliance with Recommendation 15 (new technologies including virtual assets). After publishing a table on the status of implementation of Recommendation 15 by FATF Members and FSRB Jurisdictions with materially important VASP activity to regulate VA/VASPs in 2024,[82] it announced an update to the table in 2025 and plans to release another update in 2026.
- In June 2025, the FATF published its sixth annual report summarizing global progress on the implementation of Recommendation 15, including updates to the above-mentioned table, as well as analysis of fraud cases, illicit virtual asset-related activities by North Korea, and emerging risks related to stablecoins, DeFi, and peer-to-peer transactions involving unhosted wallets.[83] The report pointed out that since 2024, the abuse of stablecoins by North Korean-related actors and terrorist financiers, etc. has been increasing in a manner similar to virtual assets. As a co-chair of the VACG, the FSA has been involved in compiling both the implementation table and the annual report.
- In August 2025, the Asia/Pacific Group on Money Laundering (APG), co-chaired by the MOF, held the 2025 APG annual meeting in Tokyo. At the meeting, the FSA hosted a technical seminar on Virtual Assets and Virtual Assets Service Providers, drawing on North Korean-related and other case studies to share challenges and best practices in enhancing understanding of PF and other risks arising from the abuse of virtual assets, as well as the implementation of FATF Recommendation 15.
- Regarding the revision of FATF Recommendation 16[84], which also includes measures to address PF, Japan, as the co-chair of the FATF Policy Development Group, played a key role in helping to shape and summarize the discussions. The revision clarifies that Recommendation 16 covers

---

[81] FSA, *JFSA hosted Financial Action Task Force (FATF) Virtual Assets Contact Group Meeting in Tokyo*, Updated on April 17, 2023, https://www.fsa.go.jp/en/news/2023/20230414/20230414.html
[82] FATF, *Status of implementation of Recommendation 15 by FATF Members and Jurisdictions with Materially Important VASP Activity*, March 28, 2024, https://www.fatf-gafi.org/en/publications/Virtualassets/VACG-Snapshot-Jurisdictions.html
[83] FATF, *Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers*, Jun 26, 2025, https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Fatfrecommendations/targeted-update-virtual-assets-vasps-2025.html
[84] FSA, *FATF updates Standards on Recommendation 16 on Payment Transparency,* Updated on December 8, 2025, https://www.fsa.go.jp/inter/fatf/20250619/20250619.html

not only ML and TF but also the prevention and detection of PF and fraud. In order to ensure the smooth implementation of the revised requirements, Japan will continue to actively participate in this initiative and lead discussions on the preparation of guidance, including details of the revised requirements, under public-private partnership.

(4) Other Initiatives

- In Bangkok, Thailand, in November 2025, the United Nations Interregional Crime and Justice Research Institute (UNICRI) held a workshop titled “Facilitating Regional Cooperation for Robust and Effective Sanctions Enforcement: UNICRI’s Southeast Asia Workshop on DPRK Sanctions and Emerging Threats” for sanctions practitioners from ASEAN countries (excluding Myanmar) to improve their UN sanctions implementation capacity and share relevant information. The workshop was held through Japan's financial contribution, and covered the FATF’s PF risk assessment and good practices for preventing PF.

Chapter 5. Conclusion

As set out in this National Risk Assessment, Japan is exposed on a daily basis to numerous PF-related threats. In addition to the existence of persons and entities designated under the UNSCRs, there are entities that conduct cyberattacks, entities that cause goods and technologies—including dual-use items—used for the development of WMD to flow out of Japan, and entities that seek to engage in PF and WMD development by exploiting all available means, including legal persons whose actual circumstances, such as activities and capital relationships, are opaque. Such entities may pose threats to Japan.

Indeed, PF-related financial sanctions have repeatedly violated or circumvented by such threats. In particular, cyberattacks, which are characterized by the continual evolution of methods and the difficulty of tracing them, have to led to year-on-year increase in number of cases, as well as substantial damage. With respect to the import and export of dual-use items, the increasing complexity and diversification of distribution structures have resulted in the outflow of many sensitive technologies and goods that may be diverted to military use. In addition, the CPFSES Report has pointed out cases of illicit exports involving legal persons whose actual circumstances, such as activities and capital relationships, are opaque. Moreover, factors such as Japan's highly developed financial sector—which can provide various means for PF—and its geographical proximity to North Korea further contribute to Japan's vulnerabilities to PF.

In response to the current PF landscape, Japan has taken various measures. In addition to designating North Korean cyber attack such as Lazarus Group, Andariel, BlueNoroff, and Kimsuky for asset-freezing, etc., Japan issued a joint statement with the U.S. and ROK on North Korean IT workers in August 2025 and updated an alert on North Korean IT workers. In addition, in order to further ensure the effectiveness of sanctions measures under the FEFTA, from April 2024 Japan has required crypto asset exchange service providers, banks, and other entities handling foreign exchange transactions to establish frameworks for implementing asset-freezing and other measures. With regard to dual-use items, Japan implements export controls under the FEFTA in light of the international export control regimes. To enhance the transparency of legal persons, Japan introduced the beneficial ownership list system in January 2022. Furthermore, since June 2023, a new mechanism has been introduced under which notaries examine, in the course of notarizing articles of incorporation, whether persons who are to become beneficial owners of legal persons are involved in WMD-related programs.

Nonetheless, as the nature of threats continues to evolve on a daily basis, it goes without saying that Japan's efforts, including various other measures under the existing legal framework, will always remain "a work in progress." It is important to further deepen risk analysis in this National Risk Assessment, and to continue strengthen coordination among relevant ministries and agencies through

the Policy Council and other mechanisms, while promoting the sharing and exchange of information and expertise as necessary. In addition, administrative authorities should appropriately disseminate information on these initiatives and amended systems so as to deepen the private sector's understanding of governmental efforts and the current regulatory framework. Public-private cooperation is also essential to promote information sharing in responding to PF.

Case Studies

Table 1: Domestic Cases

No.	Type	Summary
1	Trade	In February 2007, eight people, including an executive of a fishery product import and sales company, imported live clams of North Korean origin without obtaining approval from the METI. In April 2007, they were arrested for violating the FEFTA (import without approval).
2	Trade	In April 2007, three people, including an executive of a trading company who imported sea urchins of North Korean origin without obtaining approval from the METI. In January 2008, they were arrested for violating the FEFTA (import without approval).
3	Trade	In December 2007, the president of a food sales company imported greenbrier of North Korean origin without obtaining approval from the METI. In August 2009, the president was arrested for violating the FEFTA (import without approval).
4	Trade	In September 2010, two people, including the president of a trading company, imported matsutake mushrooms of North Korean origin without obtaining approval from the METI by falsely declaring them to be of Chinese origin. In March 2015, they were arrested for violating the FEFTA (import without approval). In relation to the same case, three people, including an executive of a trading company, were arrested for importing North Korean matsutake mushrooms without obtaining approval from the METI by falsely declaring them to be of Chinese origin in violation of the FEFTA (import without approval).
5	Trade	In January 2020, three people, including the owner-manager of a trading company who imported freshwater clams of North Korean origin without obtaining approval from the METI. In September 2024, they were arrested for violating the FEFTA (import without approval).
6	Trade	In 2017, a male North Korea agent was found to have, for an extended period of time, continued to procure large amounts of foods and other products in Japan and exported them to North Korea via a shell company established in Singapore.
7	Trade	In January 2017, a former manager of a trading company was found to have exported furniture and other goods to North Korea via Hong Kong and Dalian in China, despite the prohibition on all goods destined for North Korea that was

		introduced on June 18, 2009. The former manager was subsequently arrested in August 2019 for violating the FEFTA by engaging in unapproved exports.
8	Trade	In September 2024, a former owner-manager of a fishery processing company was arrested for violating the FEFTA by engaging in unapproved exports. Despite the comprehensive prohibition on exports of all goods destined for North Korea that has been in place since June 18, 2009, the individual exported clothing and other goods to North Korea via China in December 2019 without obtaining approval from the METI.
9	Persons	When financial institutions performed the obligation for implementing confirmation regarding the prohibition-in-principle of payment to North Korea based on Article 17 of the FEFTA in relation to an overseas remittance, no confirmation has been implemented as to whether or not the beneficial owner of remittance recipient is a resident of North Korea.
10	Persons	In implementing the obligation to conduct confirmation pursuant to Article 17 of the FEFTA in relation to the principle-based prohibition on payments to North Korea, cases were identified in which financial institutions, with respect to overseas remittances made to the three northeastern provinces of China under the stated purpose of living expenses, failed to assess the appropriateness of the remittance amounts, to verify the beneficiaries of the living expenses, and to conduct detailed inquiries into matters such as the relationship between the remittance senders and the recipients.
11	Persons	In March 2024, the president of an IT-related company, who is a South Korean national, and a former employee were arrested on fraud charges. During the investigation, it was found that the suspects had outsourced app development work consigned by a Japanese company through an online platform to a North Korean IT worker presumably residing in China.
12	Persons	In September 2024, two Japanese men were arrested on suspicion of illegally creating private electromagnetic records. The men allegedly opened accounts at a securities company by falsely declaring that they would comply with the terms of their contracts. In reality, they conducted FX transactions using an automated trading system that was prohibited by the company, in conspiracy with an individual believed to be a North Korean IT worker.
13	Persons	In April 2025, two Japanese men were arrested for the unauthorized creation of private electromagnetic records and the aid for the use of such records. The suspects provided images of their driver's licenses and bank account

		information to alleged North Korean IT workers, helping them impersonate Japanese to register accounts with crowdsourcing companies.
14	Persons	North Korean IT workers have disguised their nationality and earned income by fraudulently getting contracts for animation projects from multiple companies, including HBO Max, Amazon, and several Japanese anime studios. They received instructions and comments from Chinese nationals and contacted North Korean cyber actors.
15	Cyberattacks and Crypto Assets	In late March 2024, a North Korean cyber actor posed as a recruiter and contacted an employee of Ginco, a Japan-based crypto wallet software company, on the LinkedIn social network. The threat actor sent a URL to a malicious Python script disguised as a pre-recruitment test stored on GitHub to the Ginco employee who had access to Ginco's wallet management system. The victim copied this Python code to his GitHub page and was compromised. In or after mid-May of the same year, a TraderTraitor actor impersonated the compromised Ginco employee and exploited session cookie information to successfully gain access to Ginco's unencrypted communication system. Later that month, the actor used this access to falsify legitimate transaction requests by DMM employees, resulting in the outflow of 4,502.9 BTC (worth 308 million dollars at the time of the attack). Eventually, the stolen assets were transferred to wallets managed by TraderTraitor.
16	Dual-use Products	In September 2002, a former representative director of a trading company handling trade with North Korea illicitly exported a freeze dryer to North Korea from Yokohama Port via Taiwan without obtaining a license from the METI while knowing that the product might be used for the development of nuclear weapons.
17	Dual-use Products	On April 4, 2003, Company A exported three units of three direct current regulated power supply units, which might be used for the development of nuclear weapons and missiles, to North Korea via Thailand despite having been notified of the need to obtain an export license from the METI.
18	Dual-use Products	Around July 2003, a representative director of a trading company handling trade with North Korea exported vacuum pumps to North Korea from Narita Airport via Taiwan illicitly, without obtaining a license from the METI, while knowing that the products might be used for the development of nuclear weapons.
19	Dual-use Products	In November 2003, Limited Company B exported an inverter (frequency changer) that might be used for the development of nuclear weapons to North

		Korea via China without obtaining a license by having a conspirator transport the product as carry-on baggage despite having been notified of the need to obtain an export license from the METI.
20	Dual-use Products	Company C exported vacuum suction pressure casting machines and other products that it had manufactured to Iran, China, and Thailand, among other countries, without obtaining a license from the METI between 2007 and 2016.
21	Dual-use Products	In January 2008, the representative director of a trading company handling trade with North Korea illicitly exported two used tank trucks to the ROK—despite having been notified of the need to obtain an export license from the METI due to the possibility of the trucks being used for the development of nuclear weapons—with the aim of delivering them to North Korea via the ROK, export to which does not require a license from the minister.
22	Dual-use Products	Company D exported one jet mill to Iran in each of 1999 and 2000 without obtaining a license from the METI although the product might be used for the development of missiles.
23	Dual-use Products	The representative director of a trading company exported to China 20 units of a machine tool with a built-in numerically controlled program, an item subject to the restriction on provision to non-residents living abroad under the FEFTA, without obtaining permission from the METI, thereby providing services made available by the program.
24	Dual-use Products	Japan-made carbon fibers, though having been shipped from China to Iran, were seized in a third country before their arrival in Iran. While carbon fibers are used for civilian applications as well, they are materials indispensable to high-performance centrifugal separators, which are used for uranium enrichment, so the export of carbon fibers with a higher quality than the prescribed level has been prohibited based on UNSCRs. As Japanese carbon fibers are known for their high quality, Iran may have tried to obtain the material for the development of nuclear weapons. According to the abovementioned report, although the carbon fibers in question were exported by a Japanese company to China based on appropriate procedures, 7,200 kilograms of the material were resold to Iran and transported by vessel to the country.
25	Leakage of Technologies	When an entity received a remittance sent as a fee related to research and development from a country not subject to the sanctions, it did not implement appropriate confirmation in order to make sure that the research and development in question did not constitute an activity that could contribute to

		North Korea's nuclear-related programs or an activity conducted for the purpose of contributing to Iran's nuclear activities, and this was recognized as a case of deficiency in foreign exchange inspection under the FEFTA.

Table 2: Overseas Cases

No.	Type	Summary	Source
1	Money	North Korea is expanding its access to illicit financial networks through the Foreign Trade Bank (FTB) and Korea Kwangson Banking Corporation (KKBC) subjected to UN sanctions by using MRB Bank (MRB) accounts in the Russian-occupied Georgian region of South Ossetia. Russia's TSMR Bank is working with North Korean agents to deposit millions of dollars and rubles into MRB accounts and making payments for fuel exports from Russia to North Korea through MBR accounts. (United States)	CPFSES (BOX11)
2	Trade	In December 2023, a Chinese national who was illegally staying in the United States was indicted for exporting firearms to North Korea via Hong Kong at the direction of North Korean officials, as well as for attempting to export approximately 60,000 rounds of ammunition and sensitive technologies to North Korea.	U.S. Department of Justice
3	Trade	As raw materials for false eyelashes imported by e.l.f Cosmetics from two Chinese companies were from North Korea, e.l.f Cosmetics was accused of violating Office of Foreign Assets Control (OFAC) regulations. In this case, e.l.f Cosmetics agreed to pay 996,080 dollars to the OFAC to settle the accusation.	U.S. Department of the Treasury
4	Persons	North Korean overseas workers earn income mainly in countries such as China, Russia, and Laos, working in IT, restaurant, construction, and manufacturing (sewing and clothing) sectors. They have entered these countries on student or tourist visas. Some of them reportedly use fake nationality or identification certificates. North Korea has signed contracts to send 400,000 workers abroad. It is expected that more workers will be sent overseas.	The reports of the Panel of Experts (S/2024/215)

5	Persons	Methods of remitting or repatriating income earned by North Korean overseas workers to North Korea include online payments, the use of bank accounts in third countries, the use of bank accounts in the names of local collaborators, the purchase of refined petroleum products and other goods required by the regime, ML, insurance money collection, large cash transportation using diplomatic privileges, and the use of international financial systems running counter to UNSCRs.	The reports of the Panel of Experts (S/2024/215)
6	Persons	In response to crackdowns on North Korean IT workers operating in U.S. jurisdictions, North Korean IT workers are reportedly expanding their business scope globally, with a particular focus on job hunting for small and medium-sized IT companies in Europe. It is reported that they seek jobs in AI, blockchain technology, web development, defense, government, and other sectors, build trust with recruiters by using personas that combine stolen and fabricated information, and prefer to receive pay through crypto assets, Wise, Payoneer, etc.	MSMT (MSMT/2025/2)
7	Cyberattacks and Crypto Assets	In February 2025, about 1.5 billion dollars (225 billion yen) worth of Ethereum was leaked from the Dubai-based crypto asset exchange Bybit, recording one of the largest crypto asset losses in history. The leak represented an attack by North Korea's state-sponsored hacker group Lazarus Group (also known as TraderTraitor or APT38). The FBI has warned that stolen funds could be diverted to fund North Korea's nuclear and missile development.	FBI
8	Cyberattacks and Crypto Assets	From 2017 to 2023, North Korea was suspected to have been involved in 58 cyberattacks against crypto-related companies, which resulted in about 3 billion dollars in losses. North Korea has obtained about 50% of its foreign currency revenues through cyberattacks and has used those revenues for its WMD program.	The reports of the Panel of Experts (S/2024/215)
9	Cyberattacks and Crypto Assets	North Korea attack methodologies continue to include spearphishing, vulnerability exploits, social engineering	The reports of the Panel of Experts

		and watering holes, in addition to ongoing targeting of the cryptocurrency industry.	(S/2024/215)
10	Cyberattacks and Crypto Assets	The Lazarus Group conducts cyberattacks against defense companies around the world to obtain information such as intellectual property and blueprints for promoting and funding North Korea's WMD and ballistic missile programs.	The reports of the Panel of Experts (S/2024/215)
11	Cyberattacks and Crypto Assets	Kimsuky has created malicious apps disguised as legitimate Android apps, including popular e-commerce services, Google Authenticator, antivirus programs, and payment service apps and has been stealing information from devices infected with these apps.	The reports of the Panel of Experts (S/2024/215)
12	Cyberattacks and Crypto Assets	BlueNoroff impersonates financial institutions and venture capital firms in Japan, Vietnam, and the United States to trick victims into opening malicious content or providing login credentials.	The reports of the Panel of Experts (S/2024/215)
13	Cyberattacks and Crypto Assets	With the help of financial intermediaries in neighboring countries, North Korea has used fiat currency accounts at crypto wallets, banks, electronic financial platforms, etc. to exchange funds for fiat currency and send large sums of money to Pyongyang to purchase sanctioned supplies and fund its WMD program. (South Korea)	CPFSES （BOX22）
14	Cyberattacks and Crypto Assets	A North Korean computer programmer was charged with allegedly being involved in a wide range of criminal conspiracies, including cyberattacks and the theft of more than 1.3 billion dollars in money and cryptocurrency. The defendant belonged to a North Korea military intelligence agency. (United States)	CPFSES （BOX25）
15	Cyberattacks and Crypto Assets	In 2021, Colonial Pipeline faced a ransomware attack by DarkSide and paid the demanded ransom in the crypto asset Bitcoin.	U.S. Department of Justice
16	Cyberattacks and Crypto Assets	Iranian financiers laundered 100 million dollars related to Iranian crude oil sales through cryptocurrencies from 2023 to 2025. The funds were used to support the Iranian military through front companies in third countries.	U.S. Department of the Treasury

17	Dual-use Products	Chinese nationals were charged in an indictment in the District of Columbia for using a front company in China to smuggle U.S.-made dual-use goods such as electronic devices into Iran via China and Hong Kong by falsely declaring that the ultimate destination was China. (United States)	CPFSES （BOX３）
18	Intermediaries	Iran maintains an extensive overseas network of procurement agents, front companies, intermediaries, and suppliers to acquire highly sensitive dual-use goods. The network uses the concealment of end-users through the layering of transactions, the falsification of documents on the final use and details of shipments, transportation routes through multiple countries, disguised access to U.S. and international financial systems, and other measures to evade export controls and sanctions.	U.S. Department of Commerce U.S. Department of State U.S. Department of the Treasury U.S. Department of Justice
19	Intermediaries	North Korea gained access to international financial systems by using joint ventures, offshore bank accounts, shell companies, and crypto asset. Persons and entities related to North Korea were also using small and medium-size banks in East and Southeast Asia for making international remittances.	The reports of the Panel of Experts (S/2021/777)
20	Intermediaries	A South Korean-born Australian citizen was charged with using offshore bank accounts and Australia-based front companies to broker transactions with North Korea for various goods such as coal, graphite, copper ore, gold, crude oil (including purchasing Iranian petrol on behalf of North Korea), missiles, and missile-related technology (Australia)	CPFSES （BOX２）
21	Intermediaries	There was a case where a company that tried to export motors with application in Unmanned Aerial Vehicles to Kazakhstan through an intermediary in the United Arab Emirates gave up on the export as it was asked about whether the final destination was Russia. It was later found that the company exported other goods to Russia through intermediaries in Serbia and Hong Kong. Both	CPFSES （BOX６）

		intermediaries were companies with strong commercial relations with Russia. (Portugal)	
22	Intermediaries	A North Korean diplomat, posted in France, bought an apartment and was earning relevant rental income even after becoming subject to UN sanctions. By using various intermediaries with bank accounts in several third countries, the diplomat concealed his position as the end beneficiary. (France)	CPFSES（BOX10）
23	BO	More than 30 individuals were indicted for using more than 250 front companies established in Austria, China, Kuwait, Libya, the Marshall Islands, Russia, and Thailand to have U.S. correspondent banks process illicit payments. They teamed up with third-party financial facilitators to create front companies that could pay for commodities and other goods on behalf of North Korea and made payments for refined petroleum and coal transactions, as well as those to metals, electronics, and telecommunications companies. The defendants created new front companies when their counterparties became suspicious about existing front companies and falsely stated end destinations and end-users in contracts and invoices. (United States)	CPFSES（BOX13）
24	BO	A German limited liability company that owned luxury cars was controlled by a person listed by the EU under the Russian Sanctions Regime to conceal the true ownership of vehicles. (Germany)	CPFSES（BOX17）
25	BO	North Korea-associated individuals have illegally-obtained UnionPay debit cards issued by major China-based banks to purchase proscribed items and conduct crypto transactions through third countries while misusing accounts in the names of Chinese nationals to hide their ties to North Korea.	CPFSES（para.74-76）
26	Maritime and Shipping Sectors	An individual was accused of providing gasoil to North Korea by transferring gasoil at the Nampo Port in North Korea after ship-to-ship transfers on six occasions. The suspect is alleged to have falsified documents and utilized the bank accounts of a company of which he was a director	CPFSES（BOX30）

		and of another company under his control to facilitate payments for gasoil. (United States)	
27	Maritime and Shipping Sectors	According to investigations by Taiwanese prosecutors, North Korea's sanctions violations include the transfer of oil to North Korean ships on the high seas from third-jurisdiction ships controlled by Taiwanese oil companies and the transfer of oil to ships owned by third-party jurisdictions for the purpose of eventually reselling oil to North Korean ships. Petroleum products are still commonly used by Taiwanese UN sanctions violators in trading. As oil trading on the high seas is not illegal under local law, ship-to-ship transfers are used to disguise illicit transfers. False export information, and offshore companies and accounts are also used to frustrate funds tracing. (Taiwan)	CPFSES （BOX31）
28	Maritime and Shipping Sectors	Indonesian authorities detained a vessel subject to UN sanctions for illegal coal shipments to North Korea. The ship escaped detection by tampering with its identity and using alias flags. (Indonesia)	CPFSES （BOX29）
29	Maritime and Shipping Sectors	Indian customs authorities seized an Asian-flagged ship bound for Pakistan. It was confirmed that documents mis-declared the shipment’s dual-use items that can be used for sensitive high energy materials and for insulation and chemical coating of missile motors and subjected to export control and indicated a link between the importer and an entity involved in the development of long-range ballistic missiles. (India)	CPFSES （BOX34）

Table 3: Information Provided by Private Business Operators

No.	Type	Summary	Source
1	Trade	Authorities detected a transaction in which Mr. A, a resident in Japan, sold a car with a displacement of more than 1,900cc, subject to export restrictions for Russia under the FEFTA, to Mr. B, a nonresident in Russia and exported the car to Mr. C, its end user residing in Canada. They	MOF (provided by domestic financial institutions)

		asked for information about Mr. C and considered whether there was a possibility of the car being diverted to Russia.	
2	Persons	Domestic business operator Company D requested a Japanese yen-denominated outward remittance to Mr. E (an individual in Yanji, China). Since Yanji is close to North Korea, authorities checked the purpose of the remittance in advance. As the relevant document specified the remittance as the payment for an anime drawing request, they checked Mr. E's attributes with Company D due to concerns about dealing with North Korean IT workers. They also checked Company D's system for compliance with laws and regulations.	MOF (provided by domestic financial institutions)
3	Persons	Domestic business operator Company F requested a Japanese yen-denominated outward remittance to Company G (a corporation in Dandong, China). Since Dandong is close to North Korea, authorities checked the purpose of the remittance in advance. As the relevant document specified the remittance as the payment for an anime drawing, they checked Company G’s overview with Company F and verified the copied passport of Company G’s representative Mr. H (a Chinese national), etc. through Company F due to concerns about dealing with North Korean IT workers.	MOF (provided by domestic financial institutions)