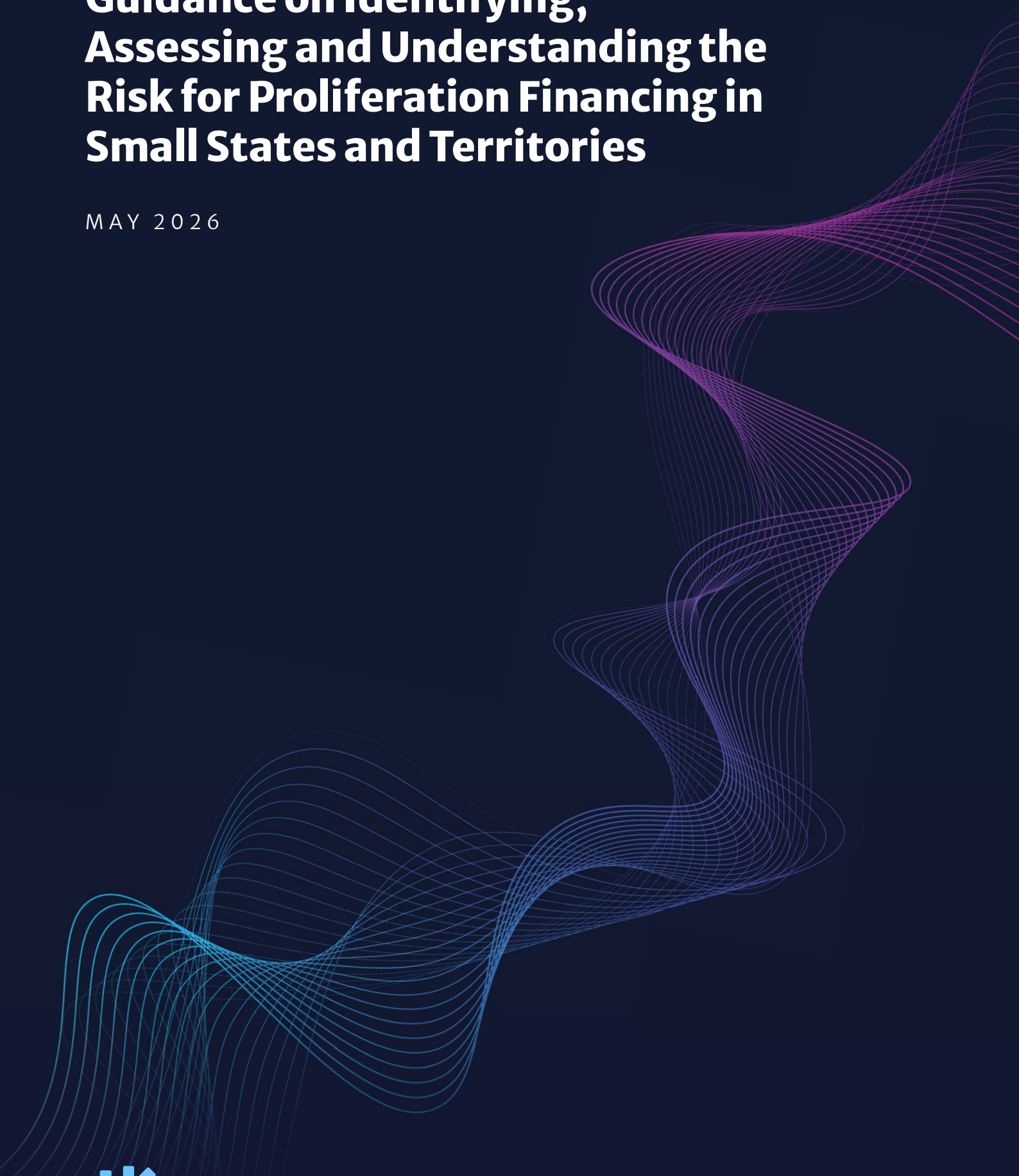
Guidance on Identifying, Assessing and Understanding the Risk for Proliferation Financing in Small States and Territories

MAY 2026



SMALL STATES &TERRITORIES WORKING GROUP

Contents

Executive summary 03

Introduction 05

Aim and scope 06

Background 08

Methodological Framework 14

Threats, Vulnerabilities and Consequences 15

Understanding PF Risks in Small States and Territories 18

Sectoral Vulnerabilities 22

Typology of Reflagging Deception Practice – DPRK 26

Cyber Enabled Proliferation Financing 27

Typologies and Red Flags 29

Mitigating PF Risks in Small States and Territories 33

Conclusion 41

References 44

Annex A – A Full List of Survey Questions 46

Annex B – Resources for Understanding and Managing PF Risks 51

Annex C – Case Studies 52

Glossary and Abbreviations 55

Executive Summary

The financing of proliferation (PF) refers to the risk of raising, moving, or making available funds, other assets or other economic resources, or financing, in whole or in part, to persons or entities for purposes of weapons of mass destruction (WMD) proliferation, including the proliferation of their means of delivery or related materials (including both dual-use technologies and dual-use goods for non-legitimate purposes.[1] While PF is often associated with larger economies, small states and territories face distinct vulnerabilities due to their economic structures, open financial systems, and limited institutional capacity. These jurisdictions may serve as transit points for funds, hosts of international finance centres (IFCs), providers of financial and/or professional services connected with export and trade, or may constitute trade and transhipment hubs, all of which can be exploited by proliferators. Recognising and addressing these risks through proportionate, risk-based, and data-driven approaches is essential to safeguarding national and international security. When assessing the effectiveness of such controls, it is also important to note that a lack of data or identified cases relating to PF does not necessarily indicate weak implementation. Conversely, it should not be interpreted alone as evidence of a low PF risk profile.

This guidance provides small states and territories with a structured framework to identify, assess, and mitigate PF risks, in alignment with Financial Action Task Force (FATF) Recommendations 1, 7 and 15. It draws upon data, technical analysis, and the experiences of members of the Small States and Territories Working Group (STWG); including Andorra, Gibraltar, Guernsey, the Holy See/ Vatican City, Isle of Man, Jersey, Liechtenstein, Malta, Monaco, and San Marino, to offer practical insights and proportionate solutions tailored to smaller jurisdictions.

Key PF risks for small states and territories stem from their potential role in facilitating financial flows, managing foreign assets, or enabling the trade and shipment of dual-use goods; items with both civilian and military applications. Within this context, the Trust and Company Service Provider (TCSP), Virtual Asset Service Provider (VASP) and shipping sectors are particularly relevant, as a number of small states have material TCSP, VASP and/or shipping industries that warrant attention and consideration in the context of PF risks. The STWG has therefore identified these risks as a commonality across small states and territories with >

"Key PF risks for small states and territories stem from their potential role in facilitating financial flows, managing foreign assets, or enabling the trade and shipment of dual-use goods; items with both civilian and military applications."

1 https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Guidance-Proliferation-Financing-Risk-Assessment-Mitigation.pdf.coredownload.inline.pdf

"The experience of the STWG demonstrates the power of shared knowledge, showing how collaboration among jurisdictions with similar vulnerabilities can build capacity, close gaps, and contribute to countering proliferation financing"

regional and international finance centres, which are further compounded by cyber-enabled threats, such as ransomware attacks and the hacking of cryptocurrency exchanges by state-sponsored groups, particularly from the Democratic People's Republic of Korea (DPRK). Even where a jurisdiction does not have a material VASP sector, there may still be significant virtual asset (VA) usage and adoption within the wider economy, which can nonetheless present PF-related risks. PF threat actors exploit "blind spots" in global financial systems, highlighting the need for awareness and strong understanding of PF typologies across the global community.

Amid shifting geopolitical dynamics, such as the deepening alignment between Russia, Iran, and the DPRK, the recent snapback of UN sanctions on Iran under the Joint Comprehensive Plan of Action (JCPOA) framework, and the end of the UN Panel of Experts on DPRK, global non-proliferation norms face renewed pressure. These developments highlight the growing intersection between financial intelligence, sanctions evasion, and proliferation activity, demanding stronger coordination between law enforcement, regulators, export control authorities and the private sector. In implementing PF-related controls, jurisdictions should also be mindful of humanitarian aid exemptions under relevant UN Security Council resolutions (for example, Resolution 2264).

The guidance aims to help jurisdictions:

- Understand their unique PF vulnerabilities, particularly those linked to financial services, shipping, and trade.
- Develop tailored mitigation strategies through effective export controls, screening of dual-use goods, and inter-agency coordination.
- Enhance capacity building and public-private collaboration, ensuring that both sectors understand their respective roles in PF prevention.
- Strengthen resilience against cyber-enabled PF, by improving technological safeguards and information-sharing mechanisms.

Effectively countering PF requires adherence to international standards. It relies on continuous learning, proactive collaboration, and strategic foresight. Small states and territories can strengthen their resilience to proliferation financing risks by developing specialised expertise, embedding risk-based decision-making across all institutions, and enhancing international cooperation. The experience of the STWG demonstrates the power of shared knowledge, showing how collaboration among jurisdictions with similar vulnerabilities can build capacity, close gaps, and contribute to countering proliferation financing.

Introduction

Proliferation Financing (PF) presents a substantial threat to global security and stability and is a complex and evolving challenge for jurisdictions worldwide. Due to the particular economic and financial structures and size of small states and territories, these unique circumstances provide an opportunity to build tailored expertise and strengthen national resilience against a threat that remains little-known. Identifying gaps and developing expertise is therefore essential for establishing proportionate and effective risk mitigation measures.

Small states and territories, like any jurisdiction, can only develop effective strategies to combat PF if they thoroughly understand the specific risks they face. Proliferation and PF are multi-factorial and PF actors exploit the vulnerabilities inherent in a particular jurisdiction or system. For this reason, the vulnerabilities faced by small states and territories will be different to those faced by larger countries and economies. For many, these risks primarily arise from being used as transit points for funds or other assets tied to proliferation activities occurring outside their borders, from managing foreign assets or businesses linked to these activities or from providing credit or others forms of (trade) financing to entities involved in proliferation or PF. It is also important to note that jurisdictions may undertake other economic activities such as shipping, manufacturing and engineering that may themselves present risks related to proliferation and PF. In addition, a number of small states have material Trust and Company Service Provider (TCSP) and/or Virtual Asset Service Provider (VASP) sectors, which are important to consider when assessing PF risk due to their potential exposure to misuse. Even where a jurisdiction does not have a material VASP sector, significant virtual asset (VA) usage or adoption within the wider economy may still create avenues for misuse by proliferators. PF threat actors thrive on 'exploiting potential blind spots in the international financial system': even if jurisdictions believe they have low levels of vulnerability to PF, vigilance and self-scrutiny is paramount.[2] This is particularly important, as PF threat actors can include state actors or state sponsored groups with significant resources and expertise.

Assessing these risks can be particularly challenging, as it often requires tracking and understanding activities beyond the jurisdiction's direct oversight, while small states and territories may lack own intelligence services beyond FIUs. For small states and territories with international finance centres (IFCs), a strong understanding of PF threats in the context of their individual circumstances and structures is essential to mitigate risks effectively. Proliferators often exploit complex networks of front companies, financial services, and transit points to mask the nature of their activities, particularly in jurisdictions with maritime hubs or financial access points that may serve as strategic nodes in proliferation networks. Increasingly, cyber-enabled PF risks also threaten these jurisdictions, as threat actors employ tactics such as ransomware attacks and hacking of cryptocurrency exchanges to acquire or launder illicit funds for use in weapons of mass destruction (WMD) programmes.

Consequently, small states and territories may unintentionally become part of these funding networks, occasionally through direct procurement of dual-use goods, but more often indirectly, through financial services that obscure the identities and transactions of proliferators >

"the vulnerabilities faced by small states and territories will be different to those faced by larger countries and economies."

2 FATF Report, *Complex Proliferation Financing and Sanctions Evasion Schemes (2025)*, p. 12.

or otherwise financially enable proliferation or PF activities. This indirect and cyber-enabled exposure creates significant risk, making it crucial for such jurisdictions to regularly assess their vulnerability. As proliferators adapt their tactics to evade sanctions, jurisdictions worldwide must remain aware, broadening their understanding of PF typologies and recognising how their unique economic, institutional, and cyber structures might be abused to enable PF.

While small states and territories may face inherent constraints in resources, institutional capacity, and access to specialised expertise, these limitations are often offset by their nimble structures and strong inter-agency coordination. The nature of their institutional frameworks enables more direct communication, rapid decision-making, and cohesive policy implementation. This nimbleness allows small states and territories to adapt quickly to emerging risks and to demonstrate effectiveness in identifying, assessing, and responding to proliferation financing threats, often in ways that larger jurisdictions may find more challenging to replicate.

Identification of specific target jurisdictions falls outside the scope of this guidance. The analysis underpinning this guidance draws upon internationally recognised sources, typologies, and open-source information. The deliberate omission of state names referenced in the document, including those cited in reports of the United Nations Panel of Experts and other research sources, is intended to maintain analytical neutrality. Each jurisdiction applying this guidance is expected to independently determine its own list of target jurisdictions based on national context, risk assessment, and intelligence holdings.

This methodological choice does not diminish the objectives of the paper. Rather, the referenced case studies in Annex C are employed solely to illustrate typological examples that may assist competent authorities in identifying red flags, enhancing situational awareness, and developing a deeper understanding of proliferation financing risks and associated threat exposures.

Aim and Scope

This guidance aims to provide small states and territories with a structured approach that they can use in identifying, assessing, understanding and mitigating their specific PF risks at a national level, drawing from the experiences of various countries. Aligned with Financial Action Task Force (FATF) standards, it is designed to support both public and private sector entities in managing PF risks, including risks associated with dual-use goods, sensitive materials, and exporting/shipping.

This guidance:

a) Assists small states and territories in meeting FATF Recommendation 1 objectives to identify, assess, and understand PF risks, with a particular focus on vulnerabilities that may arise from serving as transit jurisdictions for PF-related funds or assets or engaging in foreign asset management or financing linked to proliferation activities;

b) Supports small states and territories in implementing measures to mitigate PF risks, especially regarding the export and transit of dual-use goods and sensitive materials, which may have legitimate uses but could also be exploited in the >

"This guidance aims to provide small states and territories with a structured approach, consistent with FATF Recommendations 1 and 7, to identify, assess, understand and mitigate PF risks, both in relation to targeted financial sanctions and the broader PF threats recognised by FATF for effectiveness purposes."

development or delivery of WMDs. Export controls are crucial for managing these risks, and this guidance highlights ways to strengthen them in line with international standards;

c) Provides actionable insights on evolving PF threats, including cyber-enabled attacks, such as ransomware targeting cryptocurrency exchanges, that exploit regulatory gaps or technological vulnerabilities. It also highlights the growing risks associated with AI, including identity spoofing and autonomous agentic networks that may facilitate sanctions evasion or obscure the origin and movement of funds; and

d) Emphasises the role of the private sector, including financial institutions and DNFBPs, in assessing and managing PF risks at the institutional level.

In line with FATF Recommendation 7, this guidance focuses on targeted financial sanctions (TFS) linked to the Democratic People's Republic of Korea (DPRK) and the Islamic Republic of Iran (Iran). TFS oblige jurisdictions to freeze assets associated with UN-designated persons and entities, their associates, and those under their control.[3] These measures also extend to enhanced export controls to prevent dual-use goods and sensitive technologies from being diverted to WMD development. This guidance aims to provide small states and territories with a structured approach, consistent with FATF Recommendations 1 and 7, to identify, assess, understand and mitigate PF risks, both in relation to targeted financial sanctions and the broader PF threats recognised by FATF for effectiveness purposes.

Developed from collective discussions, data analysis, and academic and technical papers, the guidance consolidates insights on PF typologies, threat indicators, and mitigation strategies, offering a practical tool to aid small states and territories in their PF risk assessments and strengthen the global response to proliferation financing, while balancing the practical limitations they may face. >

"the risk of raising, moving, or making available funds, other assets or other economic resources, or financing, in whole or in part, to persons or entities for purposes of WMD proliferation."

3 FATF, *Methodology: For Assessing Technical Compliance with the FATF Recommendations and the Effectiveness of AML/CFT/CPF Systems (2024)*, p. 46..

Background

Defining proliferation financing

A lack of an internationally agreed-upon definition of PF, or details on the type of domestic legislation that countries are expected to implement, creates immediate variance in how individual states interpret the provisions under the United Nations Security Council Resolution (UNSCR) 1540. To cover this gap, the Financial Action Task Force (FATF), drafted their own working definition to assist countries in better interpreting the provisions of Resolution 1540.

For the purpose of this guidance document, the definition of the financing of proliferation refers to: 'the raising, moving, or making available funds, other assets or other economic resources, or financing, in whole or in part, to persons or entities for purposes of WMD proliferation, including the proliferation of their means of delivery or related materials including both dual-use technologies and dual-use goods for non-legitimate purposes.' [4]

WMD proliferation is the 'manufacture, acquisition, possession, development, export, transhipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials (including both technologies and dual-use goods used for non-legitimate purposes), in contravention of national laws or, where applicable, international obligations. It includes technology, goods, software, services or expertise'.[5] There are **three stages** involved in PF, namely:[6]

1) *Raising of funds:* **funds collected through licit and illicit means, either under the direction of a proliferating state or by non-state actors acting independently or on behalf of such states.**

2) *Obscuring of funds and money flows:* **involves laundering of funds into the international financial system, disguising their true origin and destination through typical methods: middlemen, shell companies, complex corporate structuring, and false invoicing.**

3) *Procurement and transport of goods and technology:* **these funds are finally used to obtain materials, technology, parts or expertise needed for the development or acquisition of WMDs. These may include 'dual-use goods'.**

While these three stages are internationally recognised and widely applied, the STWG has identified an additional component of PF particularly relevant to small states, relating to the storage or holding of funds and assets. This reflects circumstances where proliferation-linked assets may be retained or administered through legal entities or arrangements, including those managed by TCSPs. In such contexts, the abuse of corporate or fiduciary structures to conceal beneficial ownership or control can represent a distinct PF vulnerability, especially for jurisdictions with significant TCSP activity.

Each stage of this process represents a chance for prevention, mitigation, and interception. While such linear descriptions of PF are helpful to conceptualise and understand often-used tactics, competent authorities and relevant stakeholders should maintain a broad perspective on strategies employed by proliferators, who will not >

> *"The members include Andorra, Gibraltar, Guernsey, Holy See/Vatican, the Isle of Man, Jersey, Liechtenstein, Malta, Monaco and San Marino."*

4 FATF, *Guidance on Proliferation Financing Risk Assessment and Mitigation* (2021), p. 8.
5 FATF, *Combating Proliferation Financing: A Status Report on Policy Development and Consultation* (2010), p. 5.
6 Brewer, Jonathan, *The Financing of Nuclear and Other Weapons of Mass Destruction Proliferation* (CNAS, 2018), p.5.

confine themselves to neat or clearly distinguishable processes to achieve their aims.

Defining small states and territories

As with PF, what defines a 'small state/territory' is not easily determined. Whether using the size of a jurisdiction's territory, population, or economy there is some degree of arbitrariness involved in ascertaining boundaries. For instance, the World Bank Small States Forum sets the bar to entry at populations of 1.5 million, whereas the UN Forum of Small States allows those with up to 10 million to participate.[7] Whilst the cut-off threshold remains a matter of debate, these limited material factors still remain important because they affect the domestic functioning of the public administration, economy, and capacity of the state. Small states are therefore generally characterised by centralised and generalist public administrations, open economies with a high demand on imports and exports, personalised and localised political dynamics, and disproportionate vulnerability (exposure to exogenous shocks).

At the same time, in the realm of foreign policy, relational approaches become essential. Here, 'smallness' is relative – existing on a continuum rather than as a fixed category: Canada has the fourth largest landmass on Earth but has only two-thirds of the population of the UK, which ranks eightieth in landmass. If Switzerland is small according to the UN Forum of Small States, the Marshall Islands is on the extreme end of the 'small' spectrum. All of this indicates that small states and territories will face distinct challenges and opportunities that arise from limited scale domestically, and as a result of being on the smaller end of asymmetrical relationships in international affairs.

In this spirit, the jurisdictions that have contributed their experiences and insights to the production of this paper form a Small States and Territories Working Group (STWG). The members include Andorra, Gibraltar, Guernsey, Holy See/Vatican, the Isle of Man, Jersey, Liechtenstein, Malta, Monaco and San Marino. This mix of states, Crown Dependencies, and a British Overseas Territory are all small in both material and relational terms in the international system, and they provide a variety of perspectives. Only Malta and Jersey have populations exceeding 100,000, but several are international finance centres, augmenting their international presence and connectivity far beyond their microscopic populations and territorial limits. IFCs, according to one definition, are 'jurisdictions that facilitate the international flow of capital'.[8] Although concentrated geographically in Europe, the guidance provided below aspires to be applicable to other small jurisdictions worldwide, that share the above characteristics, and some aspects may also be relevant to larger states.[9]

> *"Shifts in international leadership and the undermining of long-term strategic partnerships are contributing to a more fractured multilateral order."*

Defining Dual Use Goods

Noting that the scope and interpretation of dual-use goods varies across international, regional, and national frameworks, this paper does not seek to provide an exhaustive definition, but rather highlights selected formulations relevant to the assessment of proliferation financing risk.

The term "dual-use goods" encompasses items, software, or technology that have both civilian and military >

7 Long, Tom, *A Small State's Guide to Influence in World Politics (Oxford: Oxford University Press, 2022)*, p. 9.
8 IFC Forum, https://www.ifcforum.org/what-is-an-ifc/ .
9 This section was written with the contribution of Dr. Hillary Briffa at King's College London.

"Iran and the DPRK are the two jurisdictions that present the highest PF risk."

applications, including those capable of contributing to the development or production of weapons of mass destruction (WMD) and their means of delivery. The concept forms a foundational element of international export control frameworks designed to prevent proliferation and illicit transfers of sensitive goods and materials. Within the European Union, Regulation (EU) 2021/821 establishes a harmonised regime governing the export, brokering, technical assistance, transit, and transfer of dual-use items relevant to nuclear proliferation, defining them as goods that may serve both non-explosive purposes and assist in the manufacture of nuclear weapons or other nuclear explosive devices.[10]

The Wassenaar Arrangement similarly defines dual-use goods and technologies as those capable of both civil and military application, serving as a foundation for national control lists and multilateral transparency in strategic trade.[11] The United Kingdom's Export Control Order 2008 retains alignment with this framework, incorporating "catch-all" provisions enabling authorities to regulate unlisted items where a WMD end-use is suspected.[12] The United Nations Security Council, through Resolution 1540 (2004), reinforces these obligations by requiring all Member States to establish effective controls over materials, equipment, and technology that could contribute to nuclear, chemical, or biological weapons and their delivery systems.13 Complementing these legal instruments, the Financial Action Task Force (FATF) recognises the relevance of dual-use goods in the context of proliferation financing, noting that legitimate commercial trade in such items can be exploited to conceal illicit activity supporting WMD programmes.[14] Collectively, these frameworks illustrate the convergence of export control and financial integrity regimes in mitigating proliferation risks associated with dual-use items.

Evolving geopolitical dynamics and their implications for proliferation financing

'The past decade has seen a precipitous decline in global non-proliferation norms…'. [15]

The international security landscape nowadays is marked by significant and ongoing geopolitical realignments, some of which carry implications for the global non-proliferation architecture. Shifts in international leadership and the undermining of long-term strategic partnerships are contributing to a more fractured multilateral order, which may have a deleterious effect on the coherence and normative significance of multilateral export control regimes (MECRs) and non-proliferation regimes. One persistent driver of geopolitical instability remains Russia's full-scale invasion and occupation of Ukraine, where North Korean troops have recently seen action and Iranian-designed Shahed drones wreak havoc on civilian infrastructure. The intensification of military, economic and financial collaboration between these states presents new threats.[16] This collaboration is borne of strategic convenience and necessity, as mutual sanctions exposure creates an incentive for deepening partnerships.

Amidst such changes, the threat of nuclear proliferation remains acute. Considerably self-sufficient, the DPRK is still reliant on dual-use goods, foreign technologies and microelectronics for its ballistic missile, unmanned aerial vehicle (UAV), and centrifuge programmes. Trade between Iran and Russia in goods (such as rocket-fuel) underlines the continuing rapport between the countries.[17] Iran's first public commitment to nuclear non-proliferation in 2003 has been undermined by threats that they would withdraw from the non-proliferation treaty.[18] >

10 Regulation (EU) 2021/821 of the European Parliament and of the Council of 20 May 2021 setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items [2021] OJ L206/1.
11 Wassenaar Arrangement, Initial Elements – Objectives and Procedures (Wassenaar Secretariat 2019).
12 Export Control Order 2008, SI 2008/3231.
13 UNSC Res 1540 (28 April 2004) UN Doc S/RES/1540.
14 FATF, *Guidance on Proliferation Financing Risk Assessment and Mitigation*, (2020).
15 Arnold, Aaron and Salisbury, Daniel, 'Guide to Conducting a National Proliferation Financing Risk Assessment', *RUSI Special Resources*, (2024), p. 3.
16 FATF, *Report on Complex Proliferation Financing and Sanctions Evasion Schemes*, (2025), p. 13.
17 POLITICO, Iran in secret talks with China, Russia to acquire sanctioned missile fuel – POLITICO
18 See What if Iran withdraws from the NPT? – Bulletin of the Atomic Scientists.

The DPRK has continued testing intercontinental ballistic missiles, even if its signalling regarding its nuclear capabilities remains muted compared to the mid-2010s. Insight into the proliferation activities of the DPRK has been limited by the expiration of the mandate of the UN Panel of Experts established by Security Council Resolution 1874, which produced its final report in March 2024. The developing nexus between the DPRK and Russia is highlighted in this report via the continued clandestine shipping of crude oil and materiel between Russian and North Korean ports, in the use of North Korean armaments and manpower in Ukraine, and in the signing of a mutual defence treaty in 2024. Recent assessments aver that it is likely the DPRK is still reliant on some imported technologies for their nuclear and ballistic programmes, and the solidifying Russia-DPRK axis should give cause for heightened vigilance,[19] not least because the two countries signed a Comprehensive Strategic Partnership Treaty[20] in 2024, in which they commit to strengthening economic cooperation in customs and banking, potentially introducing new vulnerabilities in the global financial sector.[21]

China has traditionally played a pivotal role as a facilitator of DPRK sanctions evasion, both directly and through non-state actors. Over the years, Chinese trading companies, intermediaries, and organised crime groups have been instrumental in sustaining illicit revenue streams for the DPRK through cross-border smuggling, front company operations, and maritime trade circumvention. Open-source reporting and findings indicate that these networks continue to support DPRK-linked entities by transferring funds across the land border, engaging in ship-to-ship transfers in regional waters, and assisting in the movement of sanctioned commodities, such as petroleum.[22] In the cyber domain, some of the most sophisticated DPRK-led intrusions have reportedly benefited from logistical or infrastructural support facilitated through Chinese territory, illustrating the complex interplay between geography, commerce, and technology in modern sanctions evasion.[23]

"A non-state actor is an individual, group, or organization that operates independently of any government's direct control or authority, yet can pursue substantial political, military or ideological goals."

The trajectory of international security developments points towards an increasingly complex, and potentially destabilising, environment for nuclear non-proliferation norms. This nexus between international security and financial crime elevates the role of financial intelligence and underlines the need for sufficient legal, regulatory and operational safeguards to protect jurisdictions from PF exposure.

UN sanctions architecture

UN Security Council Resolution 1540, adopted in 2004, first recognised the proliferation of nuclear, biological, and chemical weapons (in the hands of non-state actors) as a threat to international peace and security. Under Chapter VII of the UN Charter, it is binding on all member states to implement appropriate policies in accordance with the resolution's guidelines. >

19 Arnold, Aaron and Salisbury, Daniel, 'Guide to Conducting a National Proliferation Financing Risk Assessment', RUSI Special Resources (2024), p. 9; Pawlus, Wojciech, 'Russia is Now Actively Funding North Korea's Nuclear Programme', RUSI Commentary (2025).
20 Centre for Strategic and International Studies (CSIS), 'The New Russia-North Korea Security Alliance', (2024), Victor Cha and Ellen Kim, [https://www.csis.org/analysis/new-russia-north-korea-security-alliance]
21 FATF, Report on Complex Proliferation Financing and Sanctions Evasion Schemes (2025), p. 13.
22 UN Panel of Experts Report, S 2021/777 (2021), p.48..
23 Centre for Strategic and Interntaional Studies (CSIS), 'Hidden Enablers: Third Countries in North Korea's Cyber Playbook', (2025), Sunha Bae, [https://www.csis.org/analysis/hidden-enablers-third-countries-north-koreas-cyber-playbook.]

The UN sanctions regime as relates to the DPRK's nuclear proliferation activities dates to Resolution 1718, passed in 2006 in response to the country's first nuclear test. This resolution called on all members states to prevent the 'direct or indirect supply, sale or transfer' of items, materials, equipment, goods and technology that could contribute to their proliferation efforts. It also included bans on luxury goods, the provision of technical training to DPRK nationals, and the freezing of assets owned by persons or entities linked to the DPRK. Subsequent resolutions (including UNSCRs 1874, 2087, 2094, 2270, 2321, 2371 and 2375) have typically been adopted in response to further nuclear or ballistic missile tests and have expanded the scope of sanctions to include new industries, goods, and entities. The most recent, Resolution 2397, was adopted in 2017 in response to the DPRK's last acknowledged nuclear test. Other international organisations, including the EU, and numerous states have imposed unilateral sanctions on the DPRK.

Similarly, UN sanctions against Iran relating to nuclear proliferation began in 2006 with UNSCR 1737, which was adopted in response to Iran's failure to comply with a prior resolution (1696) demanding the cessation of uranium enrichment activities. Amongst other provisions, it imposed a ban on the supply of nuclear-related technology and materials and imposed asset freezes on key individuals and companies related to their enrichment programme. Subsequent resolutions (including UNSCRs 1747, 1803, and 1929) imposed arms embargoes and implemented targeted financial sanctions against entities associated with the regime in Tehran. The JCPOA, agreed by the P5+1 in 2015, provided for the gradual lifting of sanctions in exchange for restrictions on Iran's nuclear activities. The plan was endorsed by UNSCR 2231. UN sanctions against Iran have accordingly expired. The US withdrew from the deal under the first Trump administration in 2018 and subsequently imposed unilateral sanctions under the principle of 'maximum pressure', which has been reinstated since his return to the presidency in 2025.[24]

The EU has maintained targeted sanctions in response to both Iran's proliferation activities and internal repression.

Target Jurisdictions

For the purposes of this guidance paper, a 'Target Jurisdiction' is a jurisdiction that presents a higher risk of proliferation, or which has a strong geographical, political, strategic, trade or other link with such a country. Participating countries would expect to include the DPRK and Iran as target jurisdictions due to extant and historic UN provisions relating to their proliferation activities. However, countries may have unilaterally designated other jurisdictions as high-risk because of one or more factors listed above. Assessing how and why certain jurisdictions are identified as being higher risk can improve understanding on perceptions of proliferation financing.

Identification of specific target jurisdictions falls outside the scope of this guidance. The analysis underpinning this guidance draws upon internationally recognised sources, typologies, and open-source information. The deliberate omission of state names referenced in the document, including those cited in reports of the United Nations Panel of Experts and other research sources, is intended to maintain analytical neutrality. Each jurisdiction applying this guidance is expected to independently determine its own list of target jurisdictions based on national context, risk assessment, and intelligence holdings.

This methodological choice does not diminish the objectives of the paper. Rather, the referenced case studies in Annex C are employed solely to illustrate typological examples that may assist competent authorities in identifying red flags, enhancing situational awareness, and developing a deeper understanding of proliferation financing risks and associated threat exposures.

Participating countries used various sources to compile a list of target jurisdictions. As expected, Iran and the DPRK are the two jurisdictions that present the highest PF risk, and this is reflected in the responses from participating jurisdictions. In the FATF's guidance, they are the only >

24 https://www.whitehouse.gov/presidential-actions/2025/02/national-security-presidential-memorandum-nspm-2/.

two countries named, owing to targeted UN sanctions against them. Jurisdictions may also wish to consider the FATF's mutual evaluation results, including those countries rated Non-Compliant (NC) or Partially Compliant (PC) with Recommendation 7 (targeted financial sanctions related to proliferation), as such deficiencies may indicate weaknesses in the implementation of PF controls and therefore heightened residual risk.

One participating jurisdiction noted the value of the United States' national PF risk assessment and used it to model their own. Another participating jurisdiction referenced the use of the EU Sanctions Map as well as resources from the Office of Foreign Assets Control (OFAC) and Office of Financial Sanctions Implementation (OFSI) to facilitate identification of target jurisdictions.

One participating jurisdiction classified several states as target jurisdictions based on findings from the US PF NRA.[25] The same jurisdiction also incorporated additional countries on its own initiative. Another participating jurisdiction, which drew upon the same external assessment to develop its list of target jurisdictions, further identified additional high-risk countries informed by sanctions authority alerts and transshipment risk analysis. The close and well-documented interconnections among certain high-risk states provided sufficient justification for their inclusion as target jurisdictions.

Jurisdictions should also consider consulting the FATF's list of jurisdictions under increased monitoring. Although these countries may not be undertaking proliferation activities themselves, they may (wittingly or unwittingly) be part of the chain of PF. For instance, a report by The Sentry in 2020 exposed the activity of two North Korean businessmen operating in Africa in violation of international sanctions. Their construction company banked with Afriland First Bank, and routed euro and dollar payments through the Paris branch of BMCE Bank International, headquartered in London.[26]

Non-State Actors

A non-state actor is an individual, group, or organization that operates independently of any government's direct control or authority, yet can pursue substantial political, military or ideological goals. Unlike states, non-state actors lack formal sovereign power, but their capabilities can be significant, especially when they engage in transnational activity such as terrorism, insurgency or proliferation. For example, Al Qaeda has long sought to acquire weapons of mass destruction (WMD), including nuclear, biological, and chemical arms to further its strategic objectives, making it a clear example of how a non-state actor can aspire to wield state-level destructive power even in the absence of formal state backing.[27]

The inclusion of 'non-state actors' in the US list reaffirms the provisions of UNSCR 1540 and broadens the understanding of target jurisdictions beyond state entities to encompass transnational networks operating across borders. This is significant for PF risk assessments, as non-state actors can exploit jurisdictional vulnerabilities to facilitate procurement and financing activities on behalf of sanctioned programmes. While some analytical frameworks draw parallels between TF and proliferation financing PF, these should be treated cautiously: although both involve attempts to conceal the origin and destination of funds, PF is typically characterised by larger, commercially structured transactions linked to corporate or trade networks, rather than the smaller, informal transfers more common in TF. The distinction is therefore important for identifying high-risk jurisdictions where non-state actors may operate within legitimate trade systems to advance proliferation objectives.[28] >

25 See US National Proliferation Financing Risk Assessment (2024), 2024 National Proliferation Financing Risk Assessment (NPFRA).
26 The Sentry, *Overt Affairs: How North Korean Businessmen Busted Sanctions in the Democratic Republic of the Congo (2020)*, p. 3.
27 Al Qaeda Weapons of Mass Destruction Threat: Hype or Reality? | The Belfer Center for Science and International Affairs
28 També, Noémi, *Institutional Proliferation Finance Risk Assessment Guide*, RUSI Special Resource (2023), p. 7.

Methodological Framework

This guidance is based on information provided by participating jurisdictions, supported by additional research and expert analysis. Structured questionnaires were issued to STWG members to collect information on perceived PF threats, vulnerabilities and risks. Responses were received from Andorra, Gibraltar, Guernsey, the Holy See/Vatican City State, the Isle of Man, Jersey, Liechtenstein, Malta, Monaco, and San Marino. The complete list of questions included in the questionnaire can be found in Annex A.

These inputs were reviewed and analysed alongside open-source research, UN Panel of Experts reports, typologies published by international standard setters, and relevant case studies. Additional insights were drawn from engagement with international subject matter experts. The analysis combines these sources to provide guidance on assessing PF risk in small states and territories, reflecting both jurisdictional experience and external analysis.

"The analysis combines these sources to provide guidance on assessing PF risk in small states and territories, reflecting both jurisdictional experience and external analysis."

The rest of this guidance paper will be divided into five sections:

1) ***Threats, vulnerabilities, and consequences*** outline the three factors that together constitute risk according to the FATF. It expands on these three factors using Royal United Services Institute (RUSI) guidance and highlights how these three vectors might apply to small states and territories when considering PF risk.

2) ***Typologies and red flags*** highlight several key common risk areas and examples that may be particularly relevant for small states and territories.

3) ***Understanding PF risks in small states and territories*** surveys the threats and vulnerabilities that such jurisdictions may be especially prone to facing, particularly those that are IFCs.

4) ***Mitigating PF risks in small states and territories*** aims to articulate what measures can be taken to help small states and territories produce effective PF NRAs and safeguards, including export controls, public-private partnerships, and building understanding and awareness.

5 ***Conclusion*** conclude the paper by providing a summation of findings and actionable steps that can be taken to ensure that small states and territories meet and exceed international expectations when it comes to assessing and managing PF risks.

Threats, Vulnerabilities and Consequences

Proliferation financing risk is described by the FATF as a 'function of three factors': threat, vulnerability, and consequence. It further refers to the obligations to identify, assess and understand the risks of potential breach, non-implementation or evasion of TFS (pursuant to Recommendations 1 and 7) of the FATF Standards. According to the FATF, in the context of Recommendation 1, "proliferation financing risk" refers strictly and only to the potential breach, non-implementation, or evasion of the targeted financial obligations referred to in Recommendation 7.[29]

" The FATF defines 'threat' as 'designated persons and entities that have previously caused or have the potential to evade, breach or exploit a failure to implement PF-TFS in the past, present or future...'"

Risk can be further subdivided into concepts of **inherent risk** and **residual risk.**

Inherent risk= refers to 'the natural level of risk, prior to introducing any measures to mitigate or reduce the likelihood of an actor exploiting that risk...'. Can include close links with designated persons under PF-TFS regimes, production of dual use goods, or the nature of services provided by a private sector firm.

Residual risk = risk which 'remains after the risk mitigation process'. A high degree of assessed residual risk might mean control measures are inadequate and require remedial measures.[30]

Threats

To effectively combat PF, it is crucial to understand the range of actors and methods involved. The FATF defines 'threat' as 'designated persons and entities that have previously caused or have the potential to evade, breach or exploit a failure to implement PF-TFS in the past, present or future...'.[31] Implicit in this definition is intent and capability. Intent refers to the motivation or willingness of an actor (whether a state, non-state group, or individual) to engage in or support proliferation-related activity. It encompasses the ideological, political, strategic, or economic reasons that drive an actor to pursue or assist in the development, acquisition, or financing of weapons of mass destruction (WMD) or related materials. Capability, by contrast, refers to the practical means or resources that enable an actor to realise that intent. This includes access to technical expertise, financial networks, procurement channels, or materials necessary to support proliferation activities. In practice, assessing threat involves considering both dimensions together:

	High Intent	Low Intent
High Capability	**Critical Threat** - actors with both the motivation and means to evade PF-TFS (e.g. sanctioned networks, state-linked traders).	**Latent Threat** - may become dangerous if intent emerges (e.g. global logistics firms with weak controls).
Low Capability	**Limited Threat** - may want to evade but lack the means (e.g. small traders).	**Minimal Threat** - neither means nor motive.

29 FATF, *Guidance on Proliferation Financing Risk Assessment and Mitigation*, (2021).
30 FATF, *Guidance on Proliferation Financing Risk Assessment and Mitigation* (2021), p. 9.
31 Arnold, Aaron and Salisbury, Daniel, 'Guide to Conducting a National Proliferation Financing Risk Assessment', *RUSI Special Resources* (2024), p. 16.

Thus, threat under FATF's PF framework reflects what someone has done, as well as what they are capable of and inclined to do.

RUSI summarises the FATF definition by stating that threat 'refers to either the actual presence of a previous breach of sanctions or the potential future breach of sanctions within a jurisdiction'.[32]

Small states may face threats that arise from:

- **Proximity to conflict regions or alignment with larger powers that might be targeted by PF networks.**
- **Direct or indirect trade links with target jurisdictions**
- **Small states and territories with ports, free-trade zones, or similar facilities may be targeted by networks that exploit trade mechanisms for PF.**
- **Small financial sectors may give the perception to PF networks of offering lower visibility or easier integration of transactions within routine financial activity.**
- **Small states and territories with pronounced sectors with a higher exposure to PF risks (such as trust and company service providers or virtual asset service providers) may be targeted by proliferating networks.**
- **The multi-jurisdictional and multi-sector nature of PF-related activities, which means that even where threat levels are low, smaller jurisdictions should remain alert to the potential misuse of shell companies and TCSPs by individuals acting on behalf of designated entities.**

RUSI proposes a further practical distinction for the purpose of distinguishing between different types of financing threats: **'direct'** and **'indirect.**

- **Direct** refers to the 'actual or attempted financing of proliferation-sensitive goods and technologies'. For instance, Iranian procurement efforts seeking to source high-end pressure sensors for its uranium enrichment programme.
- **Indirect** refers to activities 'that could substantively contribute to a state or non-state actor's WMD programme'. The most common form is revenue-raising activity: the DPRK's use of cyber-attacks/ransomware and operation of foreign-based businesses are two such examples.[33]

The nature of PF-related activities necessitates the use of 'multi-jurisdictional, multi-sector networks', meaning that even with low threat registers, smaller states and jurisdictions should be wary of being used for the setting up of shell companies, or the exploitation of TCSPs by people acting on behalf of designated entities.[34]

The threat landscape is constantly evolving. With the rapid advancement of virtual assets and cyber technologies, small states and territories face increasing risks from cyber-enabled proliferation financing methods, which exploit weaknesses in digital systems for PF purposes.

In addition to the internationally recognised three stages of proliferation financing (raising, obscuring, and procuring), the STWG has highlighted that small states may also face risks linked to the storage or holding of funds and assets. This reflects cases where proliferation-linked assets may be retained or administered within legal persons or arrangements, including those managed by TCSPs. Such circumstances can provide a means of concealment for beneficial ownership or control and represent a material vector of PF exposure in certain jurisdictions. >

32 Arnold, Aaron and Salisbury, Daniel, 'Guide to Conducting a National Proliferation Financing Risk Assessment', ***RUSI Special Resources*** (2024), p. 25.
33 Arnold, Aaron and Salisbury, Daniel, 'Guide to Conducting a National Proliferation Financing Risk Assessment', ***RUSI Special Resources*** (2024), p. 26.
34 Ibid, p. 25.

Stage of Financing	Threat Description
Raising of funds	PF networks generate or access capital through front companies, charitable fronts, or legitimate commercial ventures, concealing the true purpose of the funds to support proliferation-related procurement.
Obscuring of funds	Funds are transferred through multiple accounts, intermediaries, or jurisdictions using complex ownership structures to hide their origin, control, and intended use, exploiting gaps in financial transparency.
Storage of funds	Retention or administration of funds or assets linked (or potentially linked) to proliferation within legal persons or arrangements, prior to or between active use in procurement or other stages. For example, TCSPs may be used to establish or manage companies, trusts, or foundations that hold bank accounts or other assets, allowing funds to remain dormant while obscuring control and intended proliferation-related purposes.
Procurement and transport of goods and technology	Concealed funds are used to purchase dual-use goods, materials, or technology through falsified end-user certificates, transshipment, or re-routing via third countries, making it difficult to identify the ultimate recipient or proliferation purpose.

Vulnerabilities

Where 'threats' refers primarily to external conditions, 'vulnerabilities' is more concerned with the internal structures and circumstances of a jurisdiction.

Every jurisdiction, irrespective of its levels of awareness and understanding, will have known and unknown vulnerabilities to proliferation financing. These can potentially be exploited by identified threats, and may 'support or facilitate the breach, non-implementation or evasion of TFS'.

Examples might include weakness in the laws or regulations comprising a country's national counter-proliferation financing regime, and contextual features that might provide opportunities for designated persons to raise or move funds. The private sector will have its own vulnerabilities, including those inherent to a particular sector or type of financial product or service.

Vulnerabilities in small states and territories can arise due to factors such as lack of availability of or access to relevant intelligence (beyond financial intelligence) and finite resources. There is also a need to stay attentive to structural vulnerabilities and emerging threats: PF involves a vast range of sectors, jurisdictions, and entities. Some sectors are more vulnerable than others in terms of their likelihood of being targeted. Small states and territories that are IFCs and have extensive international financial networks are at risk. Members of the STWG are leaders in various sectors, including insurance, banking, gambling, TCSP, and VASP, and several possess manufacturing, engineering, maritime, and port facilities.

Key areas of vulnerability, for small and large states alike, usually involve weaknesses in domestic and sectoral political, economic, legal, and technological structures and capacities. Generally, jurisdictions may be targeted if they:

- **Have perceived weak AML rules and regulations, including lax beneficial ownership transparency obligations.**
- **Lack adequate understanding and enforcement capability and capacity.**
- **Have weak governance, unstable political institutions, high levels of corruption and/or organised crime.**
- **Operate port and maritime services with scope for transshipment.**
- **Contain VASPs and other digital asset services operating in their jurisdiction.**
- **Have underdeveloped or poorly implemented export control systems, particularly in the realm of dual-use goods and/or proliferation-sensitive materials.** >

Consequences

Failing to manage PF risks can have far-reaching implications for small states and territories, including:

- **Jurisdictions with weak PF controls may face censure by the FATF (e.g. "grey listing"), political pressure or even unilateral or multilateral measures from other jurisdictions, as well as potential international sanctions, resulting in significant economic and reputational damage.**
- **PF activities can undermine the reputation and stability of local financial systems, leading to broader economic vulnerabilities. Private businesses reliant on access to international financial markets may experience operational hardship due to global community's reduced risk appetite and potential secondary sanctions.**
- **PF networks may contribute to a rise in associated criminal activities, exacerbating local crime rates and corrupt practices.**

Small states and territories can inadvertently become conduits for PF, increasing security risks within their borders and potentially contributing to broader global threats. The ultimate consequence of failing to prevent or address PF is the production and deployment of weapons of mass destruction, which can have devastating human, environmental, and economic impacts. Small states and territories are often more vulnerable in terms of supply-chains and self-sufficiency, depending on global co-operation for many critical goods and services. Consequently, they would feel the impact of international political instability most keenly.

Understanding PF Risks in Small States and Territories

Useful sources and methodologies

FATF guidance on PF methodology relating to risk assessment and mitigation is the sine qua non for any jurisdiction, small or otherwise. Understanding what the successful and effective implementation of recommendations and immediate outcomes looks like is fundamental for ensuring compliance with international standards. Jurisdictions should consult the FATF guidance on counter proliferation financing (2018), guidance on proliferation financing risk assessment and mitigation (2021), their typology report (2008), and their combating proliferation financing status report (2010).

The original typology report released by the FATF is now seventeen years old. While these risk indicators remain relevant, proliferators are constantly adapting their methods to avoid detection. A 2017 report produced by the Project Alpha team at King's College London evaluates the usefulness of these indicators and supplements them with more recent cases of proliferation financing to ensure contemporary relevance. By their own admission, however, even this report only analyses 'classic and established' financial mechanisms. It consciously omits examples relating to digital technologies or new payment methods, although it accurately predicts their future use in proliferation activities.[35] The FATF has recently published up-to-date guidance in 2025, following their 'Complex Proliferation Financing and Sanctions Evasion Schemes' project. This report is based on submissions by contributing states, and highlights the persistence of low efficacy of PF provisions internationally, an updated typologies section, best practices for mitigating PF risk, and guidance related to the evasion of sanctions relevant to PF. >

35 Brewer, Jonathan, 'Study of Typologies of Financing of WMD Proliferation: Final Report', *Project Alpha: King's College London* (2017), p. 27.

The Panel of Experts' reports, pursuant to Resolution 1874, offer an invaluable resource that remains relevant, even though it will not produce further studies after its final report was released in March 2024. Offering expert analysis and recent evaluations of case studies relating to the DPRK's nuclear programme, almost no other publicly available resource can provide such a comprehensive overview of the evolving strategies the DPRK deploys in their procurement and financing activities. Ranging from maritime sanctions evasion to their cutting-edge cybercrime capabilities to the operation of IT workers overseas, it remains a crucial repository for deepening understandings and uncovering gaps in risk assessments. A full list of the available reports can be found here. [36]

The Multilateral Sanctions Monitoring Team (MSMT) was established after the disbandment of the Panel of Experts and is composed of a broad coalition of international partners including Australia, Canada, France, Germany, Italy, Japan, the Netherlands, the Republic of Korea, the UK and US. This multilateral grouping pools resources and allows the continued monitoring of the effectiveness of UN sanctions against the DPRK. The first report of the MSMT was published in May 2025, addressing the ongoing unlawful military co-operation between the DPRK and Russia.

Nonetheless, implementing states often find that further guidance is necessary to fully understand best practices and learn, in practical terms, what measures are being taken and what form proliferation financing takes.

There are several useful resources that jurisdictions may wish to consult in developing their PF risk assessments. Guidance produced by RUSI has been extensively cited by countries in the STWG. They have developed two guides to conducting a national proliferation financing risk assessment, published in 2019[37] and 2024[38]. The most recent guide was authored by Aaron Arnold and Daniel Salisbury, academic experts in sanctions and proliferation financing. Dr. Arnold was formerly a member of the UN Panel of Experts for DPRK sanctions.

The US 2024 National Proliferation Financing Risk Assessment, produced by the Department of Treasury, serves as an insightful example of a PF risk assessment. It highlights potential target jurisdictions beyond those sanctioned by the UN, emerging trends, and articulates several case studies for reference. The continued predominance of the US dollar in international finance and trade might make this document particularly useful for broadening understandings of illicit flows. One jurisdiction found it helpful to use this PF NRA as a template in developing their own.

A full list of resources available to facilitate understanding and management of PF risks can be found in Annex A.

Dual-use goods and export controls

Dual-use goods and technologies have both civilian and military applications. For the sake of PF, this includes goods or technologies that can contribute to the development and manufacture of nuclear, biological and chemical weapons (or their means of delivery). For >

" Dual-use goods and technologies have both civilian and military applications. For the sake of PF, this includes goods or technologies that can contribute to the development and manufacture of nuclear, biological and chemical weapons."

36 These can be found and searched through an integrated tool developed by RUSI, see https://dprk-reports.org/.
37 Joshi, Anagha, Dall, Emil, and Dolzikova, Darya, RUSI, Guide to Conducting a National Proliferation Financing Risk Assessment (2019).
38 Arnold, Aaron and Salisbury, Daniel, 'Guide to Conducting a National Proliferation Financing Risk Assessment', RUSI Special Resources, (2024).

instance, a triggered spark-gap has legitimate uses in a lithotripter, a medical device used to treat kidney stones; or it can be used as a trigger for a nuclear weapon. Determining their end-use can consequently be quite challenging.

The trade and transfer of dual-use goods and technologies pose a potential PF risk. Small states and territories should have sufficient, proportionate checks (including export controls) and mechanisms to monitor the flow of dual-use goods in and out of their jurisdiction. Purchases of dual-use goods are usually settled using different forms of financial transactions, including 'conventional' financial institutions and, increasingly, VASPs and digital currencies.

To address these risks, various MECRs have been developed. These regimes restrict the export of sensitive goods, to make it more difficult for states of proliferation concern to obtain them.

- **The Zangger Committee, formed in 1971, maintains a 'trigger list' of nuclear-related strategic goods to assist parties to the Non-Proliferation Treaty in identifying equipment and materials subject to export controls.**
- **The Nuclear Suppliers Group (NSG) is a group of nuclear-supplier countries which since 1974 has implemented two sets of guidelines seeking to limit the proliferation of nuclear weapons.**
- **The Australia Group, which first met in 1985, focuses on limiting the spread of chemical and biological weapons through the harmonising of export controls, developed in response to Iraq's use of chemical weapons in the Iran-Iraq war.**
- **The Missile Technology Control Regime (MTCR), established in 1987, aims to restrict the proliferation of missiles, rocket systems, UAVs and related technologies, as well as systems intended for the delivery of WMDs via export controls applied to a common list of controlled items.**

MECRs are not legally binding but are voluntary associations that aim to establish and maintain standards for national export control systems that countries should have. Common lists of controlled goods and technologies are regulated by relevant authorities.[39] These are publicly available and are invaluable resources for small states and territories that are not participants.

Data collected for the purposes of this paper demonstrates that the measures taken by members of the STWG appear to be largely proportionate to the level of risk they face. Some jurisdictions are landlocked and have very small (or non-existent) industrial sectors and trade hubs. Others, with busy ports, manufacturing, and engineering sectors and finance centres, reported much more stringent measures in place regarding the monitoring of people and goods entering and leaving the jurisdiction. In line with R.1, states and territories should take 'commensurate action', which suggests a proportional approach.

It is also useful to understand what goods are produced, or what technologies are developed, in the jurisdiction, and whether any of these are considered dual-use, as per local definitions. This will be helpful in determining the level of risk for the country, although it will not give a full picture unless it is also understood if any dual-use goods are being imported to, or transited through, the country.

One potential way to monitor this is by implementing a dual-use goods license. A participating jurisdiction implemented this, ensuring that there is a self-declaration of intent to export dual-use goods, which is contingent upon government approval. Education and awareness raising will be a key component of implementing this action, given that the manufacturing and engineering sectors may be less familiar with the principles of AML/CFT/CPF than those in the regulated sector.>

39 Some of the preceding material was sourced from a presentation delivered by Dr. Togzhan Kassenova in July 2024.

Evidently, various resource constraints may limit abilities to screen every single item entering or leaving a jurisdiction for dual-use potential but ensuring that these processes are proportionate to the state or territory's exposure level is a key means of mitigating PF risk. The ever-increasing complexity of global trade patterns means that small states and territories with freeports or maritime anchorages must stay vigilant for future attempts to exploit their transit hubs and territorial waters for PF-related activity.

Cross-border movement and shared travel frameworks

Small states and territories that participate in, or are associated with, wider travel and mobility zones (such as regional free movement areas, customs unions, or shared border management frameworks) may face distinct challenges in managing proliferation financing (PF) risk. In some cases, border control, visa issuance, and customs responsibilities are administered jointly with, or delegated to, another state. In such arrangements, the primary point of entry for individuals or goods may be located in another jurisdiction, with subsequent movement within the shared zone occurring without further checks. This can reduce the jurisdiction's direct visibility and control over who or what enters its territory, including the ability to monitor the arrival of persons, goods, or funds that may be connected to proliferation networks. While such arrangements bring clear economic and political benefits, they can also introduce dependencies that limit the jurisdiction's ability to independently monitor, record, or restrict the movement of persons, goods, and capital for counter-proliferation purposes.

These structural factors do not reflect weaknesses in governance, but rather the realities of integrated regional systems. Nevertheless, jurisdictions should recognise the potential PF vulnerabilities associated with shared travel and customs frameworks, particularly in ensuring timely access to information, the ability to identify dual-use goods or sanctioned actors in transit, and the maintenance of domestic awareness of movements across their borders. Close cooperation and information-sharing arrangements with the partner state or regional authority responsible for border control are essential to mitigate these risks.

Students who are nationals or residents of target jurisdictions

As part of their sanctions against the DPRK, UN resolutions have imposed restrictions on the provision of 'technical or financial assistance, training, or resources related to certain nuclear and ballistic missile-related goods' (and variances on this terminology to the same effect).[40] Such risks are tangible and have been detected. The Panel of Experts reported that two DPRK researchers from the Pyongyang University of Science and Technology, who were studying PhD courses at a Swedish university, completed life science research courses in 2019 and 2020. One of them subsequently found employment at a Swedish research institute. This was deemed a violation of the overseas workers provision in paragraph 8 of Security Council resolution 2397.[41]

We acknowledge that across participants of the STWG, the threat level is likely significantly lower due to the limited size, number and profile of research institutions present. Almost all participants indicated that no courses are offered by higher education institutes in the fields of nuclear energy, cyber-science, or specialist courses more broadly that could contribute to proliferation programmes. One jurisdiction offers master's-level programmes in cybersecurity, electrical engineering, and microelectronics,

Small states and territories should nonetheless remain vigilant that if any courses are offered by national research bodies in the future, sufficient attention is placed on admissi ons to ensure that DPRK and Iranian nationals are not permitted to enrol in courses that may contribute to their country's nuclear programmes.

40 See UN Security Council Resolutions 1737 and 2270.
41 UN Security Council, *Report of the Panel of Experts established pursuant to Resolution* 1874, S/2024/215 (2024), p. 141 and S/2023/171 (2023), p. 9.

but has affirmed that no research institutions have ties to any jurisdiction of proliferation concern.

Diplomats have been identified as contributing to the DPRK's proliferation activities in several ways. Their ability to run businesses, trade sanctioned commodities, lease diplomatic real estate and engage in arms dealing generates revenue that is funnelled back into WMD and military programmes. In a related but separate vein, they have also been able to build procurement networks involving dual-use and military goods and technologies. For instance, the 2022 UN Panel of Experts report noted the case of O Yong Ho, a Moscow-based diplomat who successfully procured a range of technologies for the DPRK's missile programme between 2016 and 2020. In 2018, a German intelligence official also suggested that the Berlin embassy had been used to acquire missile and nuclear-related dual-use technologies since 2016.[42]

The DPRK's diplomatic network has decreased in scope considerably in recent decades; most members of the STWG declared no diplomatic, commercial, geographic, or cultural links to the country. However, in jurisdictions within the Schengen Area, accredited DPRK diplomats may still benefit from the ability to move freely across member states, potentially facilitating travel, logistical coordination, or the establishment of informal networks that extend beyond their country of accreditation. One participating jurisdiction did indicate limited commercial and trade ties with Iran, although it clarified that export and imports to the country are minute (0.02% of the jurisdiction's exports and 0.001% of imports involved Iran) and its commercial ties have been zero since 2022.

Sectoral vulnerabilities

Understanding sectoral PF vulnerabilities requires both jurisdiction-level and institutional-level analysis. Jurisdictions should conduct sectoral risk assessments to identify, assess, and understand PF risks within specific sectors, taking account of their size, materiality, and international exposure. Likewise, institutions (particularly those operating in higher-risk sectors such as TCSPs, VASPs, banks, and maritime actors) should complement this by conducting their own institutional risk assessments, incorporating PF typologies and sector-specific indicators into their controls. This dual approach helps ensure that both public and private sectors are able to recognise and mitigate risks arising from their unique operating contexts.

Trust and Corporate Service Providers (TCSPs)

TCSPs are inherently vulnerable because of the risk that designated persons and entities could exploit them to obscure the links between financial transactions that may have links to proliferation-sensitive goods and beneficial owners. Various members of the STWG have relatively significant TCSP sectors, which are a regular feature of many IFCs internationally. Jurisdictions should ensure that customers serviced by TCSPs are monitored for their involvement in shipping or maritime services, the manufacturing or transport of dual-use goods and weaponry, and other links to countries of proliferation concern. The regular use of third-party intermediaries and front companies alongside TCSPs makes interception more challenging (though not impossible).[43] >

" diplomats have been involved in attempting to procure sensitive materials, steal WMD-related information, and access the international financial system to transfer revenues."

42 Salisbury, Daniel, 'From Missions to Missiles: The Role of North Korea's Diplomatic Corps in Sanctions-Busting', *RUSI Emerging Insights* (2022), pp. 12-13.
43 See FATF Report, *Complex Proliferation Financing and Sanctions Evasion Schemes* (2025), pp. 22-33 for several case studies employing intermediaries, front companies, and TCSPs.

In many small states, the TCSP sector is material with common characteristics that warrant particular attention from supervisors and policymakers. The risks they face often arise from the complexity of corporate structures and the diversity of services provided (including company formation, nominee directorships, trust administration, and the provision of registered office or management/secretarial services). Where only limited services are provided (for example, purely registered office or company secretarial services), there may be minimal visibility over, or oversight of, the underlying activities of corporate clients, which can create additional proliferation financing risk. These circumstances can enable designated persons to misuse legal structures to store or hold funds and assets under the guise of legitimate activity. The opacity of cross-border corporate structures and use of multi-layered entities increases the difficulty of tracing beneficial ownership and identifying proliferation-linked activity.

Jurisdictions with significant TCSP sectors should therefore ensure that their sectoral and institutional risk assessments explicitly capture PF-related risks, including those linked to the storage and administration of assets and the use of TCSPs to facilitate front or shell company activity. Supervisory frameworks should incorporate PF-specific indicators and require TCSPs to consider proliferation risk within customer due diligence, ongoing monitoring, and beneficial ownership reporting.

Virtual Asset Service Providers (VASPs)

VASPs remain an evolving sector, regularly being transformed by technological innovations that facilitate the instant exchange of cryptocurrency. While these providers offer many useful services, the reality remains that the relative anonymity, uneven regulatory landscape and instantaneous digital nature of cryptocurrency transactions lend themselves to illicit ends. Many IFCs are leading the way in regulating VASPs and distributed ledger technology (DLT), but globally, the sector remains fledgling in terms of regulatory standards. Several small states have material VASP sectors, reflecting their broader roles as regional and international finance centres. As described below, a track record of the DPRK targeting cryptocurrency exchanges highlights the increased risk nexus facing small states and territories making forays into the sector. This also applies to alternative payment infrastructure, in particular blockchain based payments (including stablecoins).

“ the reality remains that the relative anonymity and instantaneous digital nature of cryptocurrency transactions lend themselves to illicit ends.”

Across small states, common PF exposures within the VASP sector typically relate to the complexity and speed of digital asset transfers, the challenges in tracing transactions that move across chains or jurisdictions, and the potential use of virtual assets to raise or move funds in support of sanctioned programmes (for instance, through ransomware operations or state-sponsored cyber activity). These risks are further heightened by the presence of nested relationships, particularly where over-the-counter (OTC) brokers or other un-regulated or lightly regulated virtual asset service providers access the financial system indirectly through regulated VASPs. Such nested OTC arrangements can obscure the true originator or beneficiary of transactions, weaken the effectiveness of customer due diligence, and create blind spots that may be exploited to evade sanctions or move funds on behalf of sanctioned actors. >

In addition, PF risk may arise where VASPs seek to access the traditional financial system by opening accounts with financial institutions while misrepresenting their true nature or activities, for example by presenting themselves as software developers, IT consultants, or technology service providers. In such cases, the financial institution may fail to apply appropriate VASP-specific enhanced due diligence, transaction monitoring, or sanctions screening commensurate with the actual risk posed. This misalignment between perceived and actual risk can undermine supervisory oversight and create opportunities for sanctioned entities or jurisdictions to access fiat on- and off-ramps.

Importantly, even where a jurisdiction does not have a material VASP sector, there may still be significant virtual asset activity or adoption within the wider economy (including among individuals, businesses, or financial intermediaries) which can nonetheless present PF risk. National risk assessments should therefore capture both the regulated VASP sector and wider virtual asset activity within the economy. This includes consideration of alternative payment infrastructures such as stablecoins and other blockchain-based mechanisms. Supervisors should work collaboratively with the private sector, FIUs and law enforcement to ensure that PF typologies are understood across sectors and that risk management frameworks reflect the evolving virtual asset landscape.

Banks

Banks are inherently vulnerable to PF due to their central role in international trade and cross-border payments. Core banking services are known to be exploited by sanctioned actors to obscure the movement of funds linked to the procurement of dual-use goods. Banks in IFCs are particularly exposed where they service cross-border corporate structures, complex supply chains or clients operating in higher-risk sectors and jurisdictions. Globally, local domestic banks are underequipped to tackle proliferation financing risk as efficiently as major international banks. The latter can provide useful guidance to jurisdictional private sector compliance working groups. Although the banking sector is generally well established and subject to higher regulatory scrutiny than many other sectors, its global reach, extensive correspondent relationships and involvement in complex trade activity mean that it remains a key target for proliferation networks seeking to integrate illicit transactions into legitimate financial flows.

Money Value Transfer Services (MVTS)

MVTS, including remittance providers and informal value transfer systems, are vulnerable to PF risk due to their ability to move funds rapidly across borders with limited transparency. Their business models often rely on extensive agent networks and cash-based transactions, which can be exploited by designated entities seeking to fragment payments or avoid detection by formal banking channels. MVTS are particularly exposed when servicing trade-dependent clients, migrant worker communities and high-risk corridors where funds may be routed through intermediary countries to conceal their destination as jurisdictions of proliferation concern. The frequent use of third-party senders and recipients, reliance on personal or community relationships, and minimal documentation typical of some MVTS networks create additional opportunities for PF actors to integrate into legitimate financial flows while avoiding detection. >

" Banks in IFCs are particularly exposed where they service cross-border corporate structures, complex supply chains or clients operating in higher-risk sectors and jurisdictions."

Marine insurance

Marine insurance represents an additional area of potential PF vulnerability that warrants closer attention. While it plays a critical role in facilitating international trade and maritime operations, marine insurance typically falls outside the scope of AML/CFT frameworks and, in many jurisdictions, is not subject to the same level of regulatory oversight for financial crime prevention purposes. This creates potential blind spots for PF exposure, particularly in relation to the coverage of vessels, cargoes, or companies linked to sanctioned jurisdictions or designated persons.

Risks may arise through the provision of insurance to vessels engaged in deceptive maritime practices, such as AIS spoofing, illicit transshipment, or identity laundering. The use of brokers, reinsurers, and complex ownership structures further complicates due diligence and may obscure the true beneficiary of a policy. Supervisory bodies and competent authorities should therefore consider whether CPF engagement or oversight of the marine insurance sector is warranted based on context, materiality and identified risks, even where the sector does not otherwise fall within AML/CFT supervision. This could include outreach, thematic reviews, or targeted supervisory engagement aimed at raising awareness of PF typologies and promoting the adoption of proportionate risk mitigation measures.

Maritime sector

The maritime sector is a key sector of heightened risk for PF (both inherent and residual). Maritime trade is a key conduit for dual-use and nuclear-related goods, oil and petroleum products, and military materiel. Seaborne transport presents an opportunity for proliferating states and designated entities to engage in deceptive practices and circumvent international restrictions on the import and export of restricted and banned items. In the case of DPRK specifically, UN Sanctions prohibit almost all kinds of exports and imports by the country, so vessels facilitating North Korean trade in licit, non-dual-use and non-nuclear-related goods (e.g. seafood, textiles) are also deemed to be evading sanctions for the purpose of revenue raising and ultimately proliferation financing.

"Maritime sanctions aim to limit the ability of states to generate revenue from trade involving proscribed goods or acquire critical items for their nuclear programmes."

Maritime sanctions aim to limit the ability of states to generate revenue from trade involving proscribed goods or acquire critical items for their nuclear programmes. Sanctioned states often employ various deceptive practices to circumvent these restrictions; for instance, Automatic Identification System (AIS) spoofing, where vessels falsify AIS transmissions to conceal their true location and identity. This manipulation complicates the tracing of vessels and presents significant challenges to maritime security, making it harder for authorities to monitor sanctioned vessels effectively.

Sanctioned actors might also acquire new vessels under different names/flags or through intermediary entities, reducing the risk of detection. 'Vessel identity laundering' operations represent a serious threat to the integrity of the International Maritime Organization (IMO) ship registration system. This tactic enables ships linked to illicit activities, often referred to as 'dirty' ships, to assume 'clean' identities by manipulating their AIS transmissions. In this process, vessels adopt a different identity by fraudulently obtaining legitimate information from the IMO, often using false documentation or employing shell companies to create a deceptive appearance of compliance.>

Typology of Reflagging Deception Practice – DPRK

The United Nations Panel of Experts has documented these manoeuvres in its reports (available in Annex A), highlighting the need for robust compliance frameworks to counter such evasions and mitigate PF risks associated with sanctioned states. Due to its transnational nature and inherent complexity, the global maritime industry requires multi-layered corporate structures, international safety management systems, and diverse labour sources to manage assets across jurisdictions. These structures enable legitimate companies to operate within various legal frameworks but also create opportunities for illicit actors to conceal the true ownership of sanctioned cargo through the use of shell companies, multi-tiered ownership structures, and shifting management.

The UN Panel of Experts has highlighted how the DPRK employed reflagging as a key deception tactic to evade sanctions on petroleum imports. By frequently changing vessel flags, registrations, and nominal ownership, often through short-lived shell companies that were dissolved soon after use, DPRK-linked operators sought to obscure true control of ships involved in illicit ship-to-ship fuel transfers. This constant reflagging created a misleading appearance of legitimate international ownership and complicated efforts by authorities to trace or seize the vessels. Combined with the use of small, non-IMO-numbered coastal ships, these practices enabled the DPRK to maintain covert supply chains and conceal its continued procurement of restricted petroleum products.

One commonly practiced evasive measure undertaken by the DPRK is ship-to-ship (STS) transfers, which involve direct cargo transfers between vessels at sea, presenting challenges to enforcement. While STS transfers are used for legitimate purposes such as cargo blending or moving goods between vessels of different capacities, they are vulnerable to misuse. Illicit actors exploit STS transfers to conceal the origin or destination of covertly traded commodities, often conducting these transfers at night or in high-risk areas, which makes enforcement and tracking efforts more challenging. Enforcement remains a key difficulty for states that have no recourse to prevent these transfers in the Korea Bay or Southeast Asia more broadly. This DPRK risk has a strong geographical component, which is lower in Europe. On the rare occasion that vessels suspected of engaging in illicit trade with the DPRK enter European waters (see the US and EU-designated Maia-1's unprecedented voyage from Suez through the Mediterranean), international maritime law severely limits available enforcement measures.[44]

In the case of Iran, ship-to-ship (STS) transfers also represent a principal sanctions-evasion technique, used extensively to disguise the origin and ownership of petroleum cargoes. The US Department of the Treasury has documented networks facilitating the Iranian oil trade through STS transfers, blending of Iranian crude with oil from other jurisdictions, falsified cargo documentation, and the use of third-party-flagged vessels to conceal Iranian control.[45] These networks often operate beyond Iranian territorial waters, exploiting regulatory gaps in the Gulf of Oman and the Arabian Sea. RUSI further observes that Iran's so-called "shadow fleet" employs tactics such as flag-hopping, vessel renaming, and the use of permissive registries to sustain these operations despite international sanctions.[46] Such methods highlight the growing intersection between maritime opacity and proliferation financing risk, where weak flag-state governance and limited maritime domain awareness enable sanctioned entities to continue the illicit movement of dual-use commodities and energy resources. The Iranian case demonstrates that, unlike the DPRK, which is geographically constrained, Iran's evasion risk is inherently transnational, with enforcement challenges spanning multiple jurisdictions and flag administrations.>

44 See https://www.opensourcecentre.org/research/red-passage.
45 US Department of the Treasury, 'Treasury Targets Diverse Networks Facilitating Iranian Oil Trade' (Press Release, 25 September 2024)
46 RUSI, 'Countering Shadow Fleet Activity through Flag State Reform' (Insight Paper, 7 October 2024)

Cyber-Enabled Proliferation Financing

Malicious cyber activity is playing an increasingly significant role in generating revenue and foreign currency income for sanctioned states. These revenue streams, in turn, are a crucial artery for the financing of weapons of mass destruction programmes. Criminal cyber activity also serves as a means for information gathering, accessing blueprints and other sensitive data to further proliferation efforts.

According to the final UN Panel of Experts Report (PoE) an estimated 40% of funding for the DPRK's weapons of mass destruction programmes comes from illicit cyber activity.[47] Cyberattacks originating in the DPRK, and undertaken by groups associated with the DPRK, have become infamous. They are thought to be co-ordinated by the Reconnaissance General Bureau, a North Korean intelligence agency, and are perpetrated by advanced persistent threats such as the Lazarus Group, Andariel, and Kimsuky. Their targets have included the defence, aerospace, and crypto industries worldwide.

For example, in 2022, they compromised a Spanish aerospace company via a sophisticated 'spear-phishing' campaign. They are also believed to have orchestrated dozens of cryptocurrency heists, which the PoE estimates may have resulted in the theft of up to $3 billion worth of digital assets between 2017 and 2023. In February 2025, suspected DPRK operatives conducted what is believed to be the biggest theft in digital asset history, stealing $1.5bn from Dubai-based exchange Bybit[48].

The Multilateral Sanctions Monitoring Team (MSMT) further reported that DPRK nationals working abroad in the information technology (IT) sector, often disguised as freelancers or contractors, are a key vector for sanctions evasion.[49] According to the MSMT, these IT workers >

For PF risk specifically, small states and territories should be particularly wary about abuse of their shipping registers, transshipment risks posed, and the conducting of STS transfers in their territorial waters. To avoid flag-state inspections, vessels involved in illicit activity often change their flags ('flag hopping'). Proliferators might target small states and territories' ship registers because of an assumed lack of understanding or resources to monitor them effectively. Collaboration and information-sharing between port authorities, intelligence units, and maritime administrations is critical to ensure a thorough understanding of who and what is transiting territorial waters and transshipment hubs.

"The Multilateral Sanctions Monitoring Team (MSMT) further reported that DPRK nationals working abroad in the information technology (IT) sector, often disguised as freelancers or contractors, are a key vector for sanctions evasion."

47 UN Security Council, *Report of the Panel of Experts established pursuant to Resolution* 1874, S/2024/215 (2024), p. 60
48 Centre for Strategic and International Studies, 'The ByBit Heist and the Future of US Crypto Regulation' (2025). Accessible at https://www.csis.org/analysis/bybit-heist-and-future-us-crypto-regulation.
49 Multilateral Sanctions Monitoring Team (MSMT), *The DPRK's Violation and Evasion of UN Sanctions through Cyber and Information Technology Worker Activities* (2025) p. 4–7.

generate millions of dollars annually by developing software, building blockchain platforms, and managing virtual infrastructure for foreign clients while concealing their DPRK affiliations through falsified documentation and proxy accounts. Payments are frequently received in cryptocurrency, then laundered through multiple digital wallets or layered through intermediaries in third countries before being repatriated to DPRK-controlled entities linked to the weapons programme. The MSMT also notes that DPRK operatives exploit global demand for remote IT services to infiltrate legitimate companies, enabling both financial gain and access to sensitive intellectual property and technological know-how.[50]

By way of example, the EU Commission has set up an internal FinTech TaskForce to assess technological developments, technology-enabled services and business models to identify options to 'harness opportunities or address[ing] possible risks'. Small states and territories may not have the resources or capacity to establish and maintain such specialised task forces, but some forum to help relevant authorities in at-risk jurisdictions maintain knowledge and understanding of cyber-enabled PF may prove useful.[51] The EU`s Digital Operational Resilience Act (DORA) also provides a template for a comprehensive regulatory framework aimed at enhancing the digital operational resilience of financial entities.[52] >

Mitigating the risk of cybercrime requires vigilance, technical literacy, and collaboration between the public and private sectors to ensure at-risk firms are aware of, and prepared for, the threat. Where there are growing cryptocurrency and financial technology (FinTech) sectors, those sectors should be made sufficiently conscious of the risk nexus between their area of economic activity and potential targeting by DPRK-linked hackers. States should consider adopting comprehensive yet flexible regulatory frameworks for ICT-risk management in vulnerable sectors. Precedent demonstrates that any assets stolen may subsequently contribute to DPRK proliferation programmes. Keeping abreast of these developments is critical.

"The MSMT also notes that DPRK operatives exploit global demand for remote IT services to infiltrate legitimate companies, enabling both financial gain and access to sensitive intellectual property and technological know-how."

50 Ibid, p. 8-11.
51 European Commission, https://ec.europa.eu/newsroom/fisma/items/56443/en.
52 Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011

Typologies and Red Flags

PF presents unique challenges related to identifying typologies and red flags. As the number of identified cases is so low, particularly in small states and territories, generic lists, cross-jurisdictional analysis and global case studies are the most appropriate sources to inform bespoke PF national risk assessments. Ensuring relevant authorities are up to date with emerging strategies used by proliferators is a critical goal, and collaboration with international bodies and leading states (including the EU and US) should be sought.

PF is a transnational phenomenon that utilises complex procurement networks, extensive financial networks, and multiple actors to obscure the end-users of illicitly procured dual-use goods and technologies. The ability to abuse conventional financial systems, alongside the emergent virtual asset industry that facilitates instant cross-border transactions, necessitates new methods of detection responsive to the evolving technologies used by proliferators.

Red flags

As with any financial crime, there are red flag indicators that might help members of both the public and private sectors identify when PF might be taking place. Predictably, there is overlap with ML and TF red flags, but it is important to note key distinctions that are more heavily weighted towards PF, including the ultimate perpetrators, their objectives and the consequences of their actions.

Some typical indicators might be less relevant to small states because they have very small or non-existent industrial sectors, but others (including those relating to transshipment, VASP licensing, complex corporate structures and financial regulation) are of greater significance. It is important to recognise that individual indicators may not, in isolation, demonstrate PF activity but may form part of a wider pattern of behaviour when viewed collectively. Analytical integration of multiple red flag (across customers, products, geography, and transactional flows) is therefore critical for effective detection.

Red flags are an imperfect indicator. Many are reactive: they only become evident after illicit activity has taken place and common methods are established. Moreover, the various red flags outlined are often not unique indicators of PF but rather common indicators of 'suspicious activity' (e.g., the use of shell companies, the transshipment of goods through third countries). From the perspective of identifying financial crime this is not an issue, but it could delay identification of the crime as PF-related – this requires extended due diligence, intelligence collection and network tracing.

Some red flags are listed below, subdivided into *customers, products*, and *geography*. This non-exhaustive list seeks to highlight some potential red flags with PF-related vectors.

Customers

- **Parties are involved (directly or indirectly) in the supply, sale, delivery or purchase of dual-use, proliferation-sensitive or military goods.**
- **Parties are physically located in countries of proliferation or diversion (transshipment) concern.**
- **Parties have existing or previous connections or dealings with countries of proliferation concern.** >

" The ability to abuse conventional financial systems, alongside the emergent cryptocurrency industry that facilitates instant cross-border transactions, necessitates new methods of detection responsive to the evolving technologies used by proliferators."

- Parties conduct business inconsistent with their expected activities and/or risk profile.
- Parties are resistant to providing additional information when queried.
- Parties seeking trust or company services in relation to complex, multi-jurisdictional corporate structures in connection with high-risk sectors (e.g. maritime and shipping sectors, military or high-tech sectors).

Products

- Transaction involves dual-use, proliferation-sensitive or military goods.
- Highly technical goods shipped to countries with a seeming inability to use or deploy them.
- Opaque, complex ownership and/or payment structures that obscures the end user/use of dual use or proliferation-sensitive goods.
- Transactions involving correspondent banks with a documented history of facilitating payments for proliferating regimes, high-risk jurisdictions.
- Description of goods on trade/financial documentation is non-specific or misleading, and/or declared value of goods is undervalued compared to shipment cost.
- Licit goods, including luxury goods, shipped to clients in jurisdictions of proliferation concern, where there is likelihood that the ultimate end user is North Korea. Likewise, procurement of goods from DPRK is also a PF risk.

Geography

- Use of jurisdictions with low transparency regarding beneficial ownership of corporate structures.
- Use of jurisdictions with known deficiencies in AML/CFT/CPF controls (e.g., low ratings from Mutual Evaluation).
- Involvement of diplomats from states of proliferation concern in trade-related transactions.
- Use of nationals not linked to a sanctioned country as directors, nominee shareholders, or signatories as a front for designated persons.
- Routing of shipment of goods or transactions inconsistent with normal patterns or expected business activity.
- Routing of shipment of goods or transactions through jurisdictions with weak export control laws or weak enforcement of such laws.
- Transactions involving importers, exporters, agents, or brokers active or based in the border areas of sanctioned countries. For example, the Royal United Services Institute's Project Sandstone has reported cases where shipments of proscribed goods destined for the DPRK were recorded as transiting through border hubs such as Dandong, China, to obscure their true end destination.[53]

Established typologies

A considerable number of established typologies have emerged from the detection and disruption of PF networks. Understanding how actors involved in PF operate and the mechanisms they use to exploit vulnerabilities in global trade and finance facilitates the development of effective countermeasures.

The new FATF report published in 2025 on sanctions evasion schemes outlines four major typologies used by proliferators:

a) Enlisting intermediaries to evade sanctions,
b) Obscuring beneficial ownership information to access the financial systems,
c) Using virtual assets and other technologies,
d) Exploiting the maritime and shipping sectors. [54]

The typologies described below are not comprehensive: sources named above contain exhaustive lists of typologies and a substantive range of case studies. However, those identified here may have heightened relevance for small states and territories:

- Exploitation of weak or non-existent export control regimes/weak enforcement of existing regimes

- Low awareness of PF risks within DNFBPs, such as luxury goods retailers or high-value dealers, which may be exploited for the purchase, transfer, or concealment of dual-use or sanctioned items >

53 RUSI, PROJECT SANDSTONE, *No. 7, The Billion-Dollar Border Town, North Korea's Trade Networks in Dandong (Part 1)*, (2020); also see FATF Report, *Complex Proliferation Financing and Sanctions Evasion Schemes* (2025), pp. 81-85 for a further list of indicators.
54 FATF Report, *Complex Proliferation Financing and Sanctions Evasion Schemes* (2025), p. 5

Jurisdictions lacking sufficient mechanisms to monitor the movement of goods through them might be especially vulnerable to exploitation by PF actors. Ensuring the end-use and end-users of dual-use goods are disclosed and understood is key to preventing them from falling into the hands of bad actors.

- **Geographic proximity and/or trade facilitation capacities (e.g. free trade zone) that allows jurisdiction to be used as transshipment point.**
  Small states and territories, particularly those in strategic maritime locations or with general proximity to states of proliferation concern, are at risk for being targeted by proliferators. This typology, when combined with the previous regarding weak export controls, could pose significant vulnerability to PF activity.

- **A financial sector that provides a high number of financial services in support of international trade**
  Many smaller jurisdictions worldwide have evolved heavily service-based economies, some developing thriving business and finance centres that rival much larger states. To remain competitive, these jurisdictions might have higher risk appetites for forms of international business, which require strong AML/CTF/CPF measures to combat attempts at exploitation. Financial sectors with exposure to international trade are vulnerable to potential PF risks, particularly when customers from high-risk jurisdictions are involved or implicated in vessel ownership, brokering, supplying goods, or the execution of the trade itself.

- **Movement of people and/or funds to or from target jurisdictions/countries of proliferation concern**
  Monitoring financial outflows and inflows to and from target jurisdictions is critical. Sanctions might make such direct transfers difficult or impossible, but relevant authorities across the public-private domain should ensure funds are not being rerouted and beneficial ownership structures are sufficiently transparent. Parallel to this is the movement of people from target jurisdictions, especially Iran and the DPRK, who might seek to use diplomatic immunity or other means to open bank accounts and procure proliferation-sensitive goods.

- **Cyber-heists of VASPs and other digital currency providers (DPRK and Iran)**
  A new favourite tactic of the DPRK, cyber-heists have resulted in billions of dollars' worth of stolen digital currencies. The immediate, transnational nature of cryptocurrencies and digital assets opens the door for abuse by state actors seeking to circumvent international sanctions. Various advanced-persistent threats have been extensively linked to a North Korean nexus, and as digital currencies continue to evolve, small states and territories that are venturing into that economic space must ensure risk assessments respond to the demands of this dynamic sector.

Emerging typologies & risks

As technologies evolve and global patterns of trade, finance, and geopolitics evolve, PF threats rise and fall in relevance. Entirely new means of evading international sanctions emerge: an important task inherent in effectively assessing and mitigating PF risk is keeping one eye on the future. Jurisdictions should future-proof national risk assessment outcomes and ensure that risk classifications are monitored and adjusted as necessary.

The typologies and risks highlighted below have been identified as increasingly prevalent methods of PF:

- **The exploitation and abuse of artificial intelligence (AI)**
  The exploitation and abuse of AI introduce an emerging dimension of concern for PF risk. AI systems are increasingly used to automate sanctions-evasion techniques, including the creation of synthetic identities, falsified trade documents, and even the operation of agentic AI-driven front companies that can autonomously conduct financial transactions, manage digital wallets, and interact with legitimate commercial entities online.[55] These developments significantly expand the typological landscape for PF, particularly as proliferators leverage AI to disguise the >

55 RUSI, *'Beware the Robots: AI-Enabled Sanctions Evasion is Here'* (2024).

identity of DPRK IT workers, generate false corporate data, and obfuscate links to sanctioned entities. The convergence of AI, cyber operations, and digital finance presents an acute challenge: existing AML/CFT frameworks often lack the technological depth to detect automated or self-learning evasion patterns, leaving supervisory and financial intelligence functions exposed to new forms of abuse. Incorporating AI-related typologies into national PF risk assessments is therefore becoming essential to ensure regulators and reporting entities can recognise indicators of algorithmically enabled sanctions-evasion networks.

Related to the spread of new technologies, the rapid evolution in the past several years in generative AI and self-learning technologies will present new threat vectors in relation to PF. AI has been recognised as potentially useful in the fight against illicit finance, but attention should also be paid to the way criminals (and proliferators) could exploit these technologies for malicious ends.

Although not specifically related to PF, reports of fraudsters using Deepfake technology to target international companies including Ferrari, WPP and Arup highlight the ever-increasing sophistication of AI-enabled criminality that could be used by proliferators.[56] Defence companies have already been targeted by cybercriminals, and AI will enhance the sophistication of their attacks.

Small states and territories are advised to ensure that these shifts are recognised in ongoing risk assessment activities

- **Geopolitical changes relating to the war in Ukraine**
  Shifts in geopolitical stability and dynamics dictate the pace and intensity of proliferation efforts, which in turn influence the profile of PF efforts. The ongoing Russian invasion of Ukraine has prompted extensive military collaboration between Russia, Iran, and the DPRK. Trade and defence arrangements between these countries pose a threat to non-proliferation regimes and might motivate nuclear-threshold states like Iran to pursue WMD programmes as international instability increases. As a practical consequence, it has prompted an increased use of jurisdictions in Central Asia and other third-country jurisdictions for trade diversion purposes, allowing countries to circumvent sanctions.

A list of case studies can be found in Annex C.

“Related to the spread of new technologies, the rapid evolution in the past several years in generative AI and self-learning technologies will present new threat vectors in relation to PF. AI has been recognised as potentially useful in the fight against illicit finance, but attention should also be paid to the way criminals (and proliferators) could exploit these technologies for malicious ends.”

56 Ferrari Deepfake Attack Foiled with Simple Question

Mitigating PF risks in Small States and Territories

FATF – Technical Compliance and Effectiveness

To address the rising threat of PF, the FATF established fundamental guidelines, including Immediate Outcome 11 (IO.11), aimed at evaluating the effectiveness of jurisdictions at preventing PF.[57] FATF's IO.11 emphasizes that countries should actively identify, understand, and mitigate PF risks they face. It assesses whether jurisdictions are successful in preventing PF-related breaches and ensuring that financial systems are not misused for these activities. This requires each jurisdiction to apply specific risk-based measures and maintain robust TFS in line with FATF's Recommendation 7 (R.7), which mandates targeted sanctions against those engaged in proliferation activities. IO.11 thus serves as an indicator of a jurisdiction's preparedness to address PF risks by evaluating the practical impact of implemented sanctions and controls.

Among the most significant steps introduced by the FATF is the revision of Recommendation 1 (R.1) and its Interpretive Note (INR.1), which require countries and private sector entities to conduct comprehensive PF risk assessments. R.1 recommends that both financial institutions and designated non-financial businesses and professions (DNFBPs) identify, assess, understand, and mitigate PF risks associated with potential breaches or evasions of TFS obligations. This involves examining factors such as delays in sanction communication, ineffective onboarding processes, insufficient training, and potential evasion tactics by proliferators, including the use of shell companies, front companies, and fraudulent intermediaries. Countries are also expected to establish coordination mechanisms to regularly update and communicate PF risk assessments to relevant authorities, ensuring that all sectors are informed and able to respond to new risks effectively.

> *"R.1 recommends that both financial institutions and designated non-financial businesses and professions (DNFBPs) identify, assess, understand, and mitigate PF risks associated with potential breaches or evasions of TFS obligations."*

R.1 further recommends that countries take a risk-based approach in implementing measures based on their PF risk level. For instance, where higher PF risks are identified, countries should require financial institutions and DNFBPs to introduce enhanced measures, including advanced controls to detect and address possible TFS breaches. This includes enhanced sanctions screening, rigorous customer due diligence, and updated risk management practices. Alternatively, if certain activities or financial sectors demonstrate low PF risks, countries may exempt these entities from some requirements, provided they can justify the low risk and still meet R.7 on targeted financial sanctions.

For financial institutions and DNFBPs specifically, FATF outlines detailed expectations to document, regularly update, and share their PF risk assessments with authorities. They must also establish policies and controls approved by senior management to effectively mitigate >

57 FATF, *Methodology: For Assessing Technical Compliance with the FATF Recommendations and the Effectiveness of AML/CFT/CPF Systems* (2024), p. 165.

PF risks, monitoring the effectiveness of these controls and adapting them as needed. Institutions facing higher PF risks are required to implement stronger, risk-commensurate measures, while those with lower PF risks are allowed to scale their controls accordingly, ensuring that all risk levels are managed in line with TFS obligations. By adhering to these standards, FATF aims to create a globally coordinated effort to prevent the financing of WMD proliferation, especially in jurisdictions where financial activities may be inadvertently leveraged for such purposes.

In summary, small countries must be able to effectively articulate the relevant contextual factors that may expose them to risk, which are the sum of threat factors and vulnerabilities specific to them. Based on these risk factors, jurisdictions, together with the private sector, must have a plan for mitigating or controlling them.

Targeted financial sanctions

Understanding the obligation of jurisdictions to implement and enforce TFS is one of the cornerstones of preventing WMD proliferation. The implementation of TFS is a FATF requirement to comply with UNSC resolutions relating to the 'prevention, suppression and disruption of proliferation of weapons of mass destruction and its financing'.[58] These measures require countries to 'freeze without delay the funds or other assets of, and to ensure that no funds and other assets are made available, directly or indirectly, to or for the benefit of [designated persons or entities]…'[59]

The FATF identifies several factors that may increase the risk of the breach, non-implementation, or evasion of financial sanctions. These include

a) Delay in communication of designations at the national level;
b) Lack of clear obligations on private sector entities;
c) Failure on the part of private sector entities to adopt adequate policies and procedures to address PF risks; and
d) The concerted efforts of designated persons and entities to circumvent TFS through front companies, joint ventures, and middlemen.[60] >

Redressing these risks appears relatively straightforward across jurisdictions. Where jurisdictions lack a central domestic legal authority with oversight of TFS, it may be advisable to consider establishing a forum to ensure that relevant authorities can coordinate the jurisdiction's sanctions policies and share relevant information/intelligence. Ensuring that a jurisdiction has a sufficient legislative basis to penalise those who may be implicated in PF-related TFS evasion is critical, for both dissuading potential facilitators and imposing proportionate penalties.

"Understanding the obligation of jurisdictions to implement and enforce targeted financial sanctions (TFS) is one of the cornerstones of preventing WMD proliferation."

58 FATF, *International Standards on Combating Money-Laundering and the Financing of Terrorism and Proliferation: The FATF Recommendations* (2025), p. 13.
59 Ibid.
60 FATF, *Guidance on Proliferation Financing Risk Assessment and Mitigation* (2021), pp. 3-4.

Additionally, jurisdictions must ensure that mechanisms are in place to facilitate rapid, efficient communication of designations nationally, from the public to the private sector. Such mechanisms may include, but are not limited to, public-private partnerships that facilitate information exchange, integrated IT systems for real-time updates of sanctions screening lists, automated screening of national registries against these lists, and targeted guidance to assist the private sector in developing policies and procedures to manage PF-related risks.

TFS, as the FATF itself acknowledges, possess limitations in the fight against PF: while automatic and manual name-based screening remains a core tool, the 2021 and 2025 FATF documents highlight that screening must be supported by reliable beneficial ownership information, updated identifiers, and intelligence-led risk assessment, a resource-intensive model that places smaller states and territories at a distinct disadvantage may need to be more selective in their allocation of budgets.[61] These challenges persist across the private and public sectors.

Outreach and capacity building

As the preceding chapters made clear, the path towards adopting and implementing a CPF regime requires overcoming challenges such as:

- **defining PF and its scope;**
- **understanding who PF actors are or what the PF activities are that may threaten the jurisdiction, as well as the domestic weaknesses and the contextual factors that may attract PF networks;**
- **strategising a common response through the effective allocation of resources;**
- **adjusting to the evolution of PF threats and the global security landscape; and**
- **risk-based analysis operating outside of strict FATF requirements and emphasizing indirect channels of exposure via intermediaries acting on behalf of proliferators.**

While small states and territories often face challenges in finding expertise and training opportunities in PF or export controls related to proliferation, they frequently exhibit an innovative and nimble approach to capacity-building. There are numerous open-source resources available online that competent authorities can utilise to build their own expertise.[62] Using these resources, jurisdictions can develop their own training materials to help the private and public sectors understand and implement effective safeguards. For instance, one jurisdiction has developed an online 'e-learning' workshop that allows individuals across the public and private sectors to develop and apply their PF knowledge.

While some small states and territories may have the resources and budget to hire international experts or academics to aid in the development of bespoke materials or guidance, others will not. Usefully, many of the resources produced by these experts are available for free and designating at least one staff member as a PF subject-matter-expert can make a significant difference in helping competent authorities and private sector companies understand what is expected of them. >

"There are numerous open-source resources available online that competent authorities can utilise to build their own expertise."

61 FATF, *Guidance on Proliferation Financing Risk Assessment and Mitigation* (2021) p. 4; FATF, *Complex Proliferation Financing and Sanctions Evasion Schemes* (2025) p. 54–55.
62 See the section on 'Useful sources and methodologies' above for a comprehensive list.

Proliferation and PF techniques continue to evolve, presenting challenges for law enforcement and other competent authorities. It is therefore extremely important for investigators to obtain the fundamental knowledge and necessary skills about PF investigations and to continuously receive the latest typologies. More importantly, investigators should be provided with adequate, advanced technological facilities for their use in their daily operations and training opportunities to strengthen their professional investigative capacity.

Domestic coordination and cooperation frameworks

Jurisdictions often face significant challenges in coordinating intelligence efforts to combat PF. Limited channels for information-sharing, few typologies or other PF-specific intelligence, and delays in exchanging intelligence all hinder effective action. Public sector authorities, such as law enforcement, regulatory bodies, port and maritime authorities, and immigration authorities, often manage data collection, interpretation, and storage in isolated ways, which impedes cohesive responses to PF threats.

To enhance coordination and information-sharing, the FATF recommends establishing regular or ad hoc inter-agency meetings involving a diverse range of agencies. Under R.2, countries should have inter-agency frameworks in place to enable policymakers and the relevant competent authorities to cooperate, and where appropriate, coordinate and exchange information domestically with each other concerning the development and implementation of AML/CFT/CPF policies.[63]

These collaborative sessions would enable key stakeholders, including representatives from financial intelligence units, export control authorities, law enforcement agencies, supervisory authorities, and policy entities, to systematically address and mitigate PF risks. By pooling expertise and aligning strategies, these meetings help ensure a cohesive approach to monitoring threats, developing policies, and coordinating enforcement efforts. Key areas of focus within these meetings could include the following:

- **Monitoring and analysing risks, threats, new trends, and vulnerabilities in the counter-financing of proliferation (CFP) regime.**
- **Recommending appropriate responses for competent agencies to counter the financing of proliferation.**
- **Identifying key intelligence gaps related to the financing of proliferation and proposing solutions to close those gaps.**
- **Considering potential interdiction opportunities to impede proliferation financing and coordinating such actions.**
- **Coordinating and de-conflicting activities of competent agencies, including financial, intelligence, and law enforcement agencies.**
- **Coordinating investigations into export control violations and enforcing laws related to the export and transshipment of controlled dual-use goods, particularly to sanctioned countries. This should include oversight of licit trade where there is a risk that the end user is the DPRK and/or the local procurer is sourcing from the DPRK.**
- **Reviewing mechanisms to ensure that Suspicious Transaction Reports (STRs) are thoroughly analysed and meet sanctions requirements, aiding in the detection and prevention of PF.**
- **Coordinating (ad hoc) responses to relevant geopolitical developments that may significantly alter the threat landscape of the jurisdiction.**

Designating one or more authorities or establishing a coordination or other mechanism responsible for setting national CPF policies and ensuring co-operation and co-ordination among all relevant agencies makes the establishment of an inter-agency framework crucial for >

63FATF, *Methodology: For Assessing Technical Compliance with the FATF Recommendations and the Effectiveness of AML/CFT/CPF Systems* (2024), p. 33.

an effective CPF regime. Consideration should be given to the composition of these interagency mechanisms, particularly the export control, sanctions, and wider WMD non-proliferation dimensions. In fact, some jurisdictions permit relevant agencies within the counterproliferation and export control systems to use classified intelligence to manage export and customs controls without disclosing the origin or content of the information, thereby enabling targeted action without risking information exposure. Such a group could improve coordination by enhancing the response time and accuracy of information exchange, building each authority's capacity to collaborate against PF threats.

Establishing a joint intelligence working group focused on PF could help address these limitations, allowing public sector authorities such as financial intelligence units, intelligence and law enforcement agencies, regulatory bodies, and port and maritime authorities to streamline information-sharing and better integrate their resources.

For example, one jurisdiction established a Joint Coordinating Intelligence Group to Counter Proliferation Financing, (JCIG), a strategic group designed to facilitate cross-disciplinary information-sharing related to the financing of weapons of mass destruction. By exchanging intelligence on suspected proliferators, networks, vessels, sanctioned entities, and other assets, the JCIG facilitates strategic coordination to detect, prevent, and disrupt proliferation activities. It strengthens understandings of PF, the relevant UN Security Council Resolutions, and TFS, while promoting awareness of PF risks and reporting processes among competent authorities and the private sector. Including Customs officials in this mechanism allows opportunities to discuss export control measures and the management of dual-use goods transit, making it a proactive model in PF intelligence cooperation and coordination.

Another jurisdiction set up a working group composed of its Sanctions Monitoring Board, the Office of the Attorney General, FIU, Police Force, Financial Services Authority, Business Registry, Security Service, Customs, Trade Licensing Unit, Freeport terminal, the Gaming Authority and National Coordinating Committee in Combatting ML and TF. This group drew from cases investigated (and enforcement cases) to establish a list of target jurisdictions.

This interagency approach to PF controls can further strengthen coordination by bridging gaps between the counter proliferation financing and export control frameworks. Developing standard operating procedures for routine information-sharing on importers and exporters of sensitive goods, suspicious entities, and technical specifications of dual-use goods could create preventive PF risk management. >

Additionally, regular joint training sessions could improve mutual understanding between financial crime prevention and export control experts, allowing both groups to better navigate the challenges of PF risks. By enhancing cross-training efforts led by governments, international bodies, and private firms specialising in sanctions compliance, jurisdictions can build a comprehensive PF response system that integrates expertise across agencies, industries, and regions.

" This interagency approach to PF controls can further strengthen coordination by bridging gaps between the counter proliferation financing and export control frameworks."

Public-private partnerships

The private sector plays a key role in preventing PF. Banks and gatekeepers are not the only businesses exposed to PF networks. Other economic sectors involved in WMD procurement schemes are also at risk: strategic goods manufacturers, operators in the maritime industry, insurance companies, the defence sector, money or value transfer services, and VASPs. DNFBPs remain a critical gap in PF compliance globally, with their awareness of international obligations and required controls at a substantially lower level. As a first line of defence, the private sector should be the first to detect suspicious activities and trigger further investigations.

Following the inter-agency mechanism, a second dimension of CPF cooperation is represented by the contributions that the public and private sectors can provide to one another. Private sector entities report suspicious activities or transactions, share analysis on trends, and inform the supervisory authorities of their risk assessments; at the same time, the authorities, with the support of the relevant agencies, assist the private sector by providing training, guidance, best practices, and any information useful to direct the private sector's CPF efforts.

Given that traditional financial institutions alone may not capture the full spectrum of PF risks, partnerships need to expand to include a wider range of stakeholders, including (but not limited to) VASPs, maritime, trade and logistics sectors, and universities. An inclusive approach ensures a more comprehensive understanding of PF risks and improves the ability to detect emerging methods that proliferators may exploit. Jurisdictions that have well-established PPPs can serve as valuable models, offering best practices and engaging in reciprocal learning that strengthens understanding of responsibilities across the public-private divide.

"Jurisdictions that have well-established PPPs can serve as valuable models, offering best practices and engaging in reciprocal learning that strengthens understanding of responsibilities across the public-private divide."

International co-operation and collaboration

Understanding and disrupting the financing of proliferation requires strong international cooperation and the use of analytical tools that enhance financial transparency. Mechanisms such as centralised bank account registries allow for rapid access to account ownership and financial >

In the context of PF, establishing a public-private partnership (PPP) can greatly enhance collaboration between the state and the private sector, using expertise and data to strengthen PF countermeasures. As jurisdictions increasingly rely on the private sector to support AML and CFP frameworks, it becomes crucial to create legal frameworks that define the conditions for accessing PF-related information and expertise. This framework should set clear guidelines for data access and exchange while safeguarding data protection and privacy rights.

linkages, supporting timely tracing of funds connected to proliferation networks. Expanding this collaborative spirit beyond national boundaries, small states and territories can benefit greatly from engaging internationally and sharing expertise with peers.

The STWG, which contributed data and insights to this guidance paper, exemplifies this approach, an informal operational network that promotes the exchange of ideas, best practices, and collective problem-solving. Regional working groups like the STWG can help address shared challenges, particularly for jurisdictions with limited resources or expertise in PF, while fostering mutual support in meeting international obligations. As financial crime and proliferation financing are increasingly transnational, cultivating partnerships and information-sharing channels overseas ensures that all jurisdictions, regardless of size, are better equipped to detect, understand, and disrupt cross-border PF activities.

Collecting data to understand risk exposure

Jurisdictions should continuously strengthen their data foundations to better understand and mitigate PF risks. Effective data collection and analysis are central to evidence-based policymaking, enabling authorities to identify vulnerabilities, assess exposure, and design proportionate mitigation measures. The broader and more comprehensive a jurisdiction's data collection on PF-relevant areas, the deeper its understanding of associated risks will be. Questionnaire responses from STWG participants highlight the importance, and indeed the necessity of monitoring the materiality of financial flows to and from high-risk jurisdictions. It is further worth emphasizing that due to the inherently transnational nature of PF risk, countries cannot rely solely on internal data to achieve relevant risk assessments. Cross-jurisdictional analysis and indirect exposure through links with jurisdictions of proliferation concern must be factored in to achieve a proper understanding of risk.

While landlocked states may not need to monitor vessel movements, those maintaining ship registries must ensure robust due diligence on vessels flying their flag. For small states and territories, data-driven decision-making is particularly valuable, allowing limited resources to be used efficiently while enhancing operational effectiveness. Mapping and assessing available data sources, identifying information gaps, and integrating findings across agencies are essential to improving the overall quality of intelligence and policy outcomes.

The RUSI Proliferation Financing Rapid Risk Assessment Tool provides a practical framework for structuring these efforts, guiding jurisdictions through the systematic identification and assessment of PF threats across social, economic, geographic, and institutional contexts. Complementing this, RUSI's 2019 Guide outlines key primary data sources (can be found in Annex 1 of the document), which have been adapted in this paper to reflect the specific circumstances and requirements of small states and territories. >

" For small states and territories, data-driven decision-making is particularly valuable, allowing limited resources to be used efficiently while enhancing operational effectiveness."

Table 2 – Sources of information for data collection related to PF. [64]

Information source	Stakeholder	Type of information
Financial intelligence data and reports	Financial intelligence units	Details on financial networks and patterns of behaviour used by proliferators, including STRs, international transaction reports, and intelligence analysis products
Designations and sanctions listings	Departments of foreign affairs, sanctions units and/or relevant competent authorities, UN and EU listings	Details on sanctioned entities, sanctions-related reports and enforcement actions
Criminal investigation and prosecution records, civil investigation and litigation records	Courts, law enforcement agencies, other competent authorities with investigative powers	Details on past cases involving illicit financial networks; potential patterns of behaviour used by proliferators
Economic, financial, and trade reports	Department(s) of finance, economic development, trade, industry; financial services commissions and regulatory agencies	Data and statistics about the size of the economy and financial sector, size and activities of specific sectors, trade relationships with other countries
Export/import documents and bills of lading	Port authority, customs and borders agency, department of trade, shipping companies, trade finance providers	Import and export data, data on size and nature of trade relationships and patterns, transport and transit routes
Immigration and employment records	Customs and border agencies, departments of employment, labour	Data on migrant labour, individuals in jurisdiction with passports from countries of concern, student records
Vessel management and ownership and inspection records	Maritime and port authorities, flag registry operators, beneficial ownership registry	Information on nature and size of foreign and national vessel activity
Formal and informal information sharing partnerships	Financial institutions, insurance providers, industry associates, DNFBPs, government stakeholders	Information on private sector practices, which will aid in understanding challenges related to implementing CPF obligations
Open source intelligence	Third party providers of reports into proliferation activities (groups of likeminded states, NPOs, research centres)	Information on latest case studies, emerging typologies and risk exposure areas.

Collecting a range of information – from the number and value of financial transactions with links to target jurisdictions, the presence and volume of dual-use goods transiting the jurisdiction, to the number of individuals taking higher education courses in proliferation-sensitive subjects – allows a complete picture to be built regarding the threats, vulnerabilities, and consequences faced by the jurisdiction. This can be a resource-intensive process that requires regular updating, but it imparts considerable value for risk assessments.

64 Joshi, Anagha, Dall, Emil, and Dolzikova, Darya, RUSI, *Guide to Conducting a National Proliferation Financing Risk Assessment* (2019), pp. 41-42.

Conclusion

PF remains a complex and evolving threat that demands continuous vigilance and adaptation. While small states and territories may have different exposure compared to larger economies, their openness, financial or maritime sectors make them inherently susceptible to exploitation by proliferation networks. This research highlights that building resilience against PF requires more than compliance with international obligations. It necessitates sustained commitment to understanding national vulnerabilities, enhancing inter-agency and cross-sector collaboration, and embedding a risk-based, data-driven approach across all components of a jurisdiction's counter-proliferation financing framework.

In addition, small states and territories that operate in close geographic, economic, or regulatory proximity to larger neighbours must recognise that their exposure to PF risk is influenced not only by their own controls but also by the vulnerabilities of surrounding systems. Strengthening cross-border coordination, information exchange, and joint analytical work with regional partners is therefore essential. Incorporating regional dynamics into national risk assessments allows smaller states and territories to "learn their surroundings," i.e., understanding how neighbouring markets, customs regimes, and financial flows may create indirect PF risks that transcend borders. By building structured mechanisms for cooperation with larger counterparts, small states and territories can anticipate and mitigate threats that might otherwise exploit jurisdictional seams in enforcement and supervision.

The fight against financial crime is continuous and constantly changing. PF, as a dimension of illicit finance, is particularly complex due to the multitude of actors (from states to individuals), countries, and sectors that can be implicated. This concluding section summarises key actionable steps that small states and territories can take to assess and mitigate PF risk.

"Communication is key at all levels. Developing inter-agency groups domestically that will facilitate the rapid exchange of PF-related intelligence is crucial for prevention and enforcement measures."

Consult broadly, develop expertise

Competent authorities, FIUs, LEAs, and other relevant government bodies should ensure that they possess a sufficient level of knowledge and understanding regarding PF. There is an abundance of material, provided by the FATF and institutions like RUSI, that can ensure relevant staff members are fluent in the origin, signs, and purposes of PF. This knowledge should serve as the building blocks for national PF risk assessments and is critical to implementing effective CPF regimes. It ensures that properly designed legal frameworks are developed, targeted local guidance is produced and issued to instruct and reassure the private sector, and SARs can be submitted and analysed to an appropriate standard.

Communication is key at all levels. Developing inter-agency groups domestically to facilitate the rapid exchange of PF-related intelligence is crucial to prevention and enforcement measures. Building bridges between the private and public sectors will further understanding of mutual roles and responsibilities. Staying up to date with changing international typologies, learning from partners in other jurisdictions, and understanding the consequences of geopolitical shifts on proliferation activities are also >

key tasks facing jurisdictions in their fight against PF. Developing training materials and workshops is one option for competent authorities to disseminate this knowledge to relevant stakeholders.

Understand threats, vulnerabilities, and consequences

Small states and territories present distinct challenges for PF. Guidance from the FATF and RUSI is comprehensive and provides the foundation for understanding the forms threats and vulnerabilities might take. To ensure a thorough review of PF risks, however, jurisdictions must also be aware of the characteristics that set them apart from others. Best practices are universally applicable, but small states and territories must remain aware that, even if existing typologies do not appear immediately relevant to their economic activity, proliferators will always seek to evolve and exploit new operational or regulatory gaps. IFCs and maritime centres should be particularly conscious of their unique risks.

Constructing a robust framework aligned with the assessed level of risk that allows different stakeholders to understand their role in preventing and combating PF is essential.

Implement export controls and monitoring systems

For jurisdictions that maintain transit hubs for goods, whether over land or by sea, strong monitoring systems are necessary to understand what is passing through the jurisdiction.

Relevant competent authorities should ensure that comprehensive lists of dual-use goods and services are screened against manifests and cargo lists, that MECRs are consulted and incorporated into checks, and that red flags for common evasion techniques (such as falsifying shipping codes) are well understood. Fundamental to this task is ensuring that staff are adequately trained and equipped to identify and monitor PF-related risks.

Implement import controls and due diligence measures

Effective control of imports is essential to prevent sanctioned or proliferation-sensitive goods from entering a jurisdiction, particularly those linked to DPRK procurement networks. Competent authorities should ensure that import documentation, shipping routes, and supplier information are verified against updated sanctions lists, dual-use control schedules, and known typologies of DPRK-linked front companies. Close collaboration between customs, financial intelligence, and supervisory bodies is critical to detect re-routed consignments, false country-of-origin declarations, or third-country intermediaries that disguise DPRK involvement. Incorporating financial intelligence into customs screening, maintaining automated risk-profiling systems, and participating in regional information exchanges can enhance visibility over high-risk supply >

“Constructing a robust framework aligned with the assessed level of risk that allows different stakeholders to understand their role in preventing and combating PF is essential.”

chains. Regularly updated watchlists, targeted training for customs and border officers, and awareness-raising among freight forwarders and import agents will further strengthen a jurisdiction's ability to identify and intercept proliferation-related imports.

Engage in outreach and collaboration

The private sector is the frontline of defence in the fight against financial crime, including PF. Public authorities can be experts, but if financial institutions, DNFBPs, and affected sectors do not understand the risks and concomitant responsibilities they possess, the mitigation framework will be ineffective. Public-private partnerships are a good first step for bringing stakeholders together and identifying where threats and vulnerabilities in private sector firms, regulations, and laws are most pressing. Maintaining these links enhances a jurisdiction's ability to respond quickly and effectively to counter instances of PF.

Future-proof: cybersecurity and geopolitics

The world is a volatile place, especially for small states and territories, whose prosperity and well-being are often dependent on international stability. Staying informed about current affairs, particularly as they may impact proliferation financing risks, will help jurisdictions anticipate emerging trends. The war in Ukraine has reignited the urgency of preventing the growing connections between Russia, Iran, and the DPRK from translating into material progress for nuclear capabilities.

A prominent evolving trend remains the threats posed by DPRK-linked cybercriminal groups to VASPs and other cryptocurrency providers. As a rapidly evolving industry, unevenly regulated internationally and offering high levels of anonymity, it will likely remain an attractive option for proliferators seeking to raise funds. Governments and firms must work together to defend against any such nefarious attempts.

Beyond these immediate risks, the emergence of AI is introducing a new frontier of concern in PF. AI systems are increasingly being exploited to automate sanctions evasion, generate synthetic corporate and personal identities, and even establish agentic AI-driven front companies capable of interacting autonomously with financial institutions and online service providers.[65] Such tools may enable DPRK-linked actors and other proliferators to conduct transactions, open accounts, or manipulate compliance systems at a scale and sophistication previously unattainable.

The combination of AI and digital assets, therefore, presents a dual-use risk in itself: while AI offers potential for better monitoring and compliance, it also enhances illicit networks' capacity to conceal their activities. To mitigate this, both public and private sectors should prioritise AI literacy within their financial-crime compliance frameworks, ensure regulatory sandboxes incorporate PF risk considerations, and integrate AI-related typologies into national risk assessments.

"The war in Ukraine has reignited the urgency of preventing the growing connections between Russia, Iran, and the DPRK from translating into material progress for nuclear capabilities."

65 *RUSI, 'Beware the Robots: AI-Enabled Sanctions Evasion is Here' (2024).*

References

Arnold, Aaron and Salisbury, Daniel, 'Guide to Conducting a National Proliferation Financing Risk Assessment', *RUSI Special Resources* (2024).

Bloxberg, David, Ferrari Deepfake Attack Foiled with Simple Question | Inspired eLearning Blog (2024).

Brewer, Jonathan, 'Study of Typologies of Financing of WMD Proliferation: Final Report', *Project Alpha: King's College London* (2017).

Bulletin of Atomic Scientists, 'What If Iran Withdraws from the NPT?', What if Iran withdraws from the NPT? - Bulletin of the Atomic Scientists (2025).

Byrne, James, Byrne, Joe, Somerville, Gary and Macdonald, Hamish, "Project Sandstone, No. 7, The Billion-Dollar Border Town, North Korea's Trade Networks in Dandong (Part 1)",: RUSI (2020).

Centre for Strategic and International Studies, 'The ByBit Heist and the Future of US Crypto Regulation' (2025). Accessible at https://www.csis.org/analysis/bybit-heist-and-future-us-crypto-regulation.

Centre for Strategic and International Studies (CSIS), 'The New Russia-North Korea Security Alliance', (2024). Accessible at [https://www.csis.org/analysis/new-russia-north-korea-security-alliance]

Dall, Emil and Keatinge, Tom, 'Assessing the Global Response to Proliferation Financing: *An Analysis of FATF Mutual Evaluation Data', RUSI Occasional Paper* (2021).

Erol, Eda and Spector, Leonard, 'Chinpo Shipping: A Singaporean Financial Agent of North Korea', *CNS Occasional Paper #35* (2017).

European Commission, 'Task Force on Financial Technology' https://ec.europa.eu/newsroom/fisma/items/56443/en.

FATF, *Combating Proliferation Financing: A Status Report on Policy Development and Consultation* (2010).

FATF, *Guidance on Proliferation Financing Risk Assessment and Mitigation* (2021).

FATF, *International Standards on Combating Money-Laundering and the Financing of Terrorism and Proliferation: The FATF Recommendations* (2025).

FATF, Methodology: For Assessing Technical Compliance with the FATF Recommendations and the Effectiveness of AML/CFT/CPF Systems (2024).

FATF, *Proliferation Financing Report* (2008).

GFSC and GFIU, Counter Proliferation Financing: Guidance Notes (2020).

Government of Jersey, *National Risk Assessment: Proliferation Financing* (2025).

Joshi, Anagha, Dall, Emil, and Dolzikova, Darya, RUSI, *Guide to Conducting a National Proliferation Financing Risk Assessment* (2019).

Karnitschnig, Matthew, Iran in secret talks with China, Russia to acquire sanctioned missile fuel – POLITICO (2023).

Kassenova, Togzhan and Early, Bryan, 'Countering the Challenges of Proliferation Financing', *The Centre for Policy Research: University at Albany* (2023).

Long, Tom, *A Small State's Guide to Influence in World Politics* (Oxford: Oxford University Press, 2022).

Margolin, Jack and Bukharin, Irina, 'Trick of the Trade: South Asia's Illicit Nuclear Supply Chain', *C4ADS* (2020). >

Multilateral Sanctions Monitoring Team, *Unlawful Military Co-operation including Arms Transfers between North Korea and Russia*, MSMT vol. 1 (2025).

Open Source Centre, 'Red Passage: Russian-DPRK Munitions Carrier Seeks to Transit the Suez' (2025), https://www.opensourcecentre.org/research/red-passage.

Pawlus, Wojciech, '*Russia is Now Actively Funding North Korea's Nuclear Programme*', RUSI Commentary (2025), https://www.rusi.org/explore-our-research/publications/commentary/russia-now-actively-funding-north-koreas-nuclear-programme.

Salisbury, Daniel, 'Exploring the Use of "Third Countries" in Proliferation Networks: the case of Malaysia', *European Journal of International Security*, vol. 4:1 (2019), pp. 101-122.

Salisbury, Daniel, 'From Missions to Missiles: The Role of North Korea's Diplomatic Corps in Sanctions-Busting', *RUSI Emerging Insights* (2022).

Salisbury, Daniel, 'Shopping for Mass Destruction: North Korea's Illicit Procurement Networks', *RUSI Occasional Paper* (2024).

També, Noémi, *Institutional Proliferation Finance Risk Assessment Guide*, *RUSI Special Resource* (2023).

The Sentry, *Overt Affairs: How North Korean Businessmen Busted Sanctions in the Democratic Republic of the Congo* (2020).

The White House, 'National Security Presidential Memorandum/NSPM-2' (2025), https://www.whitehouse.gov/presidential-actions/2025/02/national-security-presidential-memorandum-nspm-2/

UN Security Council, *Reports of the Panel of Experts established pursuant to Resolution 1874*.

US Department of the Treasury, 'Treasury Targets Network Linked to Iran' (2014), https://home.treasury.gov/news/press-releases/jl2287.

US Institute of Peace, The Coming Iranian Nuclear Challenge in 2025 | The Iran Primer (2025).

Annex A – Full List of Survey Questions

Section 1 – Existing PF national risk assessment

No	Question
1	**Has your jurisdiction undertaken/publicised a PF national risk assessment, and if so when was it last updated?** *NB: If your PF national risk assessment has been publicised, please include a hyperlink to the publication.*
2	**What primary sources of information (e.g. FATF guidance, UN Panel of Expert Reports, etc) were used to facilitate the assessment?**
3	**What secondary sources of information (e.g. academic articles, conferences, etc) were used to facilitate the assessment?** *NB: This can include Risk Assessment models used by other jurisdictions.*
4	**What jurisdictions were identified as "Target Jurisdictions" for the purposes of the assessment?** If you do **not** want to share this list, please explain why. *NB: For the purposes of this assessment, a "Target Jurisdiction" is a jurisdiction that presents a higher risk of proliferation or which has a strong geographical, political, strategic, trade or other link with such a country.*
5	**What methodology and/or resources were applied to determine the list of Target Jurisdictions?**
6	**Does your assessment consider the risks of cyber-enabled PF (ransomware attacks, VASP hacking)? If not, is there a separate assessment that addresses the cybersecurity threats and vulnerabilities faced by your jurisdiction?** *NB: If your jurisdiction has undertaken/publicised a separate cybersecurity assessment, please include a hyperlink to the publication.*

Section 2 – Regulated financial institutions & DNFBPs

Jurisdictions were required to confirm the following in respect of each of the below data points:

a) *Do you currently collect this data point?*
b) *Was this data point considered within your PF NRA?*
c) *Did you encounter any challenges in relation to the collection of this data?*
d) *Would you collect this data point again for another PF NRA?*
e) *What would you do differently?* >

No	Data Point
1	**Number of financial transactions to or from a Target Jurisdiction.**
2	**Value of financial transactions to or from a Target Jurisdiction.**
3	**Number of individual customers resident in a Target Jurisdiction.**
4	**Number of individual customers with nationality of a Target Jurisdiction.**
5	**Number of corporate customers registered in a Target Jurisdiction.**
6	**Number of corporate customers active in a Target Jurisdiction.**
7	**Value of banking deposits held in relation to customers based/active or resident/registered within a Target Jurisdiction.**
8	**Correspondent banking relationships held in relation to Target Jurisdictions.**
9	**Number of customers serviced by Trust & Company Service Providers ("TCSPs") associated with:** **a) Commercial shipping or aviation services; b) Maritime services;** **c) The manufacturing, handling, processing or transiting of dual-use goods; and** **d) The manufacturing, handling, processing or transiting of weaponry (or their components).** *Please provide answers for a) through d) separately.*
10	**Value of exposure between authorised VASPs and virtual asset tumbling/mixing services.** *NB: This exposure is typically identified by way of blockchain analytics tools*
11	**Value of exposure between authorised VASPs and known wallet addresses associated with cybercrime.** *NB: This exposure is typically identified by way of blockchain analytics tools.*
12	**Number of Suspicious Activity Reports submitted in relation to PF.**

Section 3 – Legal Persons & Arrangements

Jurisdictions were required to confirm the following in respect of each of the below data points:

a) *Do you currently collect this data point?*
b) *Was this data point considered within your PF NRA?*
c) *Did you encounter any challenges in relation to the collection of this data?*
d) *Would you collect this data point again for another PF NRA?*
e) *What would you do differently?*

No	Data Point
1	Number of domestic legal persons or arrangements which are active in a Target Jurisdiction.
2	Number of domestic legal persons or arrangements whose ultimate beneficial owners are resident in a Target Jurisdiction.
3	Number of domestic legal persons or arrangements whose ultimate beneficial owners are national of a Target Jurisdiction.

Section 4 – Immigration, Export Controls & Maritime/Shipping Services

Jurisdictions were required to confirm the following in respect of each of the below data points:

a) *Do you currently collect this data point?*
b) *Was this data point considered within your PF NRA?*
c) *Did you encounter any challenges in relation to the collection of this data?*
d) *Would you collect this data point again for another PF NRA?*
e) *What would you do differently?*

No	Data Point
1	Number of individuals entering your jurisdiction who are residents or nationals of a Target Jurisdiction.
2	Number of individuals undertaking higher education courses in the energy sector, nuclear science, nuclear engineering, cyber sector, and/or crypto in your jurisdiction who are residents or nationals of a Target Jurisdiction. NB: This can include students on e.g. vocational courses, exchange programmes, apprenticeships, and undergraduate and postgraduate degrees.
3	Volume of goods exported from or imported to a Target Jurisdiction.

No	Data Point
4	Volume of restricted goods (e.g. military, luxury items) exported from or imported to a Target Jurisdiction.
5	Volume of dual-use goods imported to or exported from your jurisdiction.
6	Number of bunkering operations conducted for vessels registered in a Target Jurisdiction.
7	Number of bunkering operations conducted for vessels involved in the transshipment of goods to/from a Target Jurisdiction.
8	Number of bunkering operations conducted for vessels involved in the transshipment of dual-use goods.
9	Number of transit vehicles entering your jurisdiction on route to/from a Target Jurisdiction.
10	Number of transit vehicles entering your jurisdiction involved in the transshipment of restricted or dual-use goods.
11	Number of transit vehicles entering your jurisdiction involved in the transshipment of restricted or dual-use goods.

Section 5 – Comparative Jurisdictional Analysis

No	Question
1	Please list the primary sectors/services that contribute to your jusridiction's economy, together with an approximation of the proportion of GDP that they contribute.
2a	Please list your most materially significant regulated financial sectors (including both FIs & DNFBPs). Within your response, please include: a) The number of authorised entities within each sector; and *NB: This response should disregard the level of PF risk posed by those particular sectors/services.*
2b	b) Value metrics demonstrating the scale of each sector's materiality (e.g. assets under management, deposits, number of customers, etc.). *NB: This response should disregard the level of PF risk posed by those particular sectors/services.*

No	Question
3	**Please list your highest risk sectors for PF purposes, together with any additional areas of risk identified.** *NB: Where relevant, this response should not be limited to regulated FIs & DNFBPs.*
4	**Number of Suspicious Activity Reports submitted in relation to PF, per reporting sector from 2022 to date.**
5	**Number of investigations, prosecutions and asset seizures related to PF from 2022 to date.**
6	**What are the primary typologies identified in respect of those PF-related SARs/investigations?**
7	**Does your jurisdiction have a VASP registration/licencing regime?**
8	**Number of VASPs operating in or from your jurisdiction.**
9	**Please include value metrics to contextualise the scale of your VASP sector (e.g. assets under management, transactional volumes, etc.).**
10	**Number of TCSPs operating in or from your jurisdiction.**
11	**Please include value metrics to contextualise the scale of your TCSP sector (e.g. number of companies and trusts under management, assets under management, etc.).**
12	**Number of general insurers operating in or from your jurisdiction involved in the provision of commercial shipping or aviation insurance.**
13	**Please include value metrics to contextualise the scale of your commercial shipping/aviation insurance sector (e.g. gross written premiums).**
14	**Does your jurisdiction have export control and/or trade sanctions licensing? If so, how many licenses have been a) applied for b) granted?**
15	**How does your jurisdiction screen against dual-use goods?**
16	**How do your jurisdiction's constitutional arrangements influence its ability to unilaterally develop and implement mechanisms relating to proliferation financing?**
17	**Does your jurisdiction maintain or host any diplomatic links to identified Target Jurisdictions?**

Annex B – Resources for Understanding and Managing PF Risks

FATF Guidance on Counter Proliferation Financing (2018)	Guidance document provided by the FATF that addresses TFS, inter-agency co-operation, and the supervision and monitoring of compliance.
FATF Guidance on Proliferation Financing Risk Assessment and Mitigation (2021)	Guidance document provided by the FATF focusing on the assessment and mitigation of PF risk.
FATF Proliferation Financing Report (2008)	FATF report that is particularly useful for its distinction between witting/unwitting actors and its compilation of case studies (up to 2008).
FATF Combating Proliferation Financing: A Status Report on Policy Development and Consultation (2010)	FATF report that is particularly useful for its legal commentary on PF, description of TFS efforts, and reporting responsibilities and channels for financial institutions.
FATF Report, Complex Proliferation Financing and Sanctions Evasion Schemes (2025)	Updated FATF report on the state of proliferation financing in 2025, the evasion of sanctions related to PF, and good practices in mitigating risk. Contains updated typologies compiled from the contributions of various states.
Study of Typologies of Financing of WMD Proliferation – Project Alpha (2017)	Final report produced by the Project Alpha team at King's College London, headed by Dr. Jonathan Brewer (former Acting Coordinator for UN PoE). Contains arguably the most comprehensive list of PF-related case studies (up to 2017).
Reports of the UN Security Council Committee established pursuant to resolution 1718 (2010-2024)	Reports produced by a UN Panel of Experts, which comprehensively detail the nuclear proliferation activities of the DPRK. Last and final report dated to March 2024, but remains highly relevant for examples of sanctions-evasion.
RUSI Institutional Proliferation Finance Risk Assessment Guide (2023)	Guidance paper produced by Dr. Noémi També at RUSI, focusing on the role of the private sector in PF. Also contains useful distinction between ML/TF/PF.
RUSI Guide to Conducting a National Proliferation Financing Risk Assessment (2024)	Guidance paper produced by Dr. Aaron Arnold and Dr. Daniel Salisbury at RUSI, focusing on PF risk, emerging trends, and frameworks for assessing threats and vulnerabilities.
United States National Proliferation Financing Risk Assessment (2024)	US PF NRA, cited by several participating jurisdictions as a useful example for other countries.
Unlawful Military Co-operation including Arms Transfers between North Korea and Russia, 1st MSMT Report (2025)	First report of the MSMT, a collective established after the end of the UN PoE in 2024 to continue monitoring the effectiveness of the DPRK sanctions regime.
The DPRK's Violation and Evasion of UN Sanctions through Cyber and Information Technology Worker Activities, 2nd MSMT Report (2025)	Second report of the MSMT, a collective established after the end of the UN PoE in 2024 to continue monitoring the effectiveness of the DPRK sanctions regime.

Annex C — Case Studies

Relevant case studies

To shed light on the actual forms that PF takes, several case studies that small states and territories may find instructive have been included below. Data analysed from participants of the STWG revealed that a number of PF-related SARs were submitted in the reporting period since 2022 across all jurisdictions, excluding several related to TFS evasion. Developing relevant typologies specific to these jurisdictions is often reliant on external examples. The involvement of IFCs and small states and territories in these cases is indicative of the strategies employed by malicious actors.

1.Korea Kwangson Banking Corporation (DPRK)

Between 2009 and 2015, a designated DPRK bank maintained financial operations using a Chinese trading company, with transactions totalling approximately $110m. Korea Kwangson Banking Corporation (KKBC) was designated by OFAC in 2009 for providing financial services in support of the DPRK's WMD and ballistic missile programmes. KKBC collaborated with Dandong Hongxiang Industrial Development Co., Ltd (DHID), a trading company based in Dandong, China, on the border with North Korea, to facilitate transactions funded by and/or guaranteed by KKBC.

At one stage, DHID accounted for over 20% of China's trade with the DPRK. Four companies in the British Virgin Islands and one in Anguilla acted as front companies facilitating this activity (in addition to companies in Hong Kong, the United Kingdom, and the Seychelles). The reputation of most of these jurisdictions as financial centres was clearly a factor in their exploitation for PF, demonstrating the underlying risk faced by both small and large IFCs.[66]

2. Procurement from EU suppliers by BVI-registered broker (Iran)

An Iranian-European national acted as a broker for a suspected procurement network from 2009 onwards. Registered in the British Virgin Islands, they operated through a front company that could be linked to at least one Iranian entity. The front company had bank accounts in Dubai and a Balkan EU member.

Funds would be transferred from the Dubai branch of an Iranian bank to the account of the front company in Dubai, after which the funds would be transferred to suppliers in Luxembourg. Iranian customers holding bank accounts in Luxembourg also wired money to the European account of the broker. Although no dual-use goods were found to be involved, the vulnerability was identified as a potential route for PF. Enhanced customer due diligence procedures when assessing clients from high-risk jurisdictions may have enabled earlier detection of the origin of funds.[67]

3.Procurement network based on the control of a bank (Iran)

JSC Investbank was established in Georgia in 2003 and was reorganised in 2011 to appoint three Iranian citizens as 70% shareholders, although they were not listed in the Bank's statutes. The three Iranians were designated by the US Department of the Treasury in 2014, as it was established that the Bank was partly funding a PF procurement network via various front companies. The Bank used a foundation to exploit direct correspondent ties to other international financial institutions. The designated persons then used the Bank to facilitate transactions worth the equivalent of 'tens of millions of US dollars for multiple designated Iranian banks'. In this instance, the geographic proximity of Georgia to Iran and the use of a small-state finance centre to facilitate sanctions evasion highlight the persisting risk profile facing these centres.[68] >

66 Brewer, Jonathan, 'Study of Typologies of Financing of WMD Proliferation: Final Report', *Project Alpha: King's College London* (2017), pp. 45-48.
67 Brewer, Jonathan, 'Study of Typologies of Financing of WMD Proliferation: Final Report', *Project Alpha: King's College London* (2017), p. 97.
68 See https://home.treasury.gov/news/press-releases/jl2287.

4.AMLINK (Iran)

AMLINK was a Washington-based medical supply company that raised suspicions because it was exporting commodities that did not align with its business profile. The commodities in question were nuclear power plant equipment that had been purchased in an auction by a different Washington company.

The equipment was transported to Cyprus via Rotterdam and was intended to be subsequently re-exported to Bulgaria and on to Iran. Documentation regarding the shipment did not indicate it included nuclear equipment, but Cypriot authorities who inspected it identified it as such. This equipment was controlled by the Nuclear Regulatory Commission and required a license to export. The ability of Cypriot authorities to identify and interdict the cargo is a testament to the ability of a (smaller) state to play a proactive role in identifying potential proliferation activity in their transshipment hubs. Customs and border agencies may again be constrained depending on their resources, but their successful interception of the equipment reaffirms the need for specialist knowledge of MECRs.[69]

5.PF-related TFS checks in Jersey (DPRK)

In 2023, a financial services business submitted a sanctions compliance report, having identified a link between a former customer, a Jersey-registered company (Company A), one of the directors of Company A, and an associated entity (Company B). The association was discovered through the business's overnight screening system.

Company B was named in a UNSC Panel of Experts report as possibly being connected to PF activity relating to the DPRK sanctions regime. A subsequent Panel of Experts report named Company B in the context of links to other companies suspected of involvement in sanctions evasion and proliferation activity.

The financial services business had provided registered office services to Company A (of which Person A was the ultimate beneficial owner and director). It had not provided any services to Company B. Company A was a limited partner in a multi-jurisdictional structure that included Company B, in which Person A also held an ownership stake.

None of the information received provided evidence of sanctions breach, potential or actual. The matter was referred to the Jersey Economic Crime and Confiscation Unit (ECCU) for consideration.[70]

6. Criminal prosecution and enforcement action against the Foreign Trade Bank representative (DPRK)

In April 2023, the US Department of Justice unsealed two indictments charging a DPRK Foreign Trade Bank (FTB) representative for his role in money laundering conspiracies designed to generate revenue for the DPRK using virtual assets. The individual allegedly conspired with two over-the-counter traders to launder stolen virtual assets and used funds to purchase goods on behalf of the DPRK government in U.S. dollars via Hong Kong-based front companies.

OFAC designated the individual who received tens of millions of dollars in virtual assets, in part derived from the DPRK individuals unknowingly hired by U.S.-based companies to provide IT development work. When IT workers obtain employment, they are known to request payment in virtual assets and send most of their salaries through a complex laundering pattern to funnel these illegally obtained funds back to the DPRK. After receiving money from IT development workers, the FTB representative directed the -the-counter (OTC) virtual asset traders to send payments to front companies, allowing those front companies to make payments in fiat currency for goods such as tobacco and communication devices on behalf of the DPRK regime.[71]

7.Complex Proliferation Financing Typology Involving DPRK and Russian Entities

In September 2024, the US Department of the Treasury's OFAC designated a network of entities and individuals based in Russia and the Russia-occupied Georgian region >

69 FATF, *Proliferation Financing Report* (2008), p. 32.
70 *National Risk Assessment: Proliferation Financing, Government of Jersey* (2025), p. 26.
71 FATF Report, *Complex Proliferation Financing and Sanctions Evasion Schemes* (2025), p. 42.

of South Ossetia that enabled DPRK banks to access the international financial system in breach of UNSCR 1718 and UNSCR 2270.[72] The scheme involved the DPRK's Foreign Trade Bank (FTB) and Korea Kwangson Banking Corporation (KKBC), both designated under the UN sanctions regime, which used MRB Bank in South Ossetia as a cut-out for Russian TSMR Bank to move funds and open correspondent accounts.

These channels reportedly supported payments for Russian fuel exports to the DPRK. In a parallel effort, the Russian Financial Corporation Bank JSC (RFC) assisted FTB in establishing a Moscow-based front company, Stroytreyd LLC, to recover frozen DPRK assets held in defunct Russian banks. The FATF notes that such schemes exemplify how the DPRK routinely employs foreign-based front companies, covert representatives, and third-party facilitators to obscure beneficial ownership information (BOI) and the true origin or purpose of transactions. These deceptive structures enable billions of dollars in illicit financial activity to move through the international financial system, often with the complicity or tacit support of state-linked actors. The involvement of state institutions in facilitating DPRK access to global banking networks makes it increasingly difficult to disrupt sanctions evasion and detect proliferation financing activity.[73]

"These deceptive structures enable billions of dollars in illicit financial activity to move through the international financial system."

8. Attempted Export of Controlled Military Goods from Guernsey to Macau

In December 2022, a Swedish passport holder residing in Spain (Person H) contacted a Guernsey freight agent to warehouse goods arriving from France described as "flotation panels." In January 2023, Person H inspected the shipment and arranged for six boxes to be sent to a residential address in Guernsey. Shortly after, they requested that the goods be shipped to Macau, China. When preparing the export, the freight agent raised concerns to Customs about the description. Upon inspection, Customs discovered 12 boxes containing ballistic shields and body armour clearly marked "bulletproof shield."

The items were seized under the Export Control (Military, Security and Related Matters) (Bailiwick of Guernsey) Order 2010, as they were classified as military goods requiring an export licence. The UK's Export Control Joint Unit confirmed the items were subject to a UK arms embargo on Macau. Since Person H did not hold a licence, an investigation was launched.

From the outset, coordination took place between Customs, the FIU, Law Officers, the Counter Terrorism Border Police (CTBP), the Fixed Intelligence Management Unit (FIMU), and other domestic authorities. The FIU established that no financial transactions occurred within the Bailiwick but identified use of a Ukrainian credit card and disseminated intelligence to Spain and Ukraine. Further inquiries revealed Person H's links to Russian social media and that the Macau delivery address belonged to a gun shop.

Person H was later arrested upon return to Guernsey for attempting to export military goods without a licence and for making a false import declaration. They were prosecuted, convicted, and sentenced to imprisonment, with the goods and electronic devices forfeited. While no direct PF or terrorism financing TF links were identified, the case demonstrated the Bailiwick's strong inter-agency coordination, proactive intelligence sharing, and ability to detect and disrupt potential PF-related activity involving controlled goods.

72 https://home.treasury.gov/news/press-releases/jy2590
73 FATF Report, *Complex Proliferation Financing and Sanctions Evasion Schemes* (2025), p. 78.

Glossary and Abbreviations

Acronym	Term
AI	Artificial intelligence
AML	Anti-money laundering
CFT	Combatting the Financing of Terrorism
CPF	Counter-Proliferation Financing
DNFBP	Designated Non-Financial Businesses and Professions
DPRK	Democratic People's Republic of Korea
FATF	Financial Action Task Force
FI	Financial Institution
FIU	Financial Intelligence Unit
IFC	International Financial Centre
MVTS	Money Value Transfer Service
PF	Proliferation Financing
SWTG	Small States & Territories Working Group
TFS	Targeted Financial Sanctions
UN	United Nations
UNSCR	United Nations Security Council Resolution
VA	Virtual Asset
VASP	Virtual Asset Service Provider
WMD	Weapons of Mass Destruction

The Small States and Territories Working Group (STWG) was established to enhance the collective capacity of smaller jurisdictions to address financial crime risks, including money laundering, terrorist financing, and proliferation financing. The group provides a forum for sharing expertise, developing tailored guidance, and promoting proportionate approaches aligned with FATF standards, reflecting the unique institutional and resource environments of small states and territories.

This Proliferation Financing project was co-led by Gibraltar and the Isle of Man.

This document does not prejudge the status or sovereignty of any jurisdiction, nor the delimitation of international frontiers or boundaries, nor the name of any territory, city, or area, mentioned herein.