



<Provisional Translation>

NATIONAL RISK ASSESSMENT OF PROLIFERATION FINANCING IN JAPAN DECEMBER 2024

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

Contents

Overview

Chapter 1 Proliferation financing

1. Definition of and background to proliferation financing
 - (1) Definition of proliferation financing
 - (2) Background
 - (i) North Korea
 - (ii) Iran
2. Risk assessment approach
 - (1) FATF Guidance
 - (i) Risk factors
 - (ii) Points of attention regarding assessment
 - (2) Approach of the present National Risk Assessment
 - (3) Framework for preparing the National Risk Assessment

Chapter 2 PF Threats

1. Premises
2. Threats in Japan
 - (1) Entities involved in leakage of money
 - (i) Entities that import goods from North Korea via neighboring third countries
 - (ii) Entities that act as channels for overseas remittance to North Korea, such as supporters and related parties located in neighboring countries
 - (iii) Entities that launch cyberattacks
 - (2) Entities involved in leakage of technologies and goods
 - (i) Entities that earn money through trading dual-use products
 - (ii) Entities that earn money through leakage of technologies
 - (iii) Entities involved in illegal ship-to-ship transfers of goods
 - (3) Entities that use resources of companies with opaque structures, including those that are sanctioned under the UNSCRs

Chapter 3 PF vulnerabilities and risks

1. Premises
2. Japan's vulnerabilities
 - (1) Geographic proximity to North Korea
 - (2) Globally significant international financial center
 - (3) Major industrial center and open economy regime
3. Transactions with high PF risk

Chapter 4 Japan's initiatives regarding PF

1. Initiatives regarding financial transactions
 - (1) Economic sanctions based on the Foreign Exchange Act
 - (2) Regulation on domestic transactions based on the Terrorist etc. Assets Freezing Act
2. Import and export controls
 - (1) Prohibition of imports and exports under the Foreign Exchange Act, etc.
 - (2) Security export control under the Foreign Exchange Act
3. Other related regulations
 - (1) Act on Prevention of Transfer of Criminal Proceeds (verification at the time of transaction, notification obligation)
 - (i) Verification at the time of transaction
 - (ii) Notification obligation (travel rule)
 - (2) Schemes for increasing the transparency of legal persons
 - (3) Immigration Control and Refugee Recognition Act
 - (4) Act on Prohibition of Entry of Specified Ships into Ports / Cargo Inspections Act
 - (5) Other AML/CFT related regulations
4. Major initiatives relating to close coordination among ministries and the private sector
 - (1) Major initiatives relating to close coordination among ministries
 - (2) Major initiatives relating to close coordination with and dissemination of information to the private sector
5. Promotion of international cooperation

Chapter 5 Conclusion

Acronyms

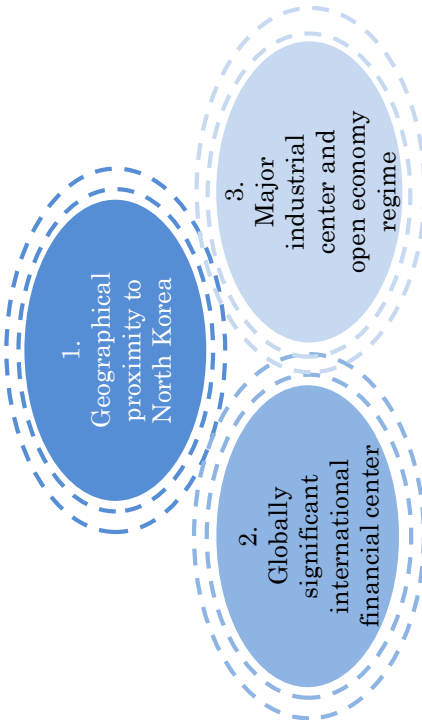
The meanings of the acronyms used in this report are as follows:

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.

Overview Of Japan's PF NRA

Definition of and Background to Proliferation Financing (PF)	
<ul style="list-style-type: none"> - PF: potential breach, non-implementation, or evasion of the targeted financial sanctions obligations referred to in FATF Recommendation 7 (Rec 7). - FATF revised Rec 1 and its Interpretive Note to require countries to identify, assess, understand, and mitigate their PF risk. 	
Analysis on our PF risk	
Threat	Vulnerabilities
<p>1. Actors involved in leakage of money</p> <ul style="list-style-type: none"> ① Trades: Actors that import goods from North Korea via neighboring third countries ② Persons: Actors that act as channels for overseas remittance to North Korea, such as supporters and related parties located in neighboring countries and other third countries ③ Actors that launch cyberattacks <p>2. Actors involved in leakage of technologies and goods</p> <ul style="list-style-type: none"> ① Actors that generate income through trading dual-use items ② Actors that generate income through leakage of technologies ③ Actors involved in illegal ship-to-ship transfers of goods <p>3. Actors that use resources of companies with opaque structures, including those that are sanctioned under the UNSCRs</p>	
Japan's counter-proliferation financing regime (measures to mitigate risks)	
<p><Mitigations Measures based on related regulations ></p> <ul style="list-style-type: none"> 1. Economic sanctions based on the Foreign Exchange and Foreign Trade Act (FEFTA) 2. Regulation on domestic transactions based on the Terrorist etc. Assets Freezing Act 3. Import and export control 4. Act on Prevention of Transfer of Criminal Proceeds ("verification at the time of transaction" "travel rule") 5. The schemes for increasing the transparency of legal persons, such as beneficial ownership (BO) frameworks 	<ul style="list-style-type: none"> 6. Immigration Control and Refugee Recognition Act 7. Act on Prohibition of Entry of Specified Ships into Ports / Cargo Inspections Act 8. Other AML/CFT related regulations <p><Close coordination among stakeholders to mitigate risk ></p> <ul style="list-style-type: none"> 1. Close coordination among ministries and the private sector 2. International cooperation

Chapter 1 Proliferation financing

1. Definition of and background to proliferation financing

(1) Definition of proliferation financing

Proliferation financing (PF) refers to the act of providing funds or financial services to persons and entities subject to asset freezing and other measures for their involvement in the development, possession, and export of weapons of mass destruction (WMDs) (nuclear, chemical and biological weapons).

The international standards for counter measures against PF have been determined and published by the Financial Action Task Force¹ (FATF) since 2012 (such as Recommendation 7 (Targeted financial sanctions related to proliferation²)). Countries are required to implement targeted financial sanctions (e.g., asset freezing) to comply with the United Nations Security Council resolutions (UNSCRs) relating to the prevention, suppression, and disruption of proliferation of WMDs and the financing of WMDs.

On the other hand, even though members of the international community, including Japan, are cooperating in implementing economic sanctions against North Korea and Iran under that framework, WMDs and related materials and technologies have been transferred to these countries and regions of concern. Therefore, in October 2020, FATF revised Recommendation 1 (Assessing risks and applying a risk-based approach) and its Interpretative Note so as to require countries 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,” take commensurate action aimed at ensuring that these risks are mitigated effectively, address higher risks where such risks have been identified, and control and mitigate lower risks where such risks have been identified. These measures are required in addition to the anti-money laundering (AML) measures and countering the financing of terrorism (CFT) measures that have already been required. The revised Recommendation 1 and its Interpretative Note will become applicable starting with the Fifth Round Mutual Evaluation, which has been gradually implemented since 2024.

¹ In response to the Economic Declaration that was issued at the Summit of the Arch in 1989, FATF was established as a multilateral framework responsible for formulating and enforcing international standards related to anti-money laundering (AML) measures. Following the simultaneous, multiple terrorist attacks in the United States in 2001, countering the financing of terrorism (CFT) was added to the scope of its missions. FATF’s members comprise 38 countries and regions and two regional organizations. Decisions on matters relating to FATF’s activities are made at FATF plenary meetings, which are held three times a year.

² Recommendation 7 requires countries to implement targeted financial sanctions to comply with the UNSCRs related to the prevention, suppression and disruption of proliferation of weapons of mass destruction (WMDs) and the financing of WMDs. 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 under Chapter VII of the Charter of the United Nations, and to ensure that no funds and other assets are made available to them or available for their benefit.

Meanwhile, in response to the Fourth Round Mutual Evaluation Report of Japan, which was published in August 2021, the policy council for countering against Anti-Money Laundering (AML), Countering the Financing of Terrorism (CFT), and Proliferation Financing (PF) Policy (hereinafter the “Policy Council”), co-chaired by the National Police Agency and the Ministry of Finance was established in the same month in order to strongly promote counter measures against AML/CFT/PF on a government-wide basis.³ In May 2022, the Policy Council determined the Strategic Policy towards Promoting counter measures against AML/CFT/PF (hereinafter the “Strategic Policy”) in order to examine the risk situation surrounding Japan and confirm the future direction of Japan’s counter measures against AML/CFT/PF and to enhance policy effects of the measures by further strengthening cooperation between relevant ministries and agencies. The Strategic Policy presented the following four pillars in order to implement more effective measures.

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

As a specific measure, the Strategic Policy states as follows: “In parallel to ML/TF risk assessment, the Government will conduct PF risk assessment to improve the effectiveness of the asset freezing measures.”⁴

In addition, the Foreign Exchange and Foreign Trade Act (Act No. 228 of 1949; hereinafter the “FEFTA”) was amended so as to require banks, etc.⁵, funds transfer service providers, electronic payment instruments service providers, etc., and currency exchange operators to conduct self-risk assessment regarding asset freezing in reference to the national risk assessment of PF in Japan (hereinafter the “National Risk Assessment”) and the guidelines and other regulatory documents formulated by relevant ministries and agencies.⁶

³ The Inter-Ministerial Council for AML, CFT, and CPF Policy is comprised of the following members (indicated in the order of establishment): Cabinet Secretariat; Cabinet Office; Personal Information Protection Commission; Japan Casino Regulatory Commission; National Police Agency; Financial Services Agency; Securities and Exchange Surveillance Commission; Ministry of Internal Affairs and Communications; Ministry of Justice; Public Security Intelligence Agency; Ministry of Foreign Affairs; National Tax Agency; Ministry of Education, Culture, Sports, Science and Technology; Ministry of Health, Labour and Welfare; Ministry of Agriculture, Forestry and Fisheries; Ministry of Economy, Trade and Industry; and Ministry of Land, Infrastructure, Transport and Tourism; Ministry of the Environment; and Ministry of Defense.

⁴ Strategic Policy, p. 12.

https://www.mof.go.jp/policy/international_policy/councils/aml_cft_policy/20220519.html

⁵ “Electronic payment service providers, etc.” include electronic payment instruments service providers, electronic payment handling service providers, etc., and crypto-asset exchange service providers.

⁶ “Foreign exchange transaction service providers” as defined under Article 55-9-2, paragraph (1) of the amended FEFTA (come into force on April 1, 2024) are required to assess the risk of breach 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 Ministry of Finance and the Ministry of Economy,

In light of the above, it is necessary for Japan to more appropriately prevent PF. The government needs to identify and analyze PF risks in consideration of cases of breach and evasion of the sanctions and to enhance the effectiveness of measures to mitigate the risks by further strengthening cooperation between relevant ministries and agencies. It is also expected that as well as banks, etc., funds transfer service providers, electronic payment instruments service providers, etc., and currency exchange operators, other private-sector business operators, including DNFBPs,⁷ will take action in consideration of the risks.

(2) Background

Because of the globalization of economic and financial services and technological innovation, such as the diffusion of crypto assets, fund flows have become more diverse, making it easier to conduct cross-border transactions. Under those circumstances, the facilitation of WMD proliferation activity through PF poses a major threat to Japan and to the international community.

Moreover, Japan, as the only country to have ever suffered atomic bombings during war, has been playing the 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 increasing the transparency of armaments and has taken various concrete actions in this regard.

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

Trade and Industry No. 1 of 2023). In the assessment of the risk, the National Risk Assessment also needs to be taken into consideration.

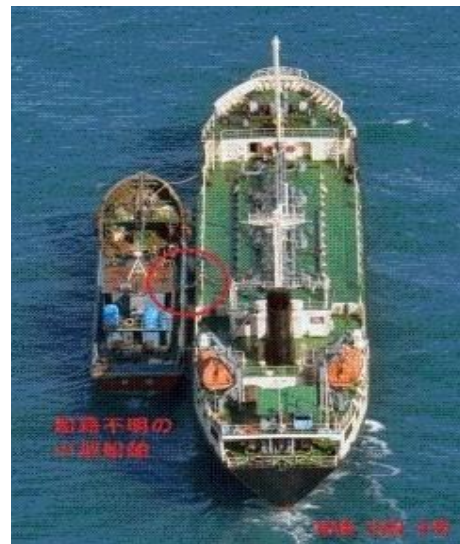
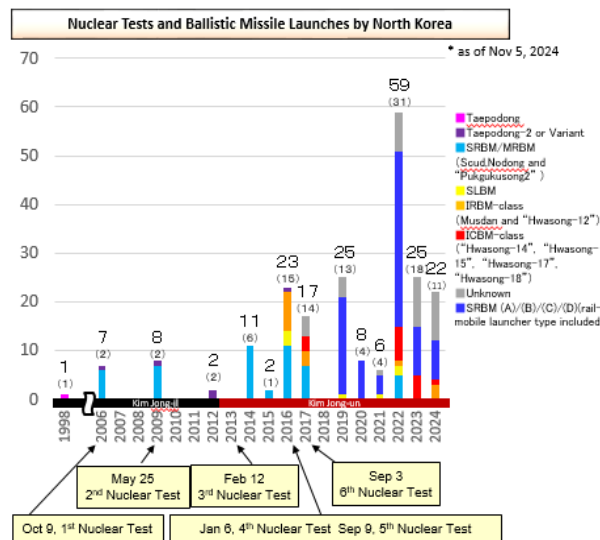
⁷ DNFBPs stands for Designated Non-Financial Businesses and Professions. In Japan, DNFBPs refer to business operators such as real estate brokers, dealers in precious metals and stones, postal receiving service providers, telephone receiving service providers, and telephone forwarding service providers, and professionals such as lawyers, judicial scriveners, certified administrative procedures specialists, certified public accountants, and certified public tax accountants.

⁸ A communique issued at the G7 Summit (Italy) held in June 2024 stated as follows: “We reiterate our call for the complete, verifiable, and irreversible dismantlement of all North Korea’s weapons of mass destruction and ballistic missiles... We strongly condemn North Korea’s continued development of its ballistic missile program in defiance of multiple UNSCRs, including through launches of intercontinental ballistic missiles (ICBM) and space launch vehicles using ballistic missile technologies.”

(i) North Korea

In order to maintain its regime, North Korea has concentrated its efforts on enhancing its arsenal of weapons of mass destruction (WMDs) and ballistic missiles. In particular, regarding ballistic missiles, North Korea is rapidly improving its related technologies and operational capabilities by, for example, diversifying launch modes. In May, August, and November 2023 and in May 2024, it conducted launches using ballistic missile technology for the purpose of a satellite launch. In 2024, it launched ballistic missiles and others at least 11 times.

According to a report by the U.S. Defense Intelligence Agency⁹, North Korea has been exporting ballistic missiles and other weapons for several decades. As the military cooperation between Russia and North Korea advances, North Korea has exported artillery shells and ballistic missiles to Russia, and North Korean missiles have been used by Russia in Ukraine.



(Source) Ministry of Defense

(Source) Ministry of Defense

Moreover, the reports of the Panel of Experts for the UN Security Council 1718 Sanctions Committee (hereinafter referred to as the "Panel of Experts")¹⁰ pointed out that North Korean tankers may have illegally transported between approximately 1.02 million and 1.52 million barrels of refined petroleum products, above the annual limit of 0.5 million barrels, between January 1 and September 15, 2023, and that malicious cyber activities by North Korea, including cryptocurrency thefts and activities of IT workers, funds its nuclear and missile activities. It is also reported that North Korea has increasingly sophisticated illicit ship-to-ship transfer prohibited by the UNSCRs in order to evade or circumvent the sanctions. Japan has developed relevant laws and regulations and ensured the effectiveness of measures implemented by law enforcement agencies in light of the cases and techniques of violation and evasion of the sanctions.

⁹ <https://www.dia.mil/Military-Power-Publications/> (p.67)

¹⁰ The most recent report of the Panel of Experts was published in March 2024. Several reports were published earlier. Hereinafter, relevant portions of the reports are indicated in footnotes.

(ii) Iran
Regarding the production and use of nuclear weapons by Iran, the supreme leader has prohibited the production of them by fatwa (religious order). On the other hand, in recent years, Iran has expanded nuclear-related activities, and Japan has conveyed its concerns over the expansion of their nuclear activities to them and called on them to take constructive measures, including full and unconditional cooperation under the Joint Statement between Iran and the International Atomic Energy Agency (IAEA). ¹¹

The above summarizes the results of the investigation and analysis of the PF risks faced by Japan, which were conducted in view of the revision of the FATF Recommendation and its Interpretative Notes and the background factors, including the international situation surrounding Japan, for the purpose of the National Risk Assessment—using other countries’ national risk assessments and information possessed by international organizations—in order to assess the PF risks in a way appropriate for Japan, which has until now implemented the sanctions based on the UNSCRs and also taken its own measures (against North Korea).

2. Risk assessment approach

(1) FATF Guidance

When preparing the National Risk Assessment, we referred to the Guidance on Proliferation Financing Risk Assessment and Mitigation (hereinafter the “FATF PF Guidance”), published by 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.

¹¹ Regarding nuclear weapons, a report dated September 8, 2023 by the Institute for Science and International Security (ISIS), a U.S. private-sector research institution, pointed out that Iran retains the ability to break out and produce enough weapon-grade enriched uranium for a nuclear weapon in 12 days. and that Iran could produce enough weapon-grade uranium for an additional five nuclear weapons within the first month of a breakout. The report also pointed out that Iran possesses the largest number of ballistic missiles among the Middle Eastern countries. On May 25, 2023, Iran announced that it had successfully test-launched a Kheibar missile (range: 2,000 km; warhead payload: 1,500 kg), which is an improved version of the Khorramshahr ballistic missile. On June 3, the Iranian Revolutionary Guard Corps unveiled Fattah, Iran’s first hypersonic ballistic missile (range: 1,400 km; flying speed: Mach 13 to 15).



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 terrorism financing (hereinafter “MF/TF”), the PF-related risks are considered to be comprised of the following three factors.

Threat	Persons and entities that have previously caused or with 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 proliferation financing.
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 individuals or entities would be used without authorization for (including the possibility of causing reputational damages 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 amount of resources necessary to mitigate the different risks.

(2) Approach of the present National Risk Assessment

The present National Risk Assessment (hereinafter the National Risk Assessment) identified and analyzed the threats to and the vulnerabilities of Japan and conducted a multi-faceted, comprehensive risk assessment in view of the FATF PF Guidance, and in reference to the FATF Recommendations and their Interpretive Notes (which are collectively referred to by 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 and regions as of now, including the United States, the United Kingdom, and Australia), and reports by the Panel of Experts.

(3) 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: <https://www.npa.go.jp/>

Financial Services Agency: <https://www.fsa.go.jp/>

Ministry of Internal Affairs and Communications: <https://www.soumu.go.jp/>

Ministry of Justice: <https://www.moj.go.jp/>

Ministry of Foreign Affairs: <https://www.mofa.go.jp/mofaj/>

Ministry of Finance: <https://www.mof.go.jp/>

Ministry of Economy, Trade and Industry: <https://www.meti.go.jp/>

Ministry of Land, Infrastructure, Transport and Tourism: <https://www.mlit.go.jp/>

Japan Coast Guard: <https://www.kaiho.mlit.go.jp/>

Ministry of Defense/Self-Defense Forces: <https://www.mod.go.jp/>

(Reference 1) Inter-Ministerial Council for AML, CFT, and CPF Policy

https://www.mof.go.jp/policy/international_policy/councils/aml_cft_policy/index.html

Chapter 2 PF Threats

1. Premises

The FATF PF Guidance defines¹² the PF threat 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 and 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 also be equivalent to PF threats. The scope of assets that may be subject to sanctions include those indirectly owned or controlled by designated entities or individuals.

2. Threats in Japan

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

- (1) Actors involved in leakage of money
 - (i) Trades: Actors that import goods from North Korea via neighboring third countries
 - (ii) Persons: Actors that act as channels for overseas remittance to North Korea, such as supporters and related parties located in neighboring countries and other third countries
 - (iii) Actors that launch cyberattacks
- (2) Actors involved in leakage of technologies and goods
 - (i) Actors that earn money through trading dual-use products
 - (ii) Actors that earn money through leakage of technologies
 - (iii) Actors involved in illegal ship-to-ship transfers of goods
- (3) Actors that use resources of companies with opaque structures, including those that are sanctioned under the UNSCRs

¹² Guidance on Proliferation Financing Risk Assessment and Mitigation (2021) (21).

In the analysis, we assumed two possible cases—one in which funds are leaked from Japan for the purpose of developing WMDs and one in which goods and technologies are leaked from Japan for that purpose. We conducted analysis as to what sorts of persons and entities may be involved in such activity in each case.

(1) Actors involved in leakage of money

When funds are leaked from Japan for the purpose of WMD development, the assumptions are as follows with respect to the three possible cases of activity—trade (movement of goods), movement of people, and a cyberattack—and the actors (threats) involved in those activities.

(i) Actors that import goods from North Korea via third countries

As measures against North Korea based on the FEFTA, Japan has designated entities and individuals subject to asset freezing and other measures¹³ and subjected payments to those entities and individuals and capital transactions therewith to a licensing system. In addition, in order to enhance the prevention of fund transfers to North Korea, the payment conducted for the purpose of contributing to activities that could facilitate North Korea's nuclear and missile programs is banned. As an enhanced restriction of its own, Japan also ban on payment to North Korea. Furthermore, on the trade front, regarding North Korea, in addition to prohibiting imports and exports of specified goods based on the UNSCRs, Japan prohibits imports of all goods from and exports of all goods to North Korea, thereby preventing flows of funds through imports.

As a measure against Iran, Japan requires prior notification for investments in industries related to nuclear technology and also applies a permission system to payments made for the purpose of assisting activities that may benefit to its sensitive nuclear activities.

However, despite those restrictions, there are entities and individuals that conduct, or seek to conduct indirect trade transactions with or make indirect remittances to North Korea via third countries, including the neighboring countries. According to the Interpretative Notes of the FATF PF Guidance, such activities constitute illegitimate transactions whose financing is sourced from illegitimate activities, so they should be dealt with strictly as violations of laws and regulations.

In this respect, published data show that North Korea and Iran are actively engaging in trade with countries and regions such as China, Asia, the Middle East, and Africa, as described below. Regarding North Korea, the reports of the Panel of Experts pointed out that business entities related to Mansudae Overseas Project Group of Companies and Korea Paekho Trading Corporation have facilitated illicit labor and access to international financial systems in sub-Saharan Africa, and the Panel of Experts recommended that due diligence should be enhanced on contractors for development projects,

¹³ The individuals and entities designated by the UNSCRs have been designated by notifications issued by the Ministry of Foreign Affairs. As for detailed information, see Chapter 4.

especially those in sub-Saharan Africa that involve municipal loans, grants or foreign direct investment.

14

(Reference 2) North Korea's 10 major trade counterpart countries (2023)

(Unit: 1 thousand dollars. %)

Ranking	Country/region	Exports by North Korea		Imports by North Korea		Total trade value		Share
		Value	Rate of change	Value	Rate of change	Value	Rate of change	
1	People's Republic of China	292,450	118.8	2,428,653	73.6	2,721,103	77.6	98.27
2	Vietnam	9,170	△11.5	6,585	18.6	15,755	△1.0	0.57
3	India	2,757	160.1	1,870	184.6	4,627	169.5	0.17
4	Mozambique	3,167	486.5	-	△100.0	3,167	436.8	0.11
5	Austria	2,993	360.5	-	-	2,993	360.5	0.11
6	Angola	2,331	156.4	-	-	2,331	156.4	0.08
7	Tanzania	2,050	298.8	232	1,121.1	2,282	328.1	0.08
8	Nigeria	1,261	△25.0	900	△12.5	2,161	△20.3	0.08
9	Argentina	220	△62.5	1,171	△90.4	1,391	△89.1	0.05
10	Netherlands	61	190.5	1,165	△53.3	1,226	△51.3	0.04

(Source) KOTRA (Korea Trade-Investment Promotion Agency)

“2023 North Korea's 10 major trade counterpart countries”

(Reference 3) Iran's major trade counterpart countries (FY2023)

(Unit: 1 million dollars. %)

Ranking	Country/region	Export				Country/region	Import			
		FY2022	FY2023				FY2022	FY2023		
		Value	Value	Share	Rate of growth		Value	Value	Share	Rate of growth
1	People's Republic of China	14,733	14,157	28.2	△3.9	United Arab Emirates	18,553	20,987	31.4	13.1
2	Iraq	10,238	9,351	18.7	△8.7	People's Republic of China	15,838	18,682	27.9	18
3	United Arab Emirates	7,638	6,715	13.4	△12.1	Türkiye	6,157	7,678	11.5	24.7
4	Türkiye	6,203	4,211	8.4	△32.1	Germany	2,030	2,177	3.3	7.2
5	India	2,127	2,197	4.4	3.3	India	2,943	1,933	2.9	△34.3
*	Japan	13	11	0.0	△15.4	Japan	77	99	0.1	27.3

(Source) JETRO

Iran's export to major countries (non-oil sector) (customs base)

Iran's import from major countries (non-oil sector) (customs base)

(Notes)

1. Usually, the period of the fiscal year in Iran is from around March 21 to March 20 in the following year.
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.

¹⁴ Final report of the Panel of Experts submitted pursuant to resolution 2515(2020)

(Reference 4) Japan's major trade counterpart countries/regions (2023)

(Unit: 1 thousand dollars, %)

Ranking	Country/region	In terms of export by Japan	
		Value	Rate of change
1	United States	144,165,986	3.4
2	People's Republic of China	126,472,833	△13.1
3	Republic of Korea	47,030,210	△13.8
4	Taiwan	43,010,344	△18.2
5	Hong Kong	32,603,258	△2.5
6	Thailand	29,407,886	△10.1
7	Germany	19,385,085	△1.5
8	Singapore	18,856,278	△16.1
9	Vietnam	17,185,975	△8.2
10	Australia	16,790,621	1.0
11	India	15,961,410	14.5

Ranking	Country/region	In terms of import by Japan	
		Value	Rate of change
1	People's Republic of China	174,226,611	△8.3
2	United States	82,478,432	△8.3
3	Australia	65,322,571	△25.9
4	United Arab Emirates	37,038,032	△19.5
5	Taiwan	35,698,270	△8.4
6	Saudi Arabia	34,777,148	△19.2
7	Republic of Korea	31,064,476	△8.1
8	Vietnam	25,846,709	△2.6
9	Thailand	25,772,048	△4.0
10	Indonesia	24,474,299	△14.8
28	India	5,650,958	△14.1

(Source) JETRO “Japan's top 50 trade counterpart countries/regions in 2023”

(*) The countries/regions indicated in red are the ones indicated in Reference 2.

The government should continue to conduct checks based on the most up-to-date information and data with respect to the countries and regions actively engaging in transactions related to North Korea and items related to North Korea. It is also useful for private-sector business operators to take appropriate actions in accordance with the risks while paying particular heed to transactions related to the countries and regions and the items that require attention.

As mentioned above, in Japan, imports of all goods originating in or shipped from North Korea have been prohibited, but the following cases of illegal imports from North Korea have been observed.

Case 1: 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 Minister of Economy, Trade and Industry. In April 2007, they were arrested for violating the FEFTA (import without approval).

Case 2: In April 2007, three people, including an executive of a trading company imported sea urchins of North Korean origin without obtaining approval from the Minister of Economy, Trade and Industry. In January 2008, they were arrested for violating the FEFTA (import without approval).

Case 3: In December 2007, the president of a food sales company imported greenbrier of North Korean origin without obtaining approval from the Minister of Economy, Trade and Industry. In August 2009, the president was arrested for violating the FEFTA (import without approval).

Case 4: In September 2010, two people, including the president of a trading company, imported matsutake mushrooms of North Korean origin without obtaining approval from the Minister of Economy, Trade and Industry 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 Minister of Economy, Trade and Industry by falsely declaring them to be of Chinese origin in violation of the FEFTA Act (import without approval).

Case 5: In January 2020, three people, including the owner manager of a trading company imported freshwater clams of North Korean origin without obtaining approval from the Minister of Economy, Trade and Industry. In September 2024, they were arrested for violating the FEFTA (import without approval).

It has been pointed out that in recent years, countries and regions of concern (countries and regions raising particular international concerns due to their involvement in WMD proliferation) have continued the transfer of goods while evading international surveillance when illicitly exporting WMDs by employing sophisticated means, including document forgery and diversification of transportation routes.¹⁵ As of now, there has been no arrest case involving the smuggling of WMDs into Japan, but it is necessary to engage in international cooperation to prevent countries and regions of concern from engaging in indirect imports via third countries.

(*) Regarding remittances subject to the restrictions on the purpose of fund usage

Even when a remittance is made from Japan to a third country other than North Korea or Iran, it may constitute a breach of the abovementioned restrictions in cases where items related to nuclear power, chemical or biological weapons, or missiles are supplied, or financing for trade or leasing of those items is provided, or a remittance related to those activities is made from the third country to North Korea, if the remittance sender's purpose is to contribute to North Korea's transactions or activities related to those items. Regarding the restrictions on the purpose of fund usage imposed against Iran as well, a remittance made to a third country may constitute a breach of the restrictions in cases where items related to nuclear activities are supplied, or financing for trade or leasing of those

¹⁵ Ministry of Defense/Self-Defense Forces, Defense of Japan 2024, P. 198.

items is provided from, or a remittance is made from the third country to Iran, if the remittance sender's purpose is to contribute to Iran's transactions or activities related to those items.

(See Ministry of Finance Notification of Payment No. 1, vii and viii, and Ministry of Economy, Trade and Industry Notification of Payment Nos. 4 and 5).

- (ii) Actors that act as channels for overseas remittance to North Korea, such as supporters and related parties located in neighboring countries

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.

On the other hand, some neighboring countries/regions and other third countries/regions have not prohibited the entry of persons of North Korean nationality. Some of those countries/regions accept workers from North Korea. There is the possibility that remittances made from Japan to persons of North Korean nationality staying in those countries/regions may be equivalent to PF regardless of whether they are legitimate or illegitimate transactions. From that viewpoint, workers of North Korean nationality who have been dispatched by North Korean authorities to third countries, including neighboring countries, and who earn reward there, and entities that seek to make remittances to persons contributing to fund-raising related to PF activity conducted by North Korean authorities are considered to be threats.

In particular, according to the reports of the Panel of Experts and other sources, North Korea earns income by dispatching IT workers abroad and having them undertake contract work under false identity, and these income are used for nuclear and missile development by North Korea.¹⁶ As for Japan as well, the threat is growing. For example, North Korean IT workers are suspected to disguise themselves as Japanese nationals to undertake contract work using online platforms intended for order placements and receipts concerning contract work offered by Japanese companies. In this respect, a relevant UN Security Council resolution stipulates that all North Korean workers earning income in the UN member states shall be repatriated. Placing orders for contract work with North Korean IT workers working abroad and making payments for the services provided by them may constitute a violation of domestic laws, including the FEFTA.

In order to respond to this situation, it is important to deepen understanding about North Korean IT workers among Japanese companies and business associations and also to strengthen countermeasures taking into account the illegal schemes that have so far been detected. Therefore, in March 2024, the government of Japan issued an alert on North Korean IT workers to companies and other

¹⁶ Midterm report of the Panel of Experts submitted pursuant to resolution 2464 (2019)

organizations.¹⁷

The following cases related to North Korean IT workers have been observed.

Case 6: 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.

Case 7: In September 2024, two Japanese men were arrested on charges of illegal creation of private electronic records in relation. The men allegedly opened an account illegally at a securities company after informing a securities company with which they had concluded a contract that they would comply with the contract terms although, in fact, they conducted FX transactions using an automated trading system, an arrangement prohibited by the company, in conspiracy with a person presumed to be a North Korean IT worker.

Moreover, the report of the Panel of the Experts published in March 2024 pointed out that North Korean IT workers are generating an estimated 250 million to 600 million U.S. dollars for North Korea annually.¹⁸

In addition, in relation to the prohibition of payments to North Korea, it is required that special attention be paid to overseas remittances made to the three provinces of the People's Republic of China's northeastern region (Liaoning Province, Jilin Province, and Heilongjiang Province) because migrant workers from North Korea have traditionally stayed there.¹⁹ In foreign exchange inspections, the following cases of inadequacy have been observed.

Case 8: Regarding an overseas remittance, no confirmation has been implemented as to whether or not the beneficial owner of remittance recipient is resident of North Korea.

Case 9: When financial institutions performed the obligation for implementing confirmation regarding the prohibition-in-principle of payments to North Korea based on Article 17 of the FEFTA in relation to overseas remittances to the abovementioned three provinces in the People's Republic of China's northeastern region made for use as living expenses, they failed to consider

¹⁷ "Alert on North Korean IT workers for Companies and Other Organizations" (dated March 26, 2024; jointly issued by the National Police Agency, the Ministry of Foreign Affairs, the Ministry of Finance, and the Ministry of Economy, Trade and Industry).

¹⁸ Final report of the Panel of Experts submitted pursuant to resolution 2680 (2023)

¹⁹ The United Kingdom's national risk assessment of proliferation financing (published in September 2021) pointed out that North Korea front companies and agents were frequently shipping goods via Liaoning Province in the People's Republic of China.

the appropriateness of the remittance amount, to check who was the beneficiary of the living expenses, and to hold interviews concerning detailed circumstances such as the relationship between the remittance sender and the recipient.

Furthermore, the Panel of Experts has pointed out that North Korean workers were working and earning income in sectors such as IT, restaurant, healthcare, and construction in Africa, Asia, the Middle East, and Russia.²⁰ According to the report of the Panel of the Experts published in March 2024, more than 100,000 North Korean workers are working in sectors such as sewing, construction, healthcare, IT, and restaurants in around 40 countries, generating income for North Korea, and it is estimated that North Korean workers other than IT workers generate annual revenue of approximately 500 million dollars according to a UN member state. The report also noted that North Korean workers are initially dispatched abroad on a student or a tourist visas, with some of them using false nationalities and ID cards. If the borders reopen further, North Korea is expected to dispatch a large number of additional workers overseas and concluded contracts to dispatch 400,000 North Korean workers abroad.²¹

The government should continue to conduct checks based on all available, most up-to-date data as to whether or not there are countries/regions that require particularly strict examination. Private-sector business operators should also conduct strict examination regarding transactions while paying heed to countries/regions requiring attention.

(iii) Actors conducting cyberattacks

According to the reports of the Panel of Experts and other sources, the cyberattack group subordinated to the Reconnaissance General Bureau, North Korea's primary foreign intelligence service, is conducting cyberattacks on companies and government agencies in other countries in order to generate revenue for nuclear and missile development programs.^{22,23} The report of the Panel of Experts published in March 2024 pointed out that North Korea attack methodologies continue to include spearphishing, vulnerability exploits, social engineering and watering holes, in addition to ongoing targeting of the cryptocurrency industry.²⁴

The Report of the Panel of Experts quoted a report written by a cybersecurity company that the total amount of crypto assets stolen by North Korea in 2023 was approximately 1.0 billion U.S. dollars.²⁵

²⁰ Midterm report of the Panel of Experts submitted pursuant to resolution 2680 (2023), Midterm report of the Panel of Experts submitted pursuant to resolution 2627 (2022)

²¹ Final report of the Panel of Experts submitted pursuant to resolution 2680 (2023)

²² Midterm report of the Panel of Experts submitted pursuant to resolution 2627 (2022)

²³ Ministry of Defense/Self-Defense Forces, Defense of Japan 2024, P. 187

²⁴ Final report of the Panel of Experts submitted pursuant to resolution 2680 (2023)

²⁵ An analysis conducted by Chainalysis (The 2024 Crypto Crime Report).

In Japan as well, threats related to cyberspace have continued to be very serious in recent years, with the number of cleared cases involving cybercrime in 2023 hitting a record high of 12,479.²⁶

The “Alert: cyberattacks against crypto-related companies by cyberattack group called Lazarus²⁷, which is believed to be a subordinate organization of the North Korean authority,” issued by the National Police Agency, the Financial Services Agency, and the National center of Incident readiness and Strategy for Cybersecurity (NISC) in October 14, 2022, described that it is strongly presumed that a cyberattack group in which North Korea is suspected to be involved (“Lazarus”) is launching cyberattacks targeting Japanese crypto asset exchange service providers and others.²⁸

It is also described that these cyberattack groups make it difficult to trace by using “mixer” to scramble the history of transactions on blockchains, when they transfer their stolen crypto assets.

In actual cases, crypto assets have been used to pay for DDoS attacks,²⁹ such as when a DDoS attacker demanded payment in crypto assets³⁰ and threatened that a more large-scale attack would be launched if not paid. The reports of the Panel of Experts pointed out that it has become difficult to trace funds stolen through North Korea’s cyberattacks targeted at crypto asset exchanges, and the lack of global framework that cover crypt assets can pose significant challenges to investigation of the stolen funds.³¹

²⁶ National Police Agency, White Paper on Police 2024.

²⁷ Cyberattack techniques used by Lazarus include social engineering, whereby the group gains access to targeted companies’ networks by causing malware infection through means such as: sending to employees of targeted companies phishing emails disguised as messages from senior officials of the companies; and using false SNS accounts to approach employees of targeted companies pretending to propose transactions.

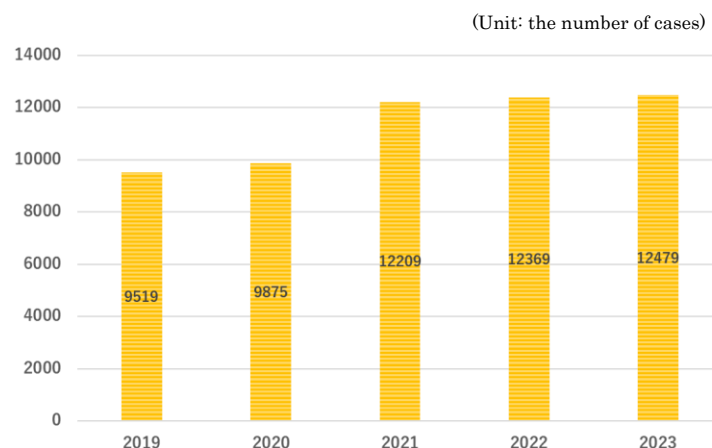
²⁸ National Police Agency, Financial Services Agency, and National center of Incident readiness and Strategy for Cybersecurity, “Regarding cyberattacks by the Lazarus cyberattack group, a subordinate organization of North Korea authorities, that are targeted at business operators related to crypto assets (alert)”

²⁹ A DDoS (distributed denial of service) attack refers to the use of multiple computers to implement a massive amount of DoS attacks, overwhelming websites and servers by causing an excessive amount of access or by sending an excessive volume of data.

³⁰ For example, in the United States, Colonial Pipeline was struck by a ransomware attack in 2021 and paid a ransom in the form of bitcoin, a crypto asset. In Japan, the system of a crypto asset exchange operated by a Japanese company was illicitly accessed from the outside in 2018, with the result that around 58 billion yen’s worth of crypto assets were illicitly transferred.

³¹ Midterm report of the Panel of Experts submitted pursuant to resolution 2627 (2022)

(Reference 5) Changes in the number of cleared cybercrime cases



(Source: National Police Agency)

(2) Actors involved in leakage of technologies and goods

Next, let us consider possible cases in which goods and technologies are leaked from Japan for the purpose of WMD development and assume persons who seek to acquire funds through the activity and other persons involved to be potential threats. As mentioned earlier, in particular, Japan possesses advanced technologies and goods that take advantage of those technologies, and if those technologies and goods have been transferred to countries engaging in WMD development, that may pose an international threat, leading to the instability of the international situation.

(i) Actors that earn money through trading dual-use products

Regarding North Korea, Japan has prohibited not only imports and exports of specified goods based on the UNSCRs but also exports of all goods destined for North Korea.

In Japan, there are high-quality, high-technology dual-use products that can be used for either civilian or military applications, so when those products have been 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 evidence destruction and sanctions evasion and circumvention become easy. Therefore, trade in dual-use products is considered to constitute a PF threat.³²









³² Separately, there is the End User List, published by the Ministry of Economy, Trade and Industry, that names companies and organizations over which there are concerns about possible involvement in WMD development and other illicit activities. Exporting goods to companies on the list requires a license from

The areas where Japan has a technological advantage include semiconductor-manufacturing equipment and high-performance electronic parts. In addition, computing technology, including advanced software and integrated circuits, and quantum computing technology used for decrypting crypto assets, are considered to pose a high PF risk.³³

Although the Ministry of Economy, Trade and Industry informs the public about what sorts of items require prior export license, there are cases in which private-sector companies import or export those products due to a lack of sufficient understanding, with the result that their transactions are regarded as regulatory violations.

The Ministry of Economy, Trade and Industry has been conducting outreach toward small and medium-size enterprises in order to maintain international peace and prevent technology leakage, not to mention prevent violations of laws and regulations.

(Reference 6) Uses of concern and civilian uses of dual-use products

	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) Extracted from a reference material prepared by the Ministry of Economy, Trade and Industry

the Minister of Economy, Trade and Industry except when it is clear that those goods are not used for WMD development or other illicit activities. As of November 9, 2022, 147 North Korean companies and organizations and 223 Iranian companies and organizations were on the End User List.

³³ Ministry of Economy, Trade and Industry, “Revised Action Plan for Strengthening Industrial and Technological Infrastructure Related to Economic Security,” P.19.

(Reference 7) Examples of goods at high risk of being used for WMD development

Items	Uses of concern	Items	Uses of concern
1. Tributyl phosphate (TBP)	Nuclear weapons	25. Equipment designed for producing prepregs	Missile
2. Carbon/Glass/Aramid fiber	Nuclear weapons, missile	26. Artificial graphite	Nuclear weapons, missile
3. Titanium alloys		27. Gyroscopes	Missile
4. Maraging steel		28. Rotary encoders	
5. Aluminum alloys tubes with a diameter of more than 75 mm	Nuclear weapons	29. Heavy trucks (incl. tractors, trailers, dump trucks)	
6. Flow-forming machines	Nuclear weapons, missile	30. Crane trucks	Biological weapons
7. Numerically-controlled (N/C) machine tools		31. Chambers (sealed) for fermentation	
8. Isostatic presses		32. Centrifugal separators	
9. Filament winding machines	Nuclear weapons	33. Freeze dryers	Missiles, chemical weapons
10. Frequency changers		34. Corrosion-resistant reactors	
11. Mass spectrometers or ion sources		35. Corrosion-resistant agitators	
12. Vibration test systems	Nuclear weapons, missile	36. Corrosion-resistant heat exchangers or condensers	Missiles, biological/chemical weapons
13. Centrifugal multiplane balancing machines		37. Corrosion-resistant distillation or absorption columns	
14. Corrosion-resistant pressure gauges/sensors		38. Corrosion-resistant filling equipment	
15. Large-size non-destructive inspection equipment	Nuclear weapons	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
16. High frequency oscilloscope and waveform digitizers		40. Spray machines that are specially designed for installing in UAVs	
17. Stable power/voltage DC power supplies		41. N-(1-phenethyl-4-piperidyl)propionanilide (also known as fentanyl) (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
18. Large generators	Nuclear weapons, missile		
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			

(Source) An extract from the Security Export Guidance (Introduction), Ministry of Economy, Trade and Industry.

The following cases of regulatory violations and deficiencies have been detected.

Case 10: 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 Minister of Economy, Trade and Industry while knowing that the product might be used for the development of nuclear weapons.

Case 11: On April 4, 2003, Company C 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 Minister of Economy, Trade and Industry.

Case 12: 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 Minister of Economy, Trade and Industry, while knowing that the products might be used for the development of nuclear weapons.

Case 13: In November 2003, Limited Company A exported an inverter (frequency changer) that might be used for the development of nuclear weapons to North Korea via the People's Republic of 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 Minister of Economy, Trade and Industry.

Case 14: Company D exported vacuum suction pressure casting machines and other products that it had manufactured to Iran, the People's Republic of China, and Thailand, among other countries, without obtaining a license from the Minister of Economy, Trade and Industry between 2007 and 2016.

Case 15: In January 2008, the representative director of a trading company handling trade with North Korea illicitly exported two used tank trucks to the Republic of Korea (ROK)—despite having been notified of the need to obtain an export license from the Minister of Economy, Trade and Industry 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.

Case 16: Company B exported one jet mill to Iran in each of 1999 and 2000 without obtaining a license from the Minister of Economy, Trade and Industry although the product might be used for the development of missiles.

Case 17: 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 Minister of Economy, Trade and Industry, thereby providing services made available by the program.

In addition to the possibility that companies may be unintentionally violating regulations, there is also the possibility that as a result of the increasing complexity of distribution structures, entities of concern may be using various techniques in order to acquire sensitive technologies and goods and technologies that may be converted to military applications while hiding the identity of real end users.

There are also cases in which such technologies and goods are resold to countries developing WMDs and conventional weapons despite the implementation of legitimate procedures in Japan as a result of being routed via third countries where export control is not strictly enforced.

Case 18: In 2014, one of the reports of the Panel of Experts revealed that carbon fibers manufactured in Japan and shipped to Iran from the People's Republic of China had been confiscated in a third country before arriving in Iran.³⁴ 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 a 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 the People's Republic of China based on appropriate procedures, 7,200 kilograms of the material were resold to Iran and transported by ship to the country in the latter half of 2012.

In the meantime, the government should continue efforts to announce and raise awareness about cases of regulatory violation and make improvements to the ways of informing the public and measures that may be taken while receiving feedback from private-sector companies.

When companies involved in trade check whether or not certain transactions are related to PF, it is useful to examine the following checkpoints for suspicious transactions.³⁵

- Whether the customers are conducting trade transactions regarding dual-use products, products subject to export control or equipment not related to their technical backgrounds, or complex equipment that is not consistent with their businesses. Whether the customers use individuals' accounts for the payment for the products. Whether the customers affiliated with universities and research institutions are handling dual-use products or products subject to export control.
- Whether customers that are manufacturing or trading companies use cash in transactions regarding industrial products or other trade transactions. Whether the outstanding amounts of deposits in their deposit accounts increased steeply, followed by cash withdrawal, as an indication of the possibility of such transactions being conducted.

³⁴ Final report of the Panel of Experts submitted pursuant to resolution 2141 (2014)

³⁵ Examples cited in the Frequently Asked Questions Concerning the Guidelines on Compliance with Foreign Exchange Laws and Regulations for Foreign Exchange Service Providers, published in November 2023.

- Whether the trade transaction counterpart at the final destination of delivery is a transportation company or a company other than the importer.
- Whether the declared price of the cargo is low compared with the transportation cost.
- Whether a product whose quality is not consistent with the technological level of the country of destination is being exported.
- Whether multiple places of destination have been indicated with no apparent purpose. Whether the flag of registry of a ship is changed frequently. Whether products are transported through roundabout means, including the use of a small or obsolete ship. Whether products are routed via a country of concern.
- Whether the customers request the issuance of a letter of credit related to dual-use products or products subject to export control before approval is given for the opening of an account.

Regarding products other than dual-use items, including daily goods such as food and clothing, there are entities engaging in illicit exports and indirect exports to North Korea via third countries, and those entities and others involved in remittances made thereby may be considered to be potential threats. For example, there have been the following cases.

Case 19: 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.

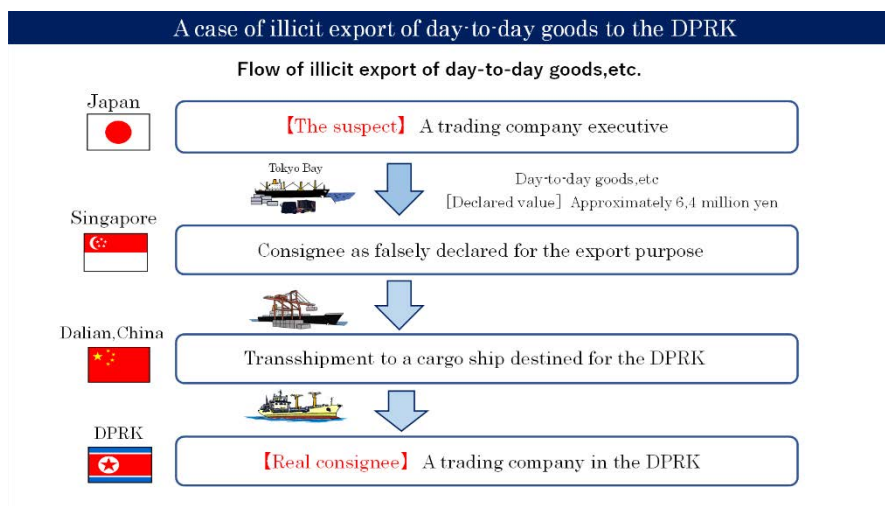
Case 20: In January 2017, a former trading company manager was found to have exported furniture and other goods to North Korea via Hong Kong and Dalian in the People's Republic of China despite the prohibition of all goods destined for North Korea that was introduced on June 18, 2009, and the former manager was arrested in August 2019 for having violated the FEFTA (unapproved export).

Case 21: In September 2024, a man who was formerly the owner manager of a fishery processing company was arrested for violating the FEFTA (export without approval). The man allegedly exported clothing and other goods to North Korea via the People's Republic of China in December 2019 without obtaining approval from the Minister of Economy, Trade and Industry despite the ban on exports of all goods to North Korea, which had been in place since June 18, 2009.

Although the above cases are rare, it is possible that even companies that are good corporate citizens may be involved in indirect exports to North Korea because of problems such as a lack of sufficient knowledge regarding the FEFTA and other laws and regulations and management resource deficiencies. Indeed, indirect export techniques are becoming increasingly sophisticated, as

exemplified by the use of two locations as transit points for indirect routing in a case of illicit export to North Korea.

(Reference 8) A case of illicit export of day-to-day goods, etc. to North Korea



(Source: National Police Agency)

(Reference 9) 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 export

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 the measures implemented against North Korea, published by the National Police Agency, major counterpart countries/regions (places of destination and transit) are as follows (the countries/regions underlined are places of destination and transit in cases in which administrative punishments were imposed in and after 2018).

Category	Specific country/region
Places of destination	<u>North Korea</u> , <u>People's Republic of China</u> , Republic of Korea, Union of Myanmar, Kingdom of Thailand, Republic of Singapore, Malaysia, Iran, Philippines, Indonesia, United States, East Germany (German Democratic Republic), Poland
Places of transit	<u>Hong Kong</u> , <u>People's Republic of China</u> , <u>People's Republic of China (Dalian)</u> , Republic of Korea, Republic of Korea (Busan), Republic of 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 are the

ones observed in cases in which administrative punishments were imposed in and after 2018).

Legal persons
<ul style="list-style-type: none"> ● <u>Trading companies (e.g., chemicals, construction materials, PCs, seafood, day-to-day goods, machinery and equipment, and automobiles)</u> ● <u>Manufacturing companies (e.g., semiconductors, electronic equipment, transportation machinery, and textiles)</u> ● <u>Industrial waste delivery companies</u> ● <u>Transportation companies</u> ● <u>EC site operating companies</u> ● <u>Retail companies</u> ● <u>Travel agencies</u>

Natural persons
<ul style="list-style-type: none"> ● <u>Company executives</u> ● <u>Former company executives</u> ● <u>Travelers from North Korea</u> ● <u>Unemployed youth</u> ● <u>Officials related to Japan-North Korea friendship associations</u>

As described above, there have been cases of illegal exports of dual-use items and daily goods from Japan to North Korea and exports of such goods from Japan to North Korea via third countries. The techniques used for such illegal exports are becoming more and more sophisticated, so entities that earn funds by providing dual-use and other goods and entities involved in remittances made thereby may be considered to be potential threats.

(ii) Actors that earn money through leakage of technologies

Japan possesses information related to advanced technologies used around the world and manufactures cutting-edge, high-performance products. Some of those technological information and products may be diverted to military applications depending on the method of usage. There are also concerns over intangible technology transfer, a practice whereby countries 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 activity is conducted in a legitimate manner, the technologies thus obtained may be exploited for WMD proliferation. From the viewpoint of the FEFTA, the following cases of deficiency, for example, have been pointed out.

Case 22: 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 activity, and this was recognized as a case of deficiency in foreign exchange inspection under the FEFTA.

(iii) Actors obtaining the funds and those involved in their remittance through activities such as illegal ship to ship transfers

Japan is an island nation all four sides of which is surrounded with the seas—the Pacific Ocean, the Sea of Okhotsk, the Sea of Japan, and the East China Sea—so the cross-border movement of people and goods is routed via seaports and airports.

According to the reports of the Panel of Experts, refined petroleum products have been delivered through illegal ship-to-ship transfers in North Korea’s territorial waters and exclusive economic zone.³⁶ In this respect, under the UNSCRs, all UN member countries are prohibited from facilitating or engaging in supply, sales, or transfers, including ship-to-ship transfer, of any type of goods or items to or from North Korea (UNSCR No. 2375-11, etc.). In accordance with the prohibition, as part of monitoring and surveillance activities, the Ministry of Defense and the Japan Self-Defense Forces (JSDFs) are using JMSDF vessels and other assets to conduct information gathering activities for vessels suspected of violating the UNSCRs.

So far (as of the end of August 2024), the Ministry of Defense has disclosed 24 strongly suspected cases of ship-to-ship transfers banned by UNSCRs. There has not been any case of ship-to-ship transfers or smuggling of goods or persons related to North Korea’s PF activity that was exposed by the Japan Coast Guard. Moreover, as of the end of December 2023, there had not been any case of activities by a suspicious ship or spy ship³⁷ from North Korea that was exposed by the Japan Coast Guard and that was judged to be related to WMD development.

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

³⁷ As of the end of December 2023, the Japan Coast Guard had observed 21 suspicious ships and spy ships since its establishment in 1948. Those suspicious ships and spy ships are highly likely to have been involved in serious crime, such as smuggling of illegal drugs and spies’ illegal entry into and departure from Japan, as exemplified by a spy ship incident that occurred in 2001 in the maritime area southwest of Kyushu. Therefore, it is an important task to prevent the activities of suspicious ships and spy ships that threaten Japan’s security.

(Reference 10) Illicit ship to ship transfers of goods by North Korea-related ships ³⁸

	Names of tankers of North Korean nationality	Names of ships 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

*Until now, a total of 24 cases of illicit ship-to-ship transfer of goods have been confirmed, with each docking counted as one case of ship-to-ship transfer.

However, as the border control measures introduced due to the COVID-19 pandemic were relaxed from October 2022, resulting in a gradual recovery in the cross-border movement of goods and people, as exemplified by the resumption of acceptance of the entry of cruise ships, the risk of smuggling being conducted through ship-to-ship transfer under the cover of increasing ship traffic poses a significant threat.

When the illicit ship-to-ship transfer operation is conducted, it is highly likely that cash transactions not involving financial institutions³⁹ as intermediaries are used for the payment, so it is likely very difficult for financial institutions, etc. to conduct strict checks. However, it is possible to conduct intensive verification in cases where the use of cash by a customer who is a manufacturing company or trading company for transactions regarding industrial products and other goods has been detected, or where a rapid increase in the balance of a deposit account followed by cash withdrawal has been detected as a sign of such activity.⁴⁰

³⁸ The website of the Ministry of Defense/Self Defense Forces.
<https://www.mod.go.jp/j/approach/defense/sedori/index.html>

³⁹ 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. (Strategic Policy towards Promoting AML/CFT/CPF, p. 12).

⁴⁰ See “Frequently Asked Questions Concerning the Guidelines on Compliance with Foreign Exchange Laws and Regulations for Foreign Exchange Service Providers,” published in November 2023.

(3) Actors that use resources of companies with opaque structures, including those that are sanctioned under the UNSCRs

Finally, let us conduct an analysis as to what types of entities and persons may be involved in activity in possible cases of funds, goods, or technologies being leaked from Japan.

In Japan, based on the UNSCRs,⁴¹ etc., the names and addresses of the designated entities and the names, job titles, birthdates, nationality, and addresses of the designated individuals have been made public.⁴² Regarding the sanctions regarding North Korea, the individuals and entities that are involved in or provide support for programs related to nuclear and other WMDs or missiles have been designated as subject to asset freezing and other measures. For example, the designated individuals and entities include those involved in illicit transactions regarding refined petroleum products and coal conducted through ship-to-ship transfers, which are prohibited by the UNSCRs. Regarding Iran, individuals and entities designated⁴³ as subject to the sanctions have mainly been those which have engaged in, directly associated with or provided support for Iran's proliferation sensitive nuclear development.⁴⁴

Until now, there has not been any PF-related arrest case involving the sanctioned entities and persons, but a close watch should be kept on the risk as a threat.

As for the means of fund transfer used for the provision of funds for WMD proliferation, the use of front companies and joint ventures 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, opaque ownership structures for the purpose of violating the sanctions. In addition, the report of the Panel of Experts published in October 2023 recommended that member countries should keep vigilance against North Korea's evasion of the financial sanctions through the use of front and subordinate companies by North Korea organizations designated by the United Nations.⁴⁵

⁴¹ The website of the Ministry of Foreign Affairs
https://www.mofa.go.jp/mofaj/gaiko/unsr/page3_003268.html

⁴² The website of the Ministry of Finance.
https://www.mof.go.jp/policy/international_policy/gaitame_kawase/gaitame/economic_sanctions/list.html

⁴³ The application period of the asset freezing and other measures imposed against the entities and individuals designated by the Attachments of the UNSCR 2231, which constitute the basis of the Ministry of Foreign Affairs notification that designates the sanctioned persons and entities, expired on October 18, 2023, so the Ministry of Foreign Affairs notification was abolished on October 27.

⁴⁴ Regarding the activities subject to the sanctions imposed against Iran, the designation of the "development of nuclear weapon delivery systems" as a sanctioned activity based on the UNSCRs was removed following the passage on October 18, 2023, of eight years after "Adoption Day" of the Joint Comprehensive Plan of Action. As a result, on October 27 of the same year, a relevant Ministry of Finance notification was amended to remove the restriction on the purpose of fund usage regarding the development of nuclear weapon delivery vehicles based on the FEFTA.

⁴⁵ Most recently, 2023 final report was published on March 21, 2024, providing a detailed report on and analysis of suspected cases of breach and evasion of the sanctions and the techniques of breach and evasion

Moreover, reports by the Panel of Experts recommended that the regulation of the registration of companies with opaque structures should be tightened.⁴⁶ In particular, the report published in August 2020 pointed out the following specifics: that North Korea gained access to international financial systems by using joint ventures, offshore bank accounts, shell companies, and crypto assets; and that individuals and entities related to North Korea were using small and medium-size banks in East and Southeast Asia for making international remittances.⁴⁷ A report published in March 2024 by the Panel of Experts also pointed out that North Korea continued to gain access to international financial systems and conduct illegal financial activity in violation of the U.N. Security Council resolutions.⁴⁸ The report also pointed out that: the situation was getting worse because of countries inadequately addressing domestic corporate registration rules; North Korea was continuing activity while hiding behind opaque corporate structures; and such loopholes make compliance regarding the sanctions and “know your customer” onboarding processes and procedures at financial institutions practically impossible.⁴⁹

As to the treatment of companies whose ownership structure and activity are lacking in transparency, as a prerequisite, the supervisory authorities should have timely access to information on beneficial ownership of legal persons.⁵⁰ While FATF Recommendation 24 and its Interpretative Note constitute a FATF standard concerning ML/TF, this is also a standard applicable as an approach to PF activity, whose financing may be sourced from either legitimate or illegitimate activity. Japan has so far developed institutional systems to check information on beneficial ownership of legal persons.

FATF Recommendation 24 and its Interpretative Note were revised in March 2022 in order to introduce a stricter international standard from the viewpoint of preventing abuse of legal persons. Specifically, as a mechanism for the investigative authorities to identify beneficial owners of legal persons in a timely manner, countries are required to: (i) obligate legal persons to obtain and hold information on their beneficial ownership (so-called company approach); (ii) obligate public organizations (e.g., tax authorities, financial information institutions, and registry organizations) to hold information on beneficial ownership (registry approach); or (iii) obligate the introduction of an

used by North Korea. Like the previous reports, the midterm report pointed out the following: (i) North Korea’s continuation of nuclear and ballistic missile programs, (ii) North Korea’s continuation of exports of coal and imports of refined petroleum products, and (iii) strong suspicion that companies and other organizations from the Russia and People’s Republic of China were involved in North Korea’s breach and evasion of the sanctions.

⁴⁶ Final report of the Panel of Experts submitted pursuant to resolution 2515 (2020), Midterm report of the Panel of Experts submitted pursuant to resolution 2515 (2020)

⁴⁷ Midterm report of the Panel of Experts submitted pursuant to resolution 2515 (2020), Midterm report of the Panel of Experts submitted pursuant to resolution 2569 (2021)

⁴⁸ Final report of the Panel of Experts submitted pursuant to resolution 2680 (2023)

⁴⁹ Midterm report of the Panel of Experts submitted pursuant to resolution 2515 (2020), Midterm report of the Panel of Experts submitted pursuant to resolution 2569 (2021)

⁵⁰ A Beneficial Owner is a person in a relationship that makes it possible to substantially control the business management of a legal entity, such as a natural person who is deemed to directly or indirectly hold more than one-quarter of the total number of voting rights of the legal entity.

alternative mechanism. The forthcoming fifth round of mutual evaluation of Japan will be conducted based on the revised FATF standards, so action should be taken promptly to adapt to the revision.

In order to prevent PF, it is necessary to obligate legal persons to obtain and hold information on their beneficial ownership and develop mechanisms to update the information and to enable public organizations to hold the information, or alternative mechanisms. Relevant ministries and agencies should cooperate in considering possible actions, including using an existing framework as the first step (as for specific activities, see Chapter 4).

In addition, when companies whose ownership structure or activity is lacking in transparency are included among the customers, remittance recipients, and other persons involved in transactions handled by financial institutions, it is important to conduct intensive checks as to the companies' ownership structure and status of business in order to ensure that the beneficiaries of the remittance transactions are not those who are subject to the sanctions.

Chapter 3 PF vulnerabilities and risks

1. Premises

The FATF PF Guidance defines PF vulnerability as follows:⁵¹

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 the entities and individuals designated by the relevant UNSCRs. As for vulnerabilities, countries are required to conduct evaluation concerning the weak points of the set of measures that they are implementing and 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 Japan⁵², published in August 2021, stated that Japan is exposed to a considerable PF vulnerability due to its geographical proximity to North Korea, its significant role as an international financial center, and its important presence in international trade, among other factors.

—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 neighbouring jurisdictions) and Japan's role as a regional and global financial centre, with an important role in international trade.**

2. Japan's vulnerabilities

In light of the above, let us look at Japan's vulnerabilities as classified below.

- (1) Geographical proximity to North Korea
- (2) Globally significant international financial center
- (3) Major industrial center and open economy regime

⁵¹ Guidance on Proliferation Financing Risk Assessment and Mitigation (2021).

⁵² https://www.mof.go.jp/policy/international_policy/amlcftcpf/3.efforts.html

(1) Geographic proximity to North Korea

The geographical proximity between Japan and North Korea is considered to make Japan more vulnerable than other countries to a PF risk associated with the flow of goods and people.

As Japan is an island country, the cross-border movement of people and goods is through seaports and airports,⁵³ and maintaining trade with other countries, in terms of both quality and quantity, is essential given the scarcity of domestic energy resources. Because of the geographical closeness to North Korea, while there have historically been wide-ranging flows of human and goods to and from the Korean Peninsula, Japan is exposed to the risk that PF-related trade may be conducted and funds may be transferred via neighboring countries that have deep relationships with North Korea. In addition, it is possible that entities conducting trade or remittance transactions with North Korea via third countries or implementing illegal ship-to-ship transfer of goods may exploit this situation, as mentioned in the previous chapter.

(2) Globally significant international financial center

As a major global financial center, Japan has an advanced financial sector, where considerable volumes of financial transactions are conducted. Specifically, the Tokyo Stock Exchange is a major global exchange in terms of the market capitalization of listed companies: for example, the total market capitalization of companies listed on the Tokyo Stock Exchange is the second largest of the major exchanges across the world, after the total market capitalization for the New York Stock Exchange.⁵⁴ In addition, the Japanese financial system, with its extensive nationwide network, provides easy access and enables quick and secure transfers of funds.⁵⁵ Of the 29 Global Systemically Important Banks (G-SIBs) designated by the Financial Stability Board (FSB) in 2023, three are Japanese megabanks. Moreover, the overall outstanding amount of investment assets in Japan is increasingly considerably,⁵⁶ and in particular, there is an abundance of financial assets held by individuals.⁵⁷

On the other hand, Japan's globalized, highly advanced economic environment provides entities and persons aiming to get involved in PF with various means and methods of PF—as in the case of ML/TF—a situation that could constitute a vulnerability. From among the various types of transactions,

⁵³ National Public Safety Commission, the 2024 edition of the National Risk Assessment-Follow-up Report, p. 10

⁵⁴ As of the end of December 2023, the total market capitalization of stocks in Japan was approximately 867 trillion yen (the 2024 edition of the National Risk Assessment-Follow-up Report).

⁵⁵ The number of branches operated by major financial institutions as of the end of March 2023 was 37,293 (including 172 foreign branches), while the number of ATMs installed was approximately 88,000. As a result, access to the financial system is easy (the 2024 edition of the National Risk Assessment-Follow-up Report).

⁵⁶ A relevant paragraph was extracted from the “Business Opportunities” section of the Financial Services Agency's website.

⁵⁷ The value of investment assets in Japan increased from approximately 222 trillion yen in 2011 to approximately 518 trillion yen in 2020. The value of household financial assets in Japan (as of the end of March 2022) is 2,005 trillion yen.

products, and services that exist around the world, those entities and persons choose the ones that are best suited to them. While funds used for PF may be sourced from either legitimate or illegitimate activity, Japan's position as a major international financial center in Asia suggests the possibility that PF-related transactions may be conducted through the Japanese financial system.⁵⁸

(3) Major industrial center and open economy regime

As Japan is the fourth largest trading power in the world, it actively conducts transactions with the rest of Asia, which is vulnerable to the risk of North Korea's PF activity. Therefore, there is the risk that under the cover of trade transactions involving Japan, North Korea's products may be procured by other countries, or foreign products may be exported to North Korea via third countries. In addition, as such procurement activity is becoming more and more complex and sophisticated, indirect exports via third countries have emerged as a challenge for catch-all control.⁵⁹ In addition, as Japan is an industrial center where companies possessing advanced technologies are concentrated,⁶⁰ it is at a comparative advantage against other major countries in terms of the manufacturing of finished products, such as transportation equipment and general machinery, whose production involves such a diverse range of processes that only a limited group of countries have manufacturing capacity.⁶¹ Therefore, Japan is a trade center where parts and semi-finished products (intermediate goods) from various countries are concentrated, so it has a vulnerability in that it is liable to be targeted by entities that try to exploit Japanese companies' high-level technologies and products for WMD development.

Japan had conducted a large amount of trade with Iran. On the import side, the main transaction items have been oil, gas, and petrochemical products procured from Iranian state-owned companies, and on the export side, the main items have been automobiles and electric products. Since 2019, exports to Japan have decreased steeply, with exports of oil and gas from Iran to Japan suspended.

On the other hand, the two countries have maintained their trade relationship to some degree, so

⁵⁸ The Financial Services Agency published the "Current State of and Challenges for Countermeasures against ML/TF/PF" (June 2023). The report provides overviews of responses made by business operators under the Financial Services Agency'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.

⁵⁹ Interim Report of the Subcommittee on Security Export Control Policy under the Trade Committee of the Industrial Structure Council (April 2024). "Catch-all control" refers to a system that requires exporters to obtain permission for exporting goods or providing technologies from the Minister of Economy, Trade and Industry 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.

⁶⁰ In terms of the Atlas of Economic Complexity (an indicator of economic complexity and capacity to export products with diverse value added), compiled by Harvard University, Japan continued to be ranked No. 1 in 2000 through 2021.

⁶¹ Cabinet Office, Annual Report on the Japanese Economy and Public Finance, Chapter 3, Section 1 "Changes in Japan's trade and investment structures."

there are concerns that Japan may continue to be exposed to the risk of PF-related trade and capital transactions which would be conducted by neighboring countries that have deep relationships with Iran.

(Reference 11) Total value of Iran's trade with Japan

(Unit: 1 million yen)

		2016	2017	2018	2019	2020	2021	2022	2023
Exports to Japan		362,048	400,866	381,068	126,925	3,618	4,178	4,626	4,336
Item-by-item breakdown	PETROLEUM	355,676	392,539	370,966	121,658	-	-	-	-
	TEXTILE YARN, FABRICS	2,694	2,837	3,229	3,140	2,275	3,118	3,281	2,423
Imports from Japan		63,165	98,468	76,958	7,246	8,561	7,687	6,559	9,062
Item-by-item breakdown	ELECTRICAL MACHINERY	3,882	13,876	5,066	606	2,871	1,732	1,471	3,213
	TRANSPORT EQUIPMENT	25,981	34,797	19,017	185	98	44	77	179

(Source) Ministry of Finance, Trade Statistics

3. Transactions with high PF risk

In light of the abovementioned vulnerabilities and the threats explained in the previous chapter, let us look at high-risk transactions that require particular attention in the context of PF.

The types of transactions with higher risks:

(i) Crypto asset transactions, (ii) non-face-to-face transactions, (iii) overseas remittances, (iv) export transactions related to dual-use products, and (v) transactions related to technology transfers that contribute to WMD development

The factor that heightens the level of risk involved in the abovementioned transactions: cyberattacks

First, crypto asset transactions pose higher risks compared with other transactions given the difficulty of tracing crypto assets, the presence of technology that increases the anonymity of such transactions, and the absence of a global regulatory mechanism regarding crypto assets.

Second, non-face-to-face transactions pose higher risks compared with other transactions as the absence of direct contact with transaction counterparts limits the availability of information on the

counterparts compared with face-to-face transactions and makes it impossible to make judgment as to the doubtful points of transactions based on direct checks regarding the counterparts' identification documents, gender, facial features, and verbal and physical behavior, etc.

Third, remittances to countries and regions where entities and persons subject to asset freezing and other measures for their involvement in the development, possession and export of WMDs (nuclear, chemical and biological weapons) and to the neighboring countries may include transactions that are equivalent to PF regardless of whether the funds are sourced from legitimate or illegitimate activity, so overseas remittances involve high risk compared with other transactions. Indeed, there are neighboring and third countries and regions that have not prohibited the entry and departure of persons of North Korea nationality, and some of those countries and regions accept workers from North Korea. Remittances made from Japan to persons of North Korean nationality located in those countries and regions may include transactions that are equivalent to PF regardless of whether the funds are sourced from legitimate or illegitimate activity. From that viewpoint, remittances made to persons of North Korean nationality located in neighboring countries involve high risk.

Moreover, in Japan, there are high-quality, high-technology, dual-use products that can be used for both civilian and military applications. When those products have been 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 evidence destruction and sanctions evasion and circumvention become easy. Therefore, trade in dual-use products is considered to be a PF threat. Japan also possesses information related to advanced technologies used around the world and manufactures cutting-edge, high-performance products. Some of those technological information and products may be diverted to military applications depending on the method of use. The areas where Japan has a technological advantage include manufacturing equipment/parts/materials/devices, and aircraft parts/materials, and those technologies are liable to become targets of technology acquisition and are at a particularly high risk of technology leakage.⁶² Attention should be paid to import and export transactions related to dual-use products and transactions related to technology transfers that contribute to WMD development.

When financial institutions, etc. conduct risk assessment regarding PF and take necessary actions subsequently, it is important to appropriately confirm the actual circumstances, trade flows, and fund flows of customers and refuse to handle transactions upon necessity. To do so it is useful to prescribe the procedures for those activities while focusing attention on the abovementioned transactions. (Regarding risk mitigation measures by the government, see the next chapter.)

⁶² Ministry of Economy, Trade and Industry, "Revised Action Plan for Strengthening Industrial and Technological Infrastructure Related to Economic Security," P.81.

(Reference 12) Current situations of cyberattacks and crypto assets

North Korea, which is subject to various sanctions, is presumed to be using cyberattacks as a means to obtain funds by evading international control measures.⁶³ According to a report published in October 2022 by the Panel of Experts, the panel recommended that U.N. member countries should implement the guidance concerning crypto assets prepared by the Financial Action Task Force (FATF) as promptly as possible in order to prevent the provision of funds for WMD proliferation.⁶⁴

Cyberattacks, by their nature, afford a high level of anonymity and confidentiality, so the sources of attack may remain unclear. Therefore, even in the case of attacks launched with the involvement of or support from governments, it is difficult to exercise deterrence compared with the case of traditional military threats because the attacking countries have easy deniability. In addition, as the techniques of attack are evolving and becoming more sophisticated day by day, regulators and attackers engage in a perpetual game of cat and mouse, so cyberattack risk constitutes a significant PF vulnerability.

Countermeasures against the cyberattack risk related to PF in particular are no different from the ones against cyberattacks in general. For example, in April 2022, the National Cyber Unit was established as a governmental investigative organization responsible for dealing with serious cyber incidents in light of the extremely serious threats existing in cyberspace, and in April 2024, it was upgraded and reorganized as the National Cyber Department.⁶⁵ The National Cyber Department is steadily conducting investigations in cooperation with prefectural police and foreign investigative agencies. In addition, the Police cooperates with companies possessing cutting-edge technologies to conduct comprehensive analysis of information provided by business operators and provide the results to the business operators. Efforts are also underway to enhance the level of security for IT users as a whole through cooperation between the public and private sectors. The government should continue to take these efforts and other actions to deal with cyberattacks.

In addition, crypto assets themselves afford a high level of anonymity to users and are capable of being transferred across borders instantaneously while being difficult to trace, and those characteristics provide an incentive for using crypto assets for the purpose of PF. Moreover, relevant technology continues to evolve day by day, as exemplified by the development of new types of crypto assets and new transaction methods. As a result, as in the case of cyberattacks, a game of cat and mouse tends to go on between the supervisory and regulatory authorities and criminals. In this respect, 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

⁶³ Ministry of Defense, Defense of Japan 2023, P. 176.

⁶⁴ Midterm report of the Panel of Experts submitted pursuant to resolution 2627 (2022)

⁶⁵ A press release by the National Police Agency, "Regarding the Status of Threats in Cyberspace in the First Half of 2024."

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 block chains 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.

On the other hand, through the amendment of the Payment Services Act in May 2019, Japan is developing an environment for crypto asset transactions, for example by making it obligatory to segregate the management of customers’ assets (management of assets using cold wallets that are not connected to the internet). According to the survey by a private organization, the amount of damage caused to centralized services operated by crypto asset exchange service providers, etc. in 2022 was less than 20% of the total hacking damage related to crypto assets, while Defi Protocols accounted for more than 80% of the total.⁶⁶ As shown above, although the government has taken some actions concerning crypto asset exchange service providers, it is necessary to continue paying attention to crypto asset transactions given the merit of those assets themselves for entities engaging in PF.

Meanwhile, the following challenges exist in relation to the examination of crypto asset transactions.

First of all, when financial institutions, etc. handle transactions on behalf of entities and individuals, they need to implement appropriate confirmation to make sure that the beneficiaries of remittance and other transactions are not persons who are subject to asset freezing or other measures for their involvement in the development, possession, and export of WMDs. However, persons who effectively receive the benefits of remittance and other transactions (“real remittance senders” and “real remittance recipients”) are not necessarily direct customers of financial institutions, etc. In some cases, real beneficiaries may be beneficial owners of customer companies, relatives of customers, or other associated persons. In other cases, in order to identify the real remittance sender, it may be necessary for financial institutions, etc. to grasp all details of transactions that constitute the cause of the remittance transaction in question (e.g., commercial transactions and transfer of liabilities).⁶⁷

Financial institutions, etc. implement confirmation regarding “real remittance senders” by sending inquiries to or requiring the submission of documents from customers. However, because of the information asymmetry between financial institutions, etc. and customers with respect to the cause of transactions, generally speaking, it is difficult to identify the real beneficiaries behind the complex

⁶⁶ Source: Chainalysis, The 2023 Crypto Crime Report.

⁶⁷ 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 real remittance senders, it is necessary to find out multiple debtors hidden behind the presence of the receiving agent service providers in some cases.

web of transactions.

In addition, while the process of screening by financial institutions, etc. of settlements related to import and export transactions is important, there are many challenges related to the practice of screening. For example, usually, import and export transactions involve the exchange of large volumes of various information between multiple parties, and the documents involved are kept in various forms and media depending on their type, so it is difficult to format them into data that can be cross-referenced with the list of the transactions subject to the economic sanctions by means of a transaction filtering system. Some financial institutions conduct the necessary screening work after manually scanning information from documents. In short, there is a challenge that should be overcome with respect to the approach to the screening of transaction data from the viewpoints of efficiency and accuracy.

Under these circumstances, it could be considered as the first step to focus on transactions with a high probability of being used for the purpose of PF and concentrate efforts on accurately identifying the real remittance senders and recipients in overseas remittance transactions. When doing that, it may be helpful to use, as reference cases, transactions with a relatively higher probability of being used for the purpose of PF that have been identified and published in other countries.

For example, as described in the previous chapter, high-risk transactions include overseas remittances related to the three northeastern provinces of the People's Republic of China, which have historically accepted many workers from North Korea; transactions with countries in sub-Saharan Africa, a region cited in the report of the Panel of Experts; and export transactions related to dual-use products.

From the viewpoint of risk mitigation, it is useful for financial institutions, etc. to focus on transactions with a relatively high probability of being used for the purpose of PF and to conduct intensive checks, not only regarding information on legal persons related to FATF Recommendation 24 and its Interpretative Note, including beneficial ownership information, but also regarding customer identification in cases where the transaction is suspected to be related to PF. "Frequently Asked Questions Concerning Guidelines for Foreign Exchange Transactions Service Providers on Compliance with the FEFTA and Its Regulations, etc.," published by the Ministry of Finance in November 2023, indicated the following situations as possible cases of violation, evasion, and circumvention of the economic sanctions. It is useful to conduct intensive checks from the viewpoint of whether the transaction under examination corresponds to any of those cases.

- The customer is reluctant to provide necessary information, or provide vague or inconsistent information.
- The customer is located in or connected with a country of proliferation or high risk.
- A customer or counterparty, declared to be a commercial business, conducts transactions that suggest

that they are acting as a money-remittance business or a pay-through account. These accounts involve a rapid movement of high-volume transactions and a small end-of-day balance without clear business reasons.

- Accounts or transactions involve possible companies with opaque ownership structures, front companies, or shell companies, e.g. companies do not have a high level of capitalization or displays other shell company indicators. There are long periods of account dormancy followed by a surge of activity.
- A trade entity is registered at an address that is likely to be a mass registration address, e.g. high-density residential buildings, post-box addresses, commercial buildings or industrial complexes, especially when there is no reference to a specific unit.
- A transaction request is made by the customer who has the same telephone number or IP address as the customer whose request for a transaction was previously declined.
- The customer's website is extremely simple, and the actual situation of the business described there is unclear.
- The transaction counterpart is different from the settlement counterpart without a rational reason. Payment for imported commodities is made by an entity other than the consignee of the commodities with no clear economic reasons, e.g. by a shell or front company not involved in the trade transaction.
- A customer engages in complex trade deals involving numerous third-party intermediaries in lines of business that do not accord with their stated business profile. Shipment of goods is made in a complicated or circuitous fashion without economic rational reasons.
- A customer withdraws funds in a manner inconsistent with the information on the purpose of the business relationship obtained by the financial institution for the inbound remittance or other transaction. Immediately before making a settlement, there is a deposit that is suspected to be made on behalf of a third party.
- A customer changes some of the information about the rejected remittance and attempts to make the remittance again. Customers make payments via routes other than the banks and remittance routes they normally use.

Finally, financial institutions, etc. should pay attention to the risk of being subjected to a secondary sanction imposed by the United States in relation to PF. A secondary sanction is in principle targeted at transactions that are conducted directly or indirectly between non-Americans and sanctioned persons and that have no connection with the United States. A secondary sanction is intended to effectively prevent such transactions by indicating the risk of being put at the same disadvantage as the sanctioned persons if they engage in the transactions. It is necessary to appropriately keep track of the specifics of the sanctions imposed by the United States.

The government should continue efforts to publish example cases of violation and issue alerts, as well as also routinely updating the method of raising public awareness and measures that may be taken while receiving feedback from private-sector companies.

Chapter 4 Japan's initiatives regarding PF

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

1. Initiatives regarding financial transactions

(1) Economic sanctions based on the FEFTA

The FEFTA is intended to contribute to the sound development of the Japanese economy by enforcing minimum necessary controls and coordination for international transactions. Regarding anti-TF and anti-PF measures, the act provides for the implementation of asset freezing and other measures against terrorists and persons involved in North Korea's PF activity. It also makes it obligatory for banks, etc. to conduct checks as to whether or not customers' remittances violate the FEFTA and implement identity verification of customers.⁶⁸

With respect to North Korea, Japan is implementing asset freezing measures under the FEFTA against designated individuals or entities as being subject to the sanctions under Ministry of Foreign Affairs notices based on the UNSCRs.⁶⁹ Specifically, Japan has designated individuals or entities subject to asset freezing measures and is implementing those measures by the ban on payments to and capital transactions (deposit contracts, trust contracts, and loan contracts) with those individuals or entities.

In addition, the Ministry of Finance publishes notices related to payments and capital transactions regulations were revised on June 1st, 2023, to clarify that the obligation of asset freezing under FEFTA extends to payments and capital transactions made in the name of a person other than the designated individuals or entities on behalf of the designated individuals or entities.⁷⁰

In December 2022, Japan designated Lazarus Group as subject to asset freezing for its involvement in North Korea's WMD and ballistic missile programs. Lazarus Group is the first cyber-related entity subject to the sanctions. Later, Japan designated North Korean cyber-related organizations, such as Andariel, Bluenoroff, and Kimsuky, as subject to asset freezing. In addition, in order to further

⁶⁸ The obligation to implement confirmations for transactions under the FEFTA (Article 17 of the Act) is applicable to banks and other prescribed financial institutions, funds transfer service providers, and electronic payment instruments service providers, etc. The obligation to verify the identities of customers under the Act (e.g., Article 18, paragraph (1) of the Act) is applicable not only to the abovementioned entities but also to trust companies, financial instruments business operator, and currency exchange operators.

⁶⁹ 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.

⁷⁰ Regardless of whether or not the activities of those legal persons and other entities are conducted on behalf of the sanctioned entities via agents, payments to them are subject to the restriction (Source: FAQs regarding the Payment and Capital Transaction Notifications Put into Effect on June 1, 2023 (May 26, 2023)).

strengthen restrictions to prevent transfers of funds to and from North Korea, Japan has prohibited payment, receipt of payment and capital transactions conducted for the purpose of contributing to activities that could facilitate North Korea's nuclear and missile programs. Japan has also totally prohibited the opening of new branches of Japanese banks in North Korea, establishment of correspondent relationships with North Korean banks and the opening of new branches of North Korean bank in Japan, etc. Japan has also imposed its own sanctions against North Korea, in addition to the sanctions based on the UNSCRs. Specifically, those sanctions include the ban on payment to North Korea and lowering the threshold for notification of the carrying out of currency and other instruments of payment to North Korea from 1 million yen to 100,000 yen, a measure intended to grasp the actual flows of funds in more detail.

Regarding Iran, the application period, for the measures related to large conventional weapons based on UNSCR 2231 expired on October 18, 2020 and on October 18, 2023, for the measures related to nuclear weapons delivery systems, but regardless of the provisions of the UNSCR, Japan has been strictly dealing with the transfer of goods and technologies related to nuclear weapons delivery systems based on the FEFTA.

(Reference 13) Purpose (Article 1 of FEFTA) and Key Points 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.

In order to ensure the effectiveness of asset freezing measures, the FEFTA makes it obligation for banks and other prescribed financial institutions and funds transfer service providers to implement confirmation as to whether or not exchange transactions related to customers' payments are equivalent to the transactions subject to asset freezing measures based on the FEFTA (hereinafter the "obligation to implement confirmations"). The act also imposes the above obligation to implement confirmations regarding asset freezing measures on electronic payment instruments service providers, etc.

In addition, based on the FEFTA, Japan conducts inspections of financial institutions, etc. providing foreign exchange service with respect to the status of compliance with laws and regulations related to asset freezing and other economic sanctions., etc. Moreover, on April 1, 2024, the Requirements for Financial Sanction Compliance on foreign exchange transactions service providers, which make it obligatory for banks, etc., funds transfer service providers, electronic payment instruments service providers, etc., and currency exchange operators, etc. to develop systems to implement asset freezing and other measures, were put into force. As a result, financial institutions and other entities to which the requirements are applicable are required to conduct risk management activities for the appropriate implementation of asset freezing and other measures, including appropriate risk evaluation regarding asset freezing and other measures as well as the development and enforcement of procedural manuals for risk mitigation.

(Reference 14) Number of entities on which foreign exchange inspection was conducted in recent years

Program year⁷¹ 2023:105; program year 2022: 110; program year 2021: 106;
program year 2020: 24; program year 2019: 78; program year 2018: 124

(2) Regulation on domestic transactions based on the Terrorist etc. Assets Freezing Act

International terrorist organizations and persons involved in WMD-related programs conduct activities across national borders. If a certain country fails to implement adequate countermeasures, it may be exploited as a “loophole” whereby anti-TF measures are evaded.

Based on that idea, regarding international anti-TF measures, Japan has regulated cross-border flows of funds between residents (those who hold an address in Japan) and non-residents under the FEFTA. On the other hand, Japan has not previously regulated domestic transactions between residents. However, in November 2014, the (former) Terrorist etc. Assets Freezing Act (put into force on October 5, 2015) was enacted in order to regulate domestic transactions as well.

Regarding anti-PF measures as well, while external transactions between residents and non-residents have been regulated under the FEFTA, domestic transactions between residents remained outside the scope of regulation until recently.⁷² In December 2022, the Act to Partially Amend the Act on Special Measures Concerning International Terrorist Assets Freezing etc. Conducted by the Government Taking into Consideration United Nations Security Council Resolution 1267, etc., to Deal with International Transfers of Unlawful Funds” (Act No. 97 of 2022) was enacted in order to regulate

⁷¹ The period of the program year is from July to June in the following year.

⁷² 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.

PF-related domestic flows of funds between residents as well.

2. Import and export controls

(1) Prohibition of imports and exports under the FEFTA, etc.

Regarding North Korea, in addition to prohibiting imports and exports of specified goods based on the UNSCRs, Japan is implementing measures of its own, as in the case of the financial measures. Those measures are as follows:

- (i) Prohibiting imports of all goods originating in or shipped from North Korea
- (ii) Prohibiting exports of all goods destined for North Korea
- (iii) Restrictions on imports and exports of payment instruments etc.

In addition, in order to prevent the evasion of the sanctions related to import and export controls prescribed under the FEFTA, the customs authorities are strictly conducting law enforcement based on the Customs Act (Act No. 61 of 1954).

Japan is also implementing the following measures from the viewpoint of preventing circumventing imports to or circumventing exports from Japan to North Korea via third countries.

- (i) Conducting strict checks as to the country/region of origin of goods when the import declaration raises concerns about possible imports from North Korea via neighboring countries
- (ii) Conducting strict checks as to the final destination of goods for export when the export declaration raises concerns about possible exports to North Korea via neighboring countries and checking contracts and other relevant documents as necessary.

In addition, the customs authorities are engaging in the close exchange of information and cooperation with relevant government agencies and enhancing information gathering from relevant business operators, such as customs brokers and shipping agents.

(2) Security export control under the FEFTA

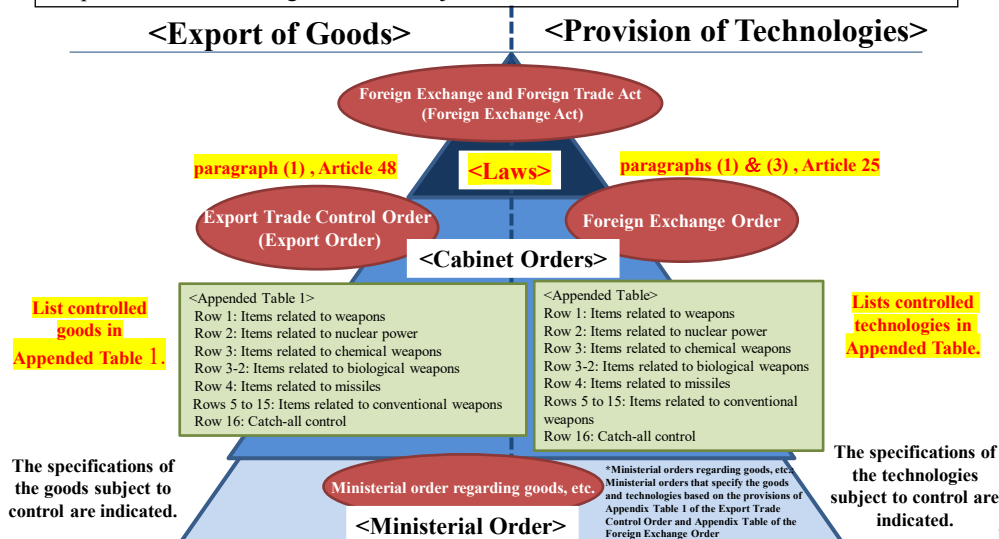
Regarding dual-use products and technologies, export controls are being promoted⁷³ under an international framework (international export control regimes) led by developed countries, and Japan is enforcing controls on exports of goods and the provision of technologies based on the FEFTA.

⁷³ 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, Republic of Korea, Luxemburg, Netherlands, New Zealand, Norway, Poland, Portugal, Spain, Sweden, Switzerland, the United Kingdom, and the United States.

(Reference 15) Overview of the security export control system

Overview of the security export control system

- Enforcing trade controls based on the Foreign Exchange Act in light of international export control regimes. Specifically, a license is required for the export of goods and the provision of technologies that are subject to control.



(Source) Ministry of Economy, Trade and Industry

Dual-use products and technologies at a particularly high risk of being used for WMD development are specified in Appended Table 1 (Rows 1 to 15) of the Export Trade Control Order in the case of products and in Appended Table of the Foreign Exchange Order (Rows 1 to 15) in the case of technologies as items subject to “list control.” When products and technologies equivalent to the specified ones are exported or provided, it is necessary to obtain a license. In cases where the products and technologies being exported or provided are not equivalent to the specified ones but where they may be used for WMD development, those transactions are subjected to “catch-all control” and require a license from the Minister of Economy, Trade and Industry.

Effective September 8, 2024, the Ordinance for Partial Amendment of the Ordinance that Prescribes Cargo Goods and Technologies Based on the Provisions of the Appended Table 1 of the Export Trade Control Order and the Appended Table of the Foreign Exchange Order was, among other regulations, put into force in order to revise the list of items subject to export control and the specifications of the existing listed items.

In the meantime, Japan is strengthening control measures regarding the provision of technologies. Previously, the Ministry of Economy, Trade and Industry enforced controls on the provision of technologies subject to the sanctions based on the FEFTA from residents to non-residents in Japan, which is deemed to be export (control of “deemed export”)—as well as the provision of those

technologies to persons and entities in foreign countries—because the non-residents are highly likely to ultimately depart from Japan. In May 2022, it was made clear that the provision of technologies to residents whose situation is equivalent to the situation of being under the strong influence of non-residents (specified types of cases)⁷⁴ is subject to the control of deemed export.

3. Other related regulations

(1) Act on Prevention of Transfer of Criminal Proceeds (verification at the time of transaction, notification obligation)

In light of FATF’s 2003 revision of the 40 Recommendations and changes in money laundering activity, the Act on Prevention of Transfer of Criminal Proceeds (Act No. 22 of 2007) was enacted with 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) and a part of the Act on Punishment of Organized Crimes and Control of Proceeds of Crime (Act No. 136 of 1999) as its base. This Act provides for a system for preventing the transfer of criminal proceeds, centering on measures including the verification of customers, etc. at the time of transaction, preparation and preservation of records, etc., and reporting of suspicious transactions by a certain scope of business operators (hereinafter referred to as “specified business operators”). Accordingly, also in regard to PF, measures against actions that may be related to crime are implemented under the framework of the Act on Prevention of Transfer of Criminal Proceeds.

(i) Verification at the time of transaction

As AML/CFT measures, basic matters concerning verification at the time of transaction and other measures are prescribed under related regulations, including the Act on Prevention of Transfer of Criminal Proceeds and the FEFTA. Specifically, the Act on Prevention of Transfer of Criminal Proceeds obligates business operators, such as financial institutions, that are positioned as “specified business operators” to implement identity verification, etc. (in the case of a legal person, this includes verification of beneficial owners) at the time of conducting specified transactions.⁷⁵

⁷⁴ Specifically, the specified types of cases apply to the following persons:

(i) Persons who are under the control of foreign governments and foreign legal persons based on employment and other contracts; (ii) persons who are under the control of foreign governments based on economic interests; (iii) persons who take acts in Japan under instructions from foreign governments.

⁷⁵ 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 16) Examples of specified business operators and specified transactions that require identity verification⁷⁶

Specified business operator	Specified transactions
Financial institution, etc.	Opening a deposit or savings account Large cash transaction exceeding 2 million yen Cash remittance exceeding 100,000 yen
Credit card company	Conclusion of a credit card contract
Finance lease company	Executing a contract for a finance lease transaction in which the amount of lease charges per occasion exceeds 100,000 yen * Excluding a contract under which a lease company leases goods it already possesses to its customer
Real estate broker	Conclusion of a real estate sales contract or the provision of intermediary or agency services therefor
Dealers in Precious Metals and Stones	Conclusion of a jewelry or precious metal sales contract for which payment exceeds 2 million yen in cash

(Reference) Website of the Public Relations Office, Government of Japan.

The Act on Prevention of Transfer of Criminal Proceeds obligates a specified business operator to promptly report to the administrative authority if it finds that assets received from a customer are suspected of being criminal proceeds or that a customer is suspected of engaging in ML through the transaction in question (the “suspicious transaction reporting system”). Information on suspicious transactions is collected at the National Public Safety Commission through administrative authorities or competent ministers. Then the information is organized and analyzed, and any information that is determined to contribute to the investigation, etc. of ML-related crime is provided to investigative organizations, etc.

(ii) Notification obligation (travel rule)

FATF Recommendation 16 and its Interpretative Note provide for a rule whereby financial institutions engaged in wire transfers are to provide notification of originator and beneficiary information (the so-called travel rule) in order to prevent people that have gained criminal proceeds and terrorists, etc. from moving their funds freely, and to make it possible to trace the assets subject to transaction when the assets are suspected of being criminal proceeds. According to FATF Recommendation 16 and its Interpretative Note, in wire transfers, Japan had conventionally obligated the ordering financial institution (a deposit-taking financial institution and a funds transfer service

⁷⁶ See the relevant webpage of the Public Relations Office, Government of Japan (<https://www.gov-online.go.jp/useful/article/201610/1.html>).

provider) to provide the originator and beneficiary information to the beneficiary financial institution. However, as a measure concerning transactions of crypto assets, FATF Recommendation 15 was revised in October 2018 and its Interpretative Note in June 2019, requiring countries to introduce and implement regulations that mandate crypto asset exchange service providers to obtain the originator and beneficiary information upon a crypto asset transfer, and to notify the beneficiary crypto asset exchange service provider of that information.

The travel rule relating to crypto asset transactions was introduced as a self-regulations by the Japan Virtual and Crypto Assets Exchange Association (JVCEA) in April 2022 at the request of the Financial Services Agency. Then in December 2022, the Act on Prevention of Transfer of Criminal Proceeds was amended to impose the travel rule on crypto asset exchange service providers, and the amendment came into effect in June 2023. Specifically, crypto asset exchange service providers, etc.⁷⁷ are obligated to provide notification of the originator and beneficiary information upon transfers of crypto assets, etc. and to record and retain the information provided or received through the notification.

Under the principle of reciprocity, 20 jurisdictions were initially designated⁷⁸ and eight additional jurisdictions were designated⁷⁹ in May 2024.

(Reference 17) Anti-cybercrime measures and regulations on crypto asset transactions

- When the police identifies a crypto asset transaction account that is used or is suspected of being used for unlawful money transfers related to internet banking, communications fraud, or ransomware infection cases, unlawful money transfers related to crypto assets, SNS-based investment or romance fraud, it promptly contacts the crypto asset exchange service provider related to the account and requests the service provider to consider freezing the account. In addition, the National Police Agency, the Financial Services Agency, and the National center of Incident readiness and Strategy for Cybersecurity has issued “Regarding cyberattacks by the Lazarus cyberattack group, a subordinate organization of North Korea authorities, that are targeted at business operators related to crypto assets (alert)” (dated October 14, 2022) because it is strongly presumed that Lazarus is launching cyberattacks targeting crypto asset exchange service providers, etc. in Japan.
- From the viewpoint of further strengthening the effectiveness of measures, such as asset freezing, against crypto assets and electronic payment instruments, Japan amended the FEFTA

⁷⁷ The obligation also applies to transfers of electronic payment instruments by electronic payment instruments service providers. However, the provisions on the obligation on electronic payment instruments service providers were promulgated in June 2022.

⁷⁸ 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.

⁷⁹ The United Arab Emirates, India, Indonesia, the United Kingdom, Estonia, Nigeria, Bahrain, and Portugal.

in April and December 2022 so as to additionally regulate transactions conducted by sanctioned persons and entities to transfer crypto assets and electronic payment instruments to third parties and to also obligate electronic payment instruments service providers, etc., as in the case of banks, to confirm asset freezing, etc.

(2) Schemes for increasing the transparency of legal persons

The reports of the Panel of Experts recommended that the regulation of the registration of companies with opaque activities should be tightened, in order to increase the transparency of legal persons.⁸⁰ In addition, requests have also been made in the FATF Recommendations and in demands from financial institutions, etc. that initiatives for increasing the transparency of legal persons be taken from the viewpoint of preventing the abuse of legal persons for ML/TF purposes. Based on such requests, Japan has so far developed institutional systems to verify information on beneficial ownership of legal persons as follows:

- Stipulated beneficial owners and obligated specified business operators to verify the identity information of the beneficial owner if its customer, etc. is a legal person.
- Obligated specified business operators that carry out services of providing a business address or accommodation, correspondence, or an administrative address for a legal person, etc. to conduct verification at the time of transaction upon the conclusion of a service contract and to prepare and preserve the verification record, transaction record, etc.
- Obligated that when certifying articles of incorporation upon the incorporation of a stock company, general incorporated association, or general incorporated foundation, a notary is to have the client report details, including the name of the person that will become the beneficial owner and whether that beneficial owner is a member of an organized crime group, an international terrorist, or a person involved in a program related to WMD.
- Stipulated a scheme whereby a commercial registry office, at the request of a stock company, keeps a document containing information about the beneficial owner of the stock company and delivers a copy of the document, in order to be able to continue identifying the beneficial owner after the incorporation of the company.

A recent specific development is that, as an initiative to continue identifying the beneficial owner after the incorporation of a legal person, the Ministry of Justice introduced the beneficial ownership of legal persons list system in which a commercial registry office keeps a document containing information about the beneficial owner prepared by a stock company (including a special limited liability company) and delivers a copy of the document, and started to operate the system in January 2022. The Strategic Policy also indicates that “the Government will promote the use of ‘the beneficial

⁸⁰ Final report of the Panel of Experts submitted pursuant to resolution 2515 (2020)

ownership of legal persons list system’ ... and consider developing a framework for finding the beneficial owners of legal persons centrally, continuously, and accurately,” and the government is promoting initiatives for increasing the transparency of legal persons in Japan. Moreover, while people incorporating a certain legal person, such as a stock company, in Japan are obligated to have the articles of incorporation certified by a notary, the Ministry of Justice introduced a new mechanism in June 2023 requiring a notary to examine that the person that will become the beneficial owner of the legal person is not a person involved in a program related to WMDs, in the procedure for certifying the articles of incorporation.

(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:

- Prohibition of the entry of North Korean citizens into Japan
- Prohibition of re-entry of North Korea authority officials and others residing in Japan with an aim to go to North Korea
- Request to all residents in Japan not to visit North Korea
- Suspension of Japanese government officials’ visits to North Korea
- Prohibition of the landing of North Korean flag vessels’ crew members and foreign crew members, and prohibition of the re-entry of foreign citizens residing in Japan, sentenced for the violation of Japan’s measures against North Korea, with an aim to go to North Korea
- Prohibition of re-entry of foreign experts of nuclear and missile technology residing in Japan with an aim to go to North Korea

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

Based on the Port entry prohibition Law (Act No. 125 of 2004), Japan implements a measure to prohibit all North Korean flag vessels (including those for humanitarian purposes), all vessels which have previously called at ports in North Korea (including Japan-flagged vessels), and vessels designated on UNSCRs, etc. from entering into Japanese ports. Moreover, Japan prohibits chartered flights to and from North Korea, and denies permission to any aircraft to take off from, land on, or overfly the territory of Japan if the aircraft is believed to contain items prohibited by UNSCRs.

With regarding to cargo, Japan implements a measure to inspect specified cargo related to North Korea based on the Act on Cargo Inspection (the Act on Special Measures Concerning Cargo Inspections Conducted by the Government Taking into Consideration UNSCR 1874 (Act No. 43 of 2010)) and other regulations (a measure to ensure the inspection under the relevant UNSCRs).

The Ministry of Foreign Affairs, together with G7 and other like-minded partners, has been working on the People’s Republic of China regarding the issue that oil tankers that appear to be transporting

oil to North Korea are active in the territorial waters of the People's Republic of China.⁸¹ In addition, at the Japan-China High-Level Consultation on Maritime Affairs held in October 2023, the ministry strongly requested the People's Republic of China once again to take action against the illegal operations by fishing vessels of the People's Republic of China in the waters around the Yamato Bank in the Sea of Japan and raised the importance of fully implementing UNSCRs related to sanctions regarding North Korea, including action against illicit maritime activities including ship-to-ship transfers prohibited by the UNSCRs.

(5) Other AML/CFT related regulations

Other regulations related to AML/CFT measures include the following Acts. While these are ML/TF-related legislations, their risk mitigation measures are expected to serve as a reference in 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 confiscation.
- 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 specifies certain instances of drug-related crime as predicate offences of the crime of concealment of proceeds of drug-related crime, etc., and provides for the confiscation of 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 Punishment of Terrorist Financing): This Act provides for punishment of the collection, provision, etc. of terrorist funds.

From the viewpoint of appropriately responding to the recommendations, etc. made in the FATF Fourth Round Mutual Evaluation of Japan, the Act to Partially Amend the Act on Special Measures Concerning International Terrorist Assets-Freezing, etc. Conducted by the Government Taking into Consideration United Nations Security Council Resolution 1267, etc., to Deal with International Transfers of Unlawful Funds” (Act No. 97 of 2022) (Act to Respond to FATF Recommendations) was enacted in December 2022 in order to collectively amend Acts including the FEFTA and the Act on

⁸¹ Reports by the Panel of Experts have indicated that multiple oil tankers often evacuate to the waters in Sansha Bay between illegal navigations.

Prevention of Transfer of Criminal Proceeds.

4. Major initiatives relating to close coordination among ministries and the private sector

(1) Major initiatives relating to close coordination among ministries

CPF measures span, and are interrelated with, fields such as finance and trade, which cover multiple ministerial jurisdictions. Therefore, it is extremely important for ministries and agencies to cooperate in implementing CPF measures. Specific examples of coordination are described below.

- In response to the publication of the FATF Fourth Round Mutual Evaluation Report of Japan, the Inter-Ministerial Council for AML, CFT, and CPF Policy, co-chaired by the National Police Agency and the Ministry of Finance, was established in August 2021 in order to strongly promote measures on a government-wide basis. The Council formulated the Action Plan for the next three years and has followed up on the progress of the efforts. The Council has also issued the Strategic Policy.
- In order to implement measures, such as asset freezing, based on the FEFTA without delay, the Ministry of Finance, the Ministry of Economy, Trade and Industry, and the Ministry of Foreign Affairs prepared an agreement among the relevant ministries and agencies, providing that if any designed individuals or entities to be subject to sanctions are additionally designated by a UNSCR, necessary measures will be implemented within 24 hours from the time of designation (including advance notification provided to financial institutions, etc.), and started its operation on May 31, 2021 (*No individuals or entities have been additionally designated based on UNSCRs 1718 and 2231 since the start of the operation).
- The Ministry of Finance and the Financial Services Agency conduct “joint inspections” where they jointly conduct the Ministry of Finance’s foreign exchange inspections and the Financial Services Agency’s AML inspections, from the perspective of sharing the inspection officials’ knowledge and inspection information between the respective supervisory authorities and effectively and efficiently ensuring financial institutions’ compliance with the related laws and regulations, based on the points mentioned in the FATF Fourth Round Mutual Evaluation Report of Japan.
- The Ministry of Foreign Affairs share information necessary for implementing the measures, such as asset freezing, prescribed in the UNSCRs regarding North Korea with the relevant ministries and agencies that are taking measures based on the FEFTA and the Terrorist etc. Assets Freezing Act. In addition, the Ministry of Foreign Affairs takes actions, including holding talks with countries such as the United States and the ROK, issuing statements with G7 and other like-minded countries, and holding UNSC emergency meetings, according to the intensity of North Korea’s provocative actions.
- As part of monitoring and surveillance activities, Japan Self-Defense Forces use JMSDF vessels

and other assets to collect information on ships suspected of violating the UNSCRs. The Joint Staff Office shares the collected and analyzed information with relevant ministries and agencies in a timely and appropriate manner. In addition, when JMSDF ships or other assets detect activities that are suspected of illicit maritime activities including ship-to-ship transfers prohibited by the UNSCRs, the Ministry of Defense provides the information to relevant ministries and agencies.

(2) Major initiatives relating to close coordination with and dissemination of information to the private sector

As mentioned so far, banks, etc., funds transfer service providers, electronic payment instruments service providers, and currency exchange operators are required to conduct self-risk assessment and to take actions in consideration of the risks. It is also expected that other private-sector business operators, including DNFBPs, will take actions in consideration of the risks, and there is a need for other private-sector business operators to reduce the risk that they are unintentionally involved in PF. To this end, it is important for the government to closely coordinate with and disseminate information to the private sector.

- In order to regularly and on an ongoing basis understand financial institutions' foreign exchange operation status and internal control framework, etc., and to utilize that information in the inspection plan (selection of the financial institutions to be inspected), the Ministry of Finance introduced off-site monitoring system in December 2018, and has collected reports based on Article 55-8 of the Foreign Exchange and Foreign Trade Act and Article 15 of the Act on Prevention of Transfer of Criminal Proceeds once every year.
- The Ministry of Finance formulated and publicly announced the Guidelines for Foreign Exchange Transactions Service Providers on Compliance with the FEFTA and Its Regulations, etc. set out and clarify a point of view and interpretations regarding compliance with the Foreign Exchange and Foreign Trade Act as a guidance, and it requires foreign exchange service providers to develop an internal control framework for complying with Foreign Exchange and Foreign Trade Act, etc. based on the guidelines.
- In preparation for the introduction of the Requirements for Financial Sanction Compliance on foreign exchange transactions upon the entry into force of the amended FEFTA (April 1, 2024), the Ministry of Finance has revised the abovementioned guidelines and conducted outreach toward financial institutions and currency exchange operators on identifying and assessing the risk of sanctions violations, implementing risk mitigation measures and establishing internal control.
- Ministries and agencies with jurisdiction over financial institutions, etc. publish reference case examples of transactions to which financial institutions, etc. should pay special attention when

fulfilling the reporting obligation due to the likelihood of transactions being suspicious. Moreover, the ministries and agencies repeatedly request financial institutions, etc. to take actions, including the following: update the sanction list without delay when sanctioned persons and entities are designated and published; conduct enhanced customer due diligence based on the Act on Prevention of Transfer of Criminal Proceeds and guidelines; thoroughly fulfill the obligation to report suspicious transactions; appropriately implement measures based on the FEFTA; and comply with the provisions of the Terrorist etc. Assets Freezing Act on International Terrorist Assets-Freezing, by taking advantage of various opportunities such as when the FATF issues statements.

- The National Police Agency and the Financial Services Agency jointly hold a workshop on the suspicious transaction reporting system every year for people in charge at financial institutions, etc. to help them deepen their understanding of the system.
- Customs authorities endeavors to keep customs brokers, etc. well-informed about the prohibition of imports from and exports to North Korea and requests their cooperation in ensuring the effectiveness of the measure.
- While inbound and outbound passenger's personal effects, etc. are excluded from the restriction of imports and exports, customs authorities conducts strict enforcement by exchanging information closely with relevant government agencies, shipping companies, and airline companies, etc. in order to deal with cases where a passenger illegally imports or exports goods disguised as their belongings, etc. or cases where a ship or aircraft crew member attempts to export luxury goods to North Korea by hiding them in goods that are considered to be used for the member's private purposes.
- Ministries and agencies with jurisdiction over DNFBPs publish reference cases of suspicious transactions that specified business operators should pay extra attention to and for which they must comply with the suspicious transactions reporting obligation. They also provided information concerning organizations and individuals subject to asset freezing to the industries under their jurisdiction. In addition, on receiving a notice from the Ministry of Justice, the Japan Federation of Bar Associations notifies its members of information on persons and entities subject to asset freezing, etc.

5. Promotion of international cooperation

- In 2023, the Ministry of Foreign Affairs, as the G7 Presidency, hosted the meetings of the G7 Global Partnership Against the Spread of Weapons and Materials of Mass Destruction Working Group. At this meeting, proposals on capacity-building assistance aimed at preventing fund-raising and illegal transactions that lead to WMD proliferation were introduced, and matchmaking with countries providing financial support was conducted.

- Under the Japanese G7 Presidency, the FATF Virtual Asset Contact Group meeting co-chaired by the Financial Services Agency was held in Tokyo in April 2023.⁸² 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. Following its adoption of a roadmap in February 2023, FATF designated the jurisdictions where FATF member countries and important crypto asset exchange service providers in those countries are conducting activity and published a list of the status of implementation of the FATF Standards (Public Table) in March 2024 from the viewpoint of promoting the implementation of the FATF Standards (Recommendation 15: New technologies).⁸³ In July, FATF summarized measures to promote the global implementation of the FATF Standards, including the travel rule, North Korean illegal activities related to crypto assets, new risks associated with DeFi, unhosted wallets, and P2P transactions, and published the fifth round annual monitoring report. In the report, FATF pointed out that crypto assets continued to be used not only for the purpose of assisting WMD proliferation but also for other purposes by fraudsters, terrorist groups and people engaging in other illegal activities. North Korea continues to exploit victims (consumers and citizens) by stealing crypto assets that they own or by using intimidation and is using increasingly sophisticated techniques to launder profits illegally earned through those means. Crypto assets are starting to be used more and more frequently by terrorist groups, particularly ISIL in Asia and groups in Syria. It is also said that terrorist groups frequently attempt to conceal illegally earned profits by using stable coins and crypto currencies that provide a high level of anonymity. The Financial Services Agency, as co-chair of the Virtual Assets Contact Group (VACG), was involved in preparing the Public Table and the fifth round annual report.⁸⁴ FATF/VACG plan to continue outreach activity and the provision of support for global compliance with Recommendation 15 and to update the Public Table in 2025.
- Apart from activities conducted by the G20 and the FSB to make improvements regarding cross-border remittances, FATF is now working to revise Recommendation 16 (Wire Transfers) from the viewpoint of enhancing AML/CFT. The revision is intended to plug loopholes in relevant regulations and prevent abuse of cross-border remittance systems by criminals and terrorists while securing the fairness of competitive conditions embodied by “same activity, same risk, same rules,” which constitute the principles of the FATF Standards, amid the increasing diversification of payment methods and payment service providers. Between February and May

⁸² <https://www.fsa.go.jp/inter/etc/20230414/20230414.html>

⁸³ <https://www.fatf-gafi.org/en/publications/Virtualassets/VACG-Snapshot-Jurisdictions.html>

⁸⁴ <https://www.fatf-gafi.org/en/publications/Virtualassets/VACG-Snapshot-Jurisdictions.html>

2024, FATF held public consultation concerning Recommendation 16 and intends to finalize the revision of Recommendation 16 while engaging in dialogue with private-sector business operators and also while ensuring consistency with other policy objectives, including AML/CFT and the cost and speed of cross-border remittances, and preventing unintended negative effects on private-sector financial institutions. Japan, as co-chair of the Policy Development Group (PDG), which is responsible for revising the FATF Standards, is involved in summarizing discussions at FATF and dialogue with global stakeholders.

(Reference 18) UNSCRs against North Korea and their outlines⁸⁵

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 intercontinental ballistic missiles (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. Human ○ Prohibition of an individual designated by the UNSC or Sanctions Committee and their family members from entering Japan and passing Japan's territory ○ Obligation to send back to North Korea any North Korean citizen 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 individuals 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 entities or individuals 4. Maritime/air transportation ○ Inspection of North Korea-related cargo in the territory of own country, 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 individuals or entities, and vessels for which there are reasonable grounds to believe that they transport prohibited items from North Korea from entering ports of Member States ○ Prohibition of facilitating or being involved in transshipment to or from North Korean-flagged vessels ("illegal ship-to-ship transfers of goods")

⁸⁵ https://www.mofa.go.jp/mofaj/gaiko/unsc/page3_003268.html

Chapter 5 Conclusion

As indicated in the National Risk Assessment, Japan is routinely exposed to many PF-related threats. There are not only entities and individuals subjected to the sanctions based on the UNSCRs but also entities that launch cyberattacks, entities that cause goods and technologies, including dual-use products, to be leaked from Japan, and entities that engage in PF and WMD development by using all available means, including legal persons whose actual circumstances, such as activities and capital relationships, are opaque. All of those entities could pose a threat to Japan.

Indeed, entities that pose a threat have violated and evaded PF-related financial sanctions over and over again. In particular, as cyberattacks evolve day by day and are difficult to trace, the number of arrests in cybercrime cases is rising year after year and the value of damage caused by cybercrimes is considerable. There have also been many cases of import and export of dual-use products because of the increasing complexity and diversification of distribution structures. Indeed, many sensitive technologies and goods that could be converted to military uses have been leaked from Japan to other countries. In addition, recommendations have been issued with respect to cases of illicit exports using legal persons whose actual circumstances, such as activities and capital relationships, are opaque, in particular in the reports of the Panel of Experts. Among other factors that make Japan especially vulnerable to PF are the presence of an advanced financial sector, which makes various means of PF activity available, and its geographic proximity to North Korea. Japan is taking various measures to deal with its current situation related to PF. In response to cyberattacks, Japan has taken a series of actions as follows. In December 2022, Japan designated Lazarus Group as subject to asset freezing, making it the first cyberattack group to be designated as such. Later, Japan designated North Korean cyber-related entities, such as Andariel, Bluenoroff, and Kimsuky, as subject to asset freezing. On March 26, 2024, it issued an alert concerning North Korean IT workers. In addition, in order to further ensure the effectiveness of the sanctions against North Korea and other countries based on the FEFTA, starting on April 1, Japan made it obligatory for crypto asset exchange service providers, and bank and other entities that handle foreign currency transactions to become prepared to implement asset freezing and other measures.

Regarding dual-use products, Japan enforces export controls based on the FEFTA in light of the international export regimes. With respect to increasing the transparency of legal persons, Japan introduced a beneficiary owner list system in January 2022. Moreover, regarding the procedures for certifying articles of incorporation, in June 2023, Japan introduced a new system under which notaries public conduct examination as to whether or not persons who should be beneficial owners of legal persons are equivalent to persons involved in WMD development.

However, at a time when the nature of threats posed to Japan changes day by day, it goes without saying that the country's efforts to deal with PF will always remain "unfinished." It is important to

conduct a more in-depth analysis for the purpose of the National Risk Assessment, and it is also essential to further strengthen coordination among relevant ministries and agencies through the Policy Council and promote sharing and exchange of information and knowledge as necessary. Moreover, it is important for the administrative authorities to appropriately inform the public about those efforts and the reform of systems so as to deepen the private sector's understanding of the efforts and the current systems. Public-private cooperation is also important for promoting the sharing of information on how to deal with PF.