Royal United Services Institute
for Defence and Security Studies

Guidance Paper

Countering Proliferation Finance: Implementation Guide and Model Law for Governments

Andrea Berger and Anagha Joshi

About this Guidance Paper

This is the second of two guidance papers produced by RUSI on countering proliferation finance. It aims to assist governments seeking to strengthen their legal and institutional frameworks to counter proliferation finance (CPF) in accordance with UN Security Council Resolutions and Financial Action Task Force Recommendations. The paper provides guidance on international CPF obligations and also offers practical tools for states to implement these obligations in their jurisdictions. Attached to the guidance paper are model legislative provisions to assist governments develop necessary CPF legislation.

RUSI's first guidance paper was aimed at those financial institutions that have carried out little or no concerted thinking on proliferation finance as distinct from other forms of financial crime. The paper sought to raise awareness of the risk of proliferation financing and create a baseline policy for mitigating the institution against it.

The authors would like to thank Tom Keatinge for the generous support provided for the development of this guidance paper by RUSI's Centre for Financial Crime and Security Studies. This guide and the model legislative provisions were developed in response to member-country needs identified by the Asia/Pacific Group on Money Laundering (APG). The APG has assisted in the development of this guidance paper.

The authors would also like to thank David Shannon, Stephanie Kleine-Ahlbrandt, Jonathan Brewer, and Richard Cupitt for their expertise and input on this guidance paper and the model legal provisions, as well as Penny Alexander and Anton Moiseienko for reviewing the legislative drafting of the model legal provisions.

A Note from the Asia/Pacific Group on Money Laundering

The APG Secretariat welcomes RUSI's publication of this guidance paper and its model legal provisions as key inputs to assist APG members to understand both policy and technical elements of the global standards to combat proliferation financing. The production of this guidance is timely because APG members have identified various needs that require additional support as they prioritise certain policy and regulatory actions, and continue to implement robust systems to combat proliferation financing. The APG notes that the guidance and the model legal provisions do not guarantee compliance with FATF standards; rather they provide a practical contribution to global efforts to implement strong measures to combat proliferation financing. The APG Secretariat appreciates the work of the authors in preparing this valuable resource.

Countering Proliferation Finance: Implementation Guide and Model Law for Governments

Andrea Berger and Anagha Joshi

RUSI Guidance Paper, July 2017

Royal United Services Institute
for Defence and Security Studies

185 years of independent thinking on defence and security

The Royal United Services Institute (RUSI) is the world's oldest and the UK's leading defence and security think tank. Its mission is to inform, influence and enhance public debate on a safer and more stable world. RUSI is a research-led institute, producing independent, practical and innovative analysis to address today's complex challenges.

Since its foundation in 1831, RUSI has relied on its members to support its activities. Together with revenue from research, publications and conferences, RUSI has sustained its political independence for 185 years.

London | Brussels | Nairobi | Doha | Tokyo | Washington, DC

Published in 2017 by the Royal United Services Institute for Defence and Security Studies.

RUSI Guidance Paper, July 2017.

Royal United Services Institute
for Defence and Security Studies
Whitehall
London SW1A 2ET
United Kingdom
+44 (0)20 7747 2600
www.rusi.org

RUSI is a registered charity (No. 210639)

Contents

Introduction **1**

I. International Obligations to Counter Proliferation Finance **5**
UN Obligations to Counter Proliferation Finance 5
FATF Obligations to Counter Proliferation Finance 6
The Key for States: Understanding Unique Proliferation Finance Risks 9

II. Developing a Legal Framework **19**
Identify a Legislative Framework 19
Legislation or Regulation? 20
Identify Lead Policy Agency/ies 21
Supervision and Private Sector Coordination 21
Penalties 22
Ancillary or Inchoate Offences 22
Mutual Legal Assistance and Extradition 22
Information-Sharing Provisions 23
Constitutional and Human Rights Compliance 23
Asset Management 23

III. Inter-Agency Coordination **25**
Key Government Agencies Involved in CPF 25
Inter-Agency Coordination During Policy and Legal Development 26
Inter-Agency Coordination During Implementation 27

IV. Harnessing International Cooperation for CPF Initiatives **29**
Legal and Law Enforcement Cooperation 29
Cooperation on Policy Development and Capacity Building 31

V. Building an Effective Public–Private Partnership on CPF **35**

Conclusion **39**

Annex: Model Provisions to Combat the Financing of the Proliferation of Weapons of Mass Destruction 41

About the Authors 109

Introduction

THE PROLIFERATION OF nuclear, chemical and biological weapons and their delivery vehicles is a persistent threat to global peace and security. In the face of the grave risks posed by proliferation, the international community must devise effective ways to prevent state and non-state actors from attaining WMDs.

This guidance paper aims to assist governments in strengthening their domestic counter proliferation finance (CPF) regimes. It outlines the increasingly complex global obligations on CPF and the various processes for meeting them. The paper then outlines what would be needed in order to put in place the essential building blocks of a CPF regime. The model legislation in the Annex is an example of provisions that states could consider incorporating into their own frameworks. The paper also explores approaches to inter-agency cooperation to facilitate CPF efforts, international avenues for collaboration, and the importance of a public–private partnership. Without these ingredients, states are likely to lack a sufficient body of real-time information to support taking action pursuant to national legislation, no matter how well it is formulated.

At a practical level, proliferation involves both the movement of goods and attendant funding. To be effective, efforts to counter the spread of WMDs must therefore also strive to disrupt both flows, supplementing the more advanced global discussion over export controls with consideration of financing.[1] Indeed, proliferation finance is not a new challenge. The AQ Khan Network in Pakistan relied on front companies and labyrinthine financial flows to conceal transactions related to Libyan, Iraqi and North Korean weapons programmes, from the mid-1980s until 2004.[2] Iran and North Korea have continued to use some of these practices. The latter remains able to access the services of major reputable financial institutions by opening front companies overseas, circulating assets offshore to avoid on-paper connections to North Korea, co-mingling the proceeds of its legitimate trade with its illegitimate activities, and using cash couriers to move money when using the formal financial system is too risky.[3]

---

1. Such measures can build upon the sophisticated system of national and international export control regimes that governments have developed during the past four decades. These efforts include UN Resolutions (most notably UN Security Council Resolution 1540), the Treaty on the Non-proliferation of Nuclear Weapons, the Biological and Toxin Weapons Convention, and the Chemical Weapons Convention. The export control regime also has significant institutional underpinnings in the International Atomic Energy Agency, the Nuclear Suppliers Group, the Missile Technology Control Regime and numerous national authorities.
2. Michael Laufer, 'A. Q. Khan Nuclear Chronology', Carnegie Endowment for International Peace, 7 September 2005.
3. Andrea Berger, 'A House Without Foundations: The North Korea Sanctions Regime and its Implementation', *Whitehall Report*, 3-17 (June 2017), chap. II.

These examples demonstrate how proliferators continue to exploit the formal financial system for their illicit activities, whether to pay for proliferation-relevant goods from overseas companies or to pay intermediaries and facilitate logistics. Eroding their access to these payment channels and disrupting sensitive financial flows can therefore have a disproportionate effect on illegal WMD programmes.

It is crucial that this is a global collaborative effort. North Korea and other similar cases highlight the fact that countering proliferation finance is a truly shared challenge, and that proliferators are adept at exploiting weak links in global regulation and enforcement. Pyongyang maintains large corporate and logistical networks in China, Russia and Southeast Asia, including front companies and attached bank accounts, which it has used repeatedly to facilitate proliferation.[4] At the same time, it also procures goods from countries with manufacturing industries, including those in Europe and North America.[5] It utilises the bank accounts of its foreign trade and diplomatic offices worldwide, and regularly asks its diplomats to carry cash across borders to assist with the financing of WMD programmes.[6] To ship its goods, North Korea takes advantage of flags of convenience[7] in various jurisdictions, such as Kiribati, Togo and Tanzania.[8] It holds funds in traditional offshore havens, and its agents deployed overseas seek passports of convenience, as happened recently when a North Korean seeking to acquire military goods was arrested while using a second Cambodian identification.[9] Detecting and countering proliferation finance will demand inter-government collaboration, particularly information sharing, across all parts of this complicated picture.

For these reasons, CPF has in recent times reportedly received increased attention from the Financial Action Task Force (FATF), the global standard-setter for anti-money laundering and counterterrorist finance (AML/CTF).[10] By 2006, FATF member governments began to recognise that while the global export control regime had constituted a significant safeguard against WMD proliferation, it was still not enough. They found it covered the transfer of proliferation-sensitive goods and technologies, but not the financial flows that had facilitated these transfers.[11] Export controls were thus failing to detect financial signals that might help governments and financial institutions identify proliferation-linked behaviour and bring greater clarity to suspicious activity.

---

4. *Ibid*.
5. *Ibid*, chap. III.
6. *Ibid*, chap. III.
7. This refers to the practice of registering a ship in a country different from that of the ship's owners.
8. *Ibid*, chap. III, p. 35.
9. *Ibid*, chap. II, p. 14.
10. Authors' interview with FATF Plenary attendee, Paris, February 2017.
11. 'French Conference on WMD Proliferation Financing', cable from US embassy in France, 06PARIS4443_a, 27 June 2006, document obtained via Wikileaks, <https://wikileaks.org/plusd/cables/06PARIS4443_a.html>, accessed 17 June 2016. See also, '(S/NF) G7 Conference on WMD Proliferation Financing', cable from US embassy in France, 06PARIS7269_a, 7 November 2006, document obtained via Wikileaks, <https://wikileaks.org/plusd/cables/06PARIS7269_a.html>, accessed 17 June 2016.

FATF also recognised that CPF constituted a significant gap in the discussion over broader financial crime, despite the gravity of the threat posed by the spread of WMDs and the potential contribution of financial information to combating that threat. CPF efforts similarly lacked global leadership. Consequently, in 2012, FATF for the first time included CPF in its formal recommendations.[12] Countries must now cut off any funds or assets that belong to or benefit any individual or entity designated under UN Security Council sanctions. The FATF Recommendations, discussed in greater detail in Chapter I, are an important step in encouraging governments and financial institutions (FIs) to understand their UN obligations with regard to financial transactions involving countries of proliferation concern, such as North Korea.

Despite the FATF recommendations having been in place for several years, approaches to CPF remain highly uneven across governments and FIs.[13] At the domestic level, many governments have yet to put into practice concrete and/or comprehensive measures designed to combat proliferation financing, as the current round of FATF Mutual Evaluations has already highlighted. Non-existent, incomplete or ineffective legislation can cripple a government's ability to take action against a proliferation-linked transaction, individual or entity.

At present, the domestic conversation between most governments and their FIs over CPF is also lacking. FIs require assistance from governments to devise more nuanced approaches to risk mitigation and detection. While FIs may take some instruction from existing risk-assessment procedures related to fraud, the drug trade and terrorism financing, CPF presents a unique case that requires its own mechanisms for assessing risk, carrying out due diligence and remaining attentive to issues such as trade finance and insurance products.[14] Without a more coherent approach and stronger government support, the risk remains that FIs may become complicit in the financing of proliferation due to the difficulty of detecting connections between known proliferators and their networks. With tailored outreach, governments and regulators can help to make their financial sectors a more active partner in CPF. Such outreach can serve the dual purposes of education and awareness, focusing on both the nature of proliferation financing and the need to counter it. Formalised training may also be explored, whether provided directly by government or by external parties working in consultation with government.

It is important that governments individually and collectively seek to rectify these deficiencies and improve their efforts to counter the financing of WMDs and their delivery vehicles. Indeed, there has never been a more opportune moment to do so, with recent FATF impetus and an ongoing mutual evaluation round, the potential to learn lessons from previous experiences with Iranian proliferation financing, and the persistent threat posed by North Korea.

12. FATF, 'International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation: The FATF Recommendations', February 2012 (updated June 2017), pp. 11, 13.
13. Emil Dall, Andrea Berger and Tom Keatinge, 'Out of Sight, Out of Mind? A Review of Efforts to Counter Proliferation Finance', *Whitehall Report*, 3-16 (June 2016), pp. 13–14, 19–21.
14. Emil Dall, Tom Keatinge and Andrea Berger, 'Countering Proliferation Finance: An Introductory Guide for Financial Institutions', RUSI Guidance Paper, April 2017.

Chapter I of the guidance paper outlines the increasingly complex global obligations on CPF, and the recommendations, guidance and evaluation processes for meeting them offered by FATF. The chapter emphasises the importance of conducting national risk assessments as part of a state's discussion regarding CPF. Doing so is imperative for states and regions globally. By way of example, the Asia-Pacific is known to be home to a major proliferator – North Korea – and the region's geographic proximity to the country, its comparatively large diaspora communities, booming manufacturing industries and numerous transshipment hubs – to name but a few factors – result in a high risk exposure for Asia to proliferation finance.

Once states have developed a clear understanding of national risk exposure, this paper then outlines what would be needed in order to put in place the essential building blocks of a CPF regime. Chapter II covers the need for appropriate and comprehensive national legislation to allow states to take effective action in service of their UN Security Council obligations. Deficiencies in national legislation worldwide have already thwarted efforts to stop the financing of proliferation networks, or impose penalties on violators. The model legislation contained in the Annex should act as an example of provisions that states could consider incorporating into their own frameworks.

Chapters III, IV and V explore, respectively, approaches to inter-agency cooperation to facilitate CPF efforts, international avenues for collaboration, and the importance of a public–private partnership. In addition to their individual significance, each of these forms of cooperation represents a potentially critical source of information into competent national authorities. Without these ingredients, states are likely to lack a sufficient body of real-time information to support taking action pursuant to national legislation, no matter how well formulated.

By taking concrete steps in each of these areas, states can mitigate their national risk of involvement in proliferation finance. Yet this must be a joint enterprise at the regional and global levels. Like other forms of illicit finance, proliferators exploit jurisdictions with weak legislation, regulation, monitoring and enforcement. Collective action and a focused conversation among states can help to ensure that efforts by individual countries do not simply displace risk to their neighbours.

I. International Obligations to Counter Proliferation Finance

SINCE 2012, FATF has been the home for formal and coordinated international initiatives on countering proliferation finance. Prior to entering FATF's remit, the global CPF architecture was developed exclusively through UN Security Council Resolutions. The first CPF requirements were laid out in Resolution 1540 in 2004.[1] Since then, a series of increasingly detailed UN resolutions has considerably enhanced state CPF responsibilities. For example, resolutions relating to North Korea have imposed controls over the holding of bank accounts by DPRK diplomats, prohibitions against participation in joint ventures with DPRK, and prohibitions against financing trade with DPRK.[2] While the FATF framework develops more slowly than UN Security Council sanctions, and until recently was concerned only with targeted financial sanctions relating to proliferation finance (PF), states are nevertheless required to swiftly implement the broader and complex financial measures outlined by the UN Security Council. In order to combat the proliferation of WMD and ensure compliance with a shifting regulatory structure, states will need to understand not only the UN and FATF frameworks, but also their own unique PF risks.

UN Obligations to Counter Proliferation Finance

UN Security Council Resolutions form binding obligations on all UN member states. CPF-specific requirements derive largely from several resolutions passed under Chapter VII of the UN Charter,[3] which addresses threats to international peace and security. These include resolutions on WMD proliferation and non-state actors, as well as those forming the sanctions regime on North Korea. Recent restrictions (including financial restrictions) on Iran, although adopted pursuant to Article 25 of the Charter, have the same universally binding character. In all these cases, the UN has created mechanisms for evaluating the progress of member states in meeting their relevant obligations, in the form of sanctions committees, expert groups or UN Secretariat monitoring.

UN Security Council Resolution 1540 introduced the first universal expectations on states to counter proliferation finance, in response to concerns that non-state actors were becoming more capable of acquiring and transporting WMD-relevant material.[4] It directed member states to take financial measures to prevent proliferation, including the adoption and enforcement of laws prohibiting non-state actors from financing attempts to 'manufacture, acquire, possess,

1. UN Security Council Resolution 1540, 28 April 2004, S/RES/1540.
2. UN Security Council Resolution 2270, 2 March 2016, S/RES/2270; UN Security Council Resolution 2321, 30 November 2016, S/RES/ 2321.
3. UN, 'Charter of the United Nations', 24 October 1945.
4. Dall, Berger and Keatinge, 'Out of Sight, Out of Mind?', p. 3.

develop, transport, transfer or use nuclear, chemical or biological weapons and their means of delivery, in particular for terrorist purposes'.[5] Resolution 1540 also urged states to enact new controls on financial services that related to proliferation-sensitive trade, and criminalise PF, but it left the modalities to the discretion of national authorities.[6]

Since Resolution 1540 was passed in 2004, subsequent UN Resolutions have created new CPF requirements specifically related to the Iranian and North Korean nuclear programmes. While UN financial restrictions related to Iran have been significantly reduced as a result of the 2015 Joint Comprehensive Plan of Action,[7] requirements related to North Korea have stiffened. In March 2016, the UN Security Council passed Resolution 2270, which added a raft of new restrictions on North Korea's trade and finance, including on the ability of its banks to have correspondent banking relations, foreign offices and joint ventures.[8] Resolution 2270 also expanded the scope of 'prohibited activities' – which states must refrain from financing – to cover a wide range of commodities, such as gold, titanium and aviation fuel.[9] Resolution 2321, passed in November 2016,[10] further expanded both the financial sanctions and commodity-based sanctions of the North Korea regime. These complex requirements are covered further below, including in the model legislation appended in the Annex.

Despite the incorporation of finance-related initiatives in multiple UN Securit Council Resolutions, national CPF efforts remain highly uneven. A review of state implementation of Resolution 1540 in 2009 found that CPF was one of the areas of the resolution that required further development.[11]

FATF Obligations to Counter Proliferation Finance

Despite the attention paid to CPF in UN Resolutions, a group of countries active in CPF (including the US, France, Japan and Canada) determined in the mid-2000s that a forum for leadership and

5. UN Security Council Resolution 1540, 28 April 2004, S/RES/1540, p. 2, para. 2.
6. UN Security Council Resolution 1540.
7. UN Security Council Resolution 2231, 20 July 2015, S/RES/2231. Sanctions against Iranian individuals involved in ballistic missile-related activities, however, remain. Nuclear-related requirements that have been lifted include Resolution 1737 (2006), which froze assets of certain individuals and entities involved in Iran's nuclear programme and installed import/export bans on certain sensitive goods and technology. Resolution 1929 (2010) extended asset freezes and prohibited the provision of financial services in support of illicit activities.
8. UN Security Council Resolution 2270, 2 March 2016, S/RES/2270.
9. Previous rounds were as follows: Resolution 1718 (2006) imposed an arms embargo, froze assets on individuals involved in Pyongyang's nuclear programme, and installed import and export bans; Resolution 1874 (2009) further called on member states to withhold financial services that could support prohibited nuclear activities; and Resolution 2094 (2013) expanded targeted financial sanctions against individuals and entities and expanded the list of prohibited items.
10. UN Security Council Resolution 2321, 9 September 2016, S/RES/2321.
11. Another comprehensive review of Resolution 1540 was conducted in 2016, but featured little discussion of financial issues. See UN Security Council, 'Report of the Security Council Committee Established Pursuant to Resolution 1540 (2004)', S/2016/1038, 9 December 2016.

intergovernmental coordination was needed.[12] FATF, which already had a portfolio of AML/CTF efforts, was chosen to be the centre of these efforts. As a result, since 2008 FATF has issued a series of reports, guidance documents, formal recommendations and standards related to CPF. These documents provide guidance for regulators and officials in jurisdictions party to FATF and in association with FATF-style regional bodies.[13] The expectations and guidance articulated by FATF allow countries and regional bodies to work alongside their financial sectors to mitigate the risks of PF.[14]

The FATF framework consists of three parts: recommendations; assessment methodology; and guidance. As part of a process of mutual evaluation reviews, states are measured against technical compliance with the recommendations and effectiveness. It is thus important that governments continually examine all three parts of the FATF framework. FATF recommendations, while not having the law-forming character of UN Security Council Resolutions, represent political commitments by participants. These recommendations constitute the most powerful FATF action to combat financial crime. As a result, there are only two FATF recommendations related to PF. The first is Recommendation 2, which addresses the implementation of required policies and activities:

> Countries should ensure that policy-makers, the financial intelligence unit (FIU), law enforcement authorities, supervisors and other relevant competent authorities, at the policy-making and operational levels, have effective mechanisms in place which enable them to cooperate, and, where appropriate, coordinate domestically with each other concerning the development and implementation of policies and activities to combat money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction.[15]

The other recommendation that addresses CPF issues, Recommendation 7, deals directly with the financing of individuals and entities designated in UN Resolutions, requiring member states to:

> [Implement] targeted financial sanctions to comply with United National Security Council resolutions relating to the prevention, suppression and disruption of proliferation of weapons of mass destruction and its financing. These resolutions require countries to freeze without delay the finds or other assets

12. 'French Conference on WMD Proliferation Financing'. See also, '(S/NF) G7 Conference on WMD Proliferation Financing'.
13. FATF currently has 34 member countries and two member organisations. However, it also maintains a global network of nine affiliated regional bodies (FATF-style regional bodies), which use the FATF's 40 Recommendations on AML/CTF and CPF as their guidelines, and conduct national Mutual Evaluations similar to those carried out for FATF's 34 member countries. This paper is co-sponsored by the Asia/Pacific Group on Money Laundering (APG), one of the FATF-style regional bodies. See US Department of State, 'The Financial Action Task Force and FATF-Style Regional Bodies', <https://www.state.gov/j/inl/rls/nrcrpt/2015/vol2/239046.htm>, accessed 13 July 2017; and APG, 'Financial Action Task Force and FATF-Style Regional Bodies', <http://www.apgml.org/fatf-and-fsrb/page.aspx?p=94065425-e6aa-479f-8701-5ca5d07ccfe8>, accessed 13 July 2017.
14. Dall, Berger and Keatinge, 'Out of Sight, Out of Mind?', p. 5.
15. FATF, 'International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation: The FATF Recommendations', p. 11.

> of, and to ensure that no funds and other assets are made available, directly or indirectly, to or for the benefit of, any person or entity designated by, or under the authority of, the United Nations Security Council under Chapter VII of the Charter of the United Nations.[16]

While Recommendation 7 ties requirements under FATF to UN Security Council Resolutions, it focuses exclusively on targeted financial sanctions, namely the individuals or entities designated by the UN, and while these are an important component of UN Security Council-imposed obligations to counter proliferation finance, UN Resolutions include a series of other requirements, which will be discussed later. FATF's assessment methodology, particularly its 'immediate outcomes' (IOs), relate exclusively to these limited FATF recommendations. IOs provide a means of assessing the effectiveness of a country's efforts to implement UN-targeted financial sanctions relating to proliferation. IO 1 directs states to ensure there are domestic coordination mechanisms in place to combat the financing of proliferation. IO 11 adds that '[p]ersons and entities involved in the proliferation of weapons of mass destruction are prevented from raising, moving and using funds, consistent with the relevant UNSCRs [UN Security Council Resolutions]'.[17] For each, FATF has outlined the characteristics of an effective system and core issues to be considered by assessors.

Beyond targeted financial sanctions, the UN requirements also include activity-based financial sanctions, vigilance measures and cash-carry restrictions (Table 1). For example, Resolution 1540's broad instructions to enact new financial controls on proliferation-sensitive trade are not treated by FATF recommendations or their corresponding IO. Nor are the North Korea sanctions regime's prohibitions on, among other things, maintaining correspondent or payable-through accounts for its financial institutions or providing loans or guarantees for the country's trade. FATF has recently undertaken an effort to update relevant documents concerning CPF to acknowledge the expanded activity-based financial requirements of the Security Council sanctions regime on North Korea.

FATF generally emphasises the importance of risk mitigation as a component of robust AML/CTF frameworks. This principle has not been explicitly extended to cover CPF, as evidenced by the fact that neither Recommendation 1 on domestic reviews of financial crime risks nor Recommendation 20 on reporting suspicious activity mentions proliferation.[18] Nevertheless, governments should conduct risk assessments and outline corresponding mitigation approaches for this threat.[19] Doing so reflects good practice and can help states implement their binding UN obligations and meet FATF IOs during mutual evaluations.

16. *Ibid*., p. 13.
17. FATF, 'An Effective System to Combat Money Laundering and Terrorist Financing', <http://www.fatf-gafi.org/publications/mutualevaluations/documents/effectiveness.html>, accessed 28 June 2017.
18. FATF, 'International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation: The FATF Recommendations', pp. 11, 19.
19. Dall, Berger and Keatinge, 'Out of Sight, Out of Mind?', p. 9.

FATF has also issued guidance to member states to assist them with CPF, including in ways relevant to UN obligations not covered by its own recommendations.[20] Given the pace of developments regarding both the Iranian and North Korean nuclear issue, some of this guidance is out of date. In partial recognition of this, FATF has issued more recent and informal guidance statements. On 21 October 2016, it called on members and other jurisdictions to apply countermeasures and targeted financial sanctions in line with recent UN Security Council Resolutions, noting that '[J]urisdictions should take necessary measures to close existing branches, subsidiaries and representative offices of DPRK banks within their territories and terminate correspondent relationships with DPRK banks, where required by relevant UNSC Resolutions'.[21] As mentioned previously, FATF is also in the process of updating its guidance to reflect changing circumstances in relevant Security Council sanctions regimes.

The Key for States: Understanding Unique Proliferation Finance Risks

In order to effectively implement an increasingly complex regulatory framework, it is important that countries understand their PF risk exposure. Proliferation-related funds can touch any of the phases of the production, transportation and funding of global trade. In addition, it is important to recall that funds related to proliferation may not be visibly linked to the physical movement of goods.

PF risk therefore varies substantially between countries. A proliferation risk assessment can help countries understand where to look and what to look for in the context of PF risks. States should review their history of involvement in proliferation incidents, including that of their nationals, and draw lessons learned. Furthermore, states should consider, for example:

- Whether they host a major financial centre, and are thus more likely to be involved in illicit financial flows.
- Whether they have a major transshipment centre in their territory.
- Whether they are home to a manufacturing sector that produces goods controlled by international supplier regimes related to WMD and their delivery vehicles.[22]
- Whether they are geographically close to a proliferating country.
- Whether a proliferating state has a diplomatic presence in the country.

---

20. In 2013, for example, FATF issued guidance on implementing financial provisions included in UN Resolutions that cover WMD proliferation. The guidance document divides UN financial sanctions related to WMD programmes into the categories of targeted financial sanctions, activity-based prohibitions, vigilance measures, and other financial provisions, but requires compliance only with targeted financial sanctions, despite the UN obligation for member states to address all four types. See FATF, 'The Implementation of Financial Provisions of United Nations Security Council Resolutions to Counter the Proliferation of Weapons of Mass Destruction', June 2013.
21. FATF, 'Public Statement – 21 October 2016', <http://www.fatf-gafi.org/publications/high-riskandnon-cooperativejurisdictions/documents/public-statement-october-2016.html>, accessed 28 June 2017.
22. These are the Nuclear Suppliers Group, the Missile Technology Control Regime, and the Australia Group.

- Whether a proliferating state has significant corporate and trade networks in the country.
- Whether they offer shipping flags of convenience or passports of convenience, which proliferators have been known to exploit.

Such a risk assessment should be particularly vigilant to the possibility of indirect and inadvertent involvement in the financing of proliferation activities. For example, the vast majority of North Korean trade and finance, including illicit activity, is routed through China by trading networks that often have no on-paper link to Pyongyang. Consequently, it may not be immediately apparent to states conducting risk assessments that they are exposed to potential indirect involvement in North Korea's illicit finance.[23]

In addressing the risks of inadvertent involvement with covert proliferation networks, existing typologies from FATF provide some guidance. A 2008 FATF report outlined general evasive techniques used by proliferation networks, and illustrated opportunities to detect associated financial flows.[24] However, many of the typologies in the 2008 report were not specific to PF, indicating instead general techniques used in money laundering and illicit trade. Of the PF indicators identified by FATF, the vast majority were already included in financial crime guidance related to AML/CTF. Eighteen were featured in financial crime guidance issued by other bodies that were not concerned specifically with CPF.[25] The only indicator unique to PF addressed the possibility that transported goods were misaligned with the destination country's technical capabilities. Recognising and addressing this proliferation indicator in real time, however, requires knowledge of the technical nature of the shipped item and its potential applications, as well as an assessment of the industrial state of the destination country and the possibility of near-term expansion. Such an assessment requires the use of trade specialists sufficiently well versed to flag potential misalignments.[26]

The limited availability of proliferation indicators and the difficulty of acting on what limited indicators exist highlight the need for countries and their financial institutions to better understand country-specific proliferation signatures and potential exposure. Banks interviewed in a recent report by RUSI discussed the need for 'real, actionable typologies with proliferation finance specifics' to help them understand what PF indicators they should be looking for, distinct from indicators of other forms of financial crime.[27] Such PF risk-assessment efforts can draw on domestic expertise – such as trade specialists and customs officials – as well as international input from UN panels of experts and others. Ultimately, however, the success of recognising and countering proliferation finance, especially in collaboration with the financial sector, will depend on the ability of states to understand and address their own risk exposure. Table 1 summarises CPF obligations contained in UN Security Council Resolutions and corresponding references to the model legislative provisions provided in the Annex.

23. For a more detailed discussion of North Korean evasive practices, see Berger, 'A House Without Foundations', chap. II.
24. FATF, 'Typologies Report on Proliferation Financing', 18 June 2008, pp. 24–42, 53–54.
25. Dall, Berger and Keatinge, 'Out of Sight, Out of Mind?', p. 16.
26. *Ibid*., p. 17.
27. *Ibid*., p. 16.

Table 1: CPF Obligations under UN Security Council Resolutions and FATF Recommendations

UN Security Council Resolution (UNSCR)/FATF Reference	Summary of Requirement	Model Provisions to Combat the Financing of the Proliferation of WMDs
Proliferation Financing Offence		
UNSCR 1540 on proliferation of WMDs, Operative Paragraph [OP] 2 and 3(d)	Criminalise financing the proliferation of nuclear, chemical and biological weapons and their means of delivery.	**Chapter II: Proliferation Financing** Section 7: Offence of proliferation financing
Targeted Financial Sanctions		
UNSCR 1718 on DPRK, OP 8(d) UNSCR 2231 on Iran, Annex B paras 6(c) and 6(d) FATF Recommendation 7	Requirement to implement designation of persons and entities by United Nations Security Council or its Committees by enforcing: – freezing of 'assets' (funds, financial assets and economic resources) – prevention of assets from being made available.	**Chapter III: Targeted financial sanctions** Section 8: Designations by the United Nations Security Council relating to Iran Section 9: Designations by the United Nations Security Council relating to DPRK Section 16: Prohibition against dealing with assets Section 17: Prohibition against making assets available
UNSCR 1718 on DPRK, OP 9 UNSCR 2231 on Iran, Annex B para. 6(d) FATF Recommendation 7	Exceptions for basic expenses, contractual obligations apply as well as exceptions on other grounds.	**Chapter IX: Administration of the Act** Section 40: Authorisations
UNSCR 2270 on DPRK, OP 32	Requirement for countries to enforce: – freezing of assets – prevention of assets from being made available to certain persons and entities of the DPRK that the country determines is associated with DPRK's nuclear or ballistic missile programs.	**Chapter III: Targeted Financial Sanctions** Section 10: Designation relating to DPRK Section 16: Prohibition against dealing with assets Section 17: Prohibition against making assets available **Chapter IX: Administration of the Act** Section 40: Authorisations

UN Security Council Resolution (UNSCR)/FATF Reference	Summary of Requirement	Model Provisions to Combat the Financing of the Proliferation of WMDs
UNSCR 2270 on DPRK, OP 12	Defines 'economic resources', broadly, as any asset which potentially may be used to obtain funds, goods or services, such as vessels	**Chapter I: Preliminary** Section 6: Definitions [of 'asset', including economic resources]
UNSCR 2270 on DPRK, OP 23 UNSCR 2321 on DPRK, OP 12	Provides that designated Offshore Marine Management (OMM) vessels are economic resources that should be subject to asset-freezing requirements.	**Chapter I: Preliminary** Section 6: Definition of 'asset' includes vessels. [The note to this definition highlights the list of OMM vessels that should be subject to the asset-freezing requirements in Annex III of UNSCR 2270.]
UNSCR 2270 on DPRK, OP 15	Prohibition against designated persons and entities participating in joint ventures and business arrangements.	**Chapter III: Targeted financial sanctions** Section 18: Prohibition on joint ventures with designated persons and entities of DPRK
FATF Recommendation 7, Interpretive Note and Methodology	Provides a range of standards for the implementation of targeted financial sanctions related to PF.	**Chapter III: Targeted financial sanctions** Sections 11–15 relating to designation and notification processes Section 19. Court may grant order for seizure of frozen assets **Chapter VIII: Reporting obligations** Sections 35 and 36 on verification and reporting of assets of a designated person or entity **Chapter IX: Administration of the Act** All sections **Chapter X: Supervision and enforcement** All sections

UN Security Council Resolution (UNSCR)/FATF Reference	Summary of Requirement	Model Provisions to Combat the Financing of the Proliferation of WMDs
FATF Immediate Outcome 1 FATF Immediate Outcome 11	Coordinate actions domestically to combat proliferation. Persons and entities involved in the proliferation of WMDs are prevented from raising, moving and using funds consistent with relevant UNSCRs.	**Chapter VIII: Reporting obligations** Sections 37–39 on suspicious transaction reporting and additional reporting obligations **Chapter IX: Administration of the Act** All sections **Chapter X: Supervision and enforcement** All sections
Other Financial Measures Relating to DPRK		
UNSCR 2270, OP 6 UNSCR 1718, OP 8(a) and (c)	Prohibit assistance, services and financial transactions to/from DPRK related to the supply, sale or transfer of WMDs, all arms and related materiel.	**Chapter IV: Other financial measures relating to DRPK** Section 20: Prohibition on financing related to DPRK Section 21: Prohibition on financial transactions related to DPRK
UNSCR 2270, OP 33	Countries must prohibit branches, subsidiaries and representative offices of DPRK banks. Financial institutions must be prohibited from establishing joint ventures, taking an ownership interest in, or establishing or maintaining correspondent relationships with DPRK banks; except with those the Committee approves on a case-by-case basis. Existing branches, subsidiaries and representative offices, joint ventures, ownership interests and correspondent banking relationships with DPRK must be closed within 90 days.	**Chapter IV: Other financial measures relating to DRPK** Section 25: Prohibition on maintaining offices in DPRK Section 23: Prohibition on relationships with DPRK financial institutions
UNSCR 2270, OP 34	Requires countries to prohibit financial institutions from opening new representative offices or subsidiaries, branches or bank accounts in the DPRK.	**Chapter IV: Other financial measures relating to DRPK** Section 24: Prohibition on maintaining offices in DPRK

UN Security Council Resolution (UNSCR)/FATF Reference	Summary of Requirement	Model Provisions to Combat the Financing of the Proliferation of WMDs
UNSCR 2270, OP 35 UNSCR 2321, OP 31	Requires countries to take measures to close existing representative offices, subsidiaries or bank accounts in the DPRK where there are reasonable grounds to believe that such financial services could contribute to DPRK's nuclear or ballistic missile programs; except if the Committee approves on a case-by-case basis where the services are required for: – humanitarian assistance – diplomatic activities – other purposes consistent with UNSCRs.	**Chapter IV: Other financial measures relating to DRPK** Section 25: Prohibition on maintaining offices in DPRK **Chapter IX: Administration of the Act** Section 40: Authorisations
UNSCR 2321, OP 16	States must limit the number of bank accounts of DPRK diplomatic missions and consular offices and DPRK diplomats and consular officers.	**Chapter IV: Other financial measures relating to DRPK** Section 26: Prohibition on accounts related to DPRK missions **Chapter IX: Administration of the Act** Section 40: Authorisations
UNSCR 2321, OP 17	States must prohibit diplomatic agents of DPRK from receiving personal profit from professional or commercial activities.	**Chapter IV: Other financial measures relating to DRPK** Section 27: Prohibition against financial transactions related to professional or commercial activities
UNSCR 2321, OP 18	Prohibit the use of real property owned or leased by DPRK from being used for any purpose other than diplomatic or consular activities.	**Chapter IV: Other financial measures relating to DRPK** Section 28: Prohibition against use of real property
UNSCR 2270, OP 36 UNSCR 2321, OP 32	Prohibition on public and private financial support for trade with DPRK, including the granting of export credits, guarantees or insurance to their nationals or entities involved in such trade; except as approved by the Committee on a case-by-case basis.	**Chapter IV: Other financial measures relating to DRPK** Section 22: Prohibition on trade with DPRK **Chapter IX: Administration of the Act** Section 40: Authorisations

UN Security Council Resolution (UNSCR)/FATF Reference	Summary of Requirement	Model Provisions to Combat the Financing of the Proliferation of WMDs
UNSCR 2270, OP 37 UNSCR 2094, OPs 11 and 14 UNSCR 2321, OP 35	Prohibit transfer of bulk cash and gold to DPRK that could be used to evade UNSCR requirements.	**Chapter IV: Other financial measures relating to DRPK** Section 21: Prohibition on financial transactions related to DPRK **Chapter VI: Cross-border transportation of cash, precious metals and precious stones** All sections
Requirements Relating to Coal, Metals, Fuels, Minerals, etc.		
UNSCR 2321, OP 26	Prohibition on supply, sale and transfer of coal, iron and iron ore, with exceptions.	**Chapter IV: Other financial measures relating to DRPK** Section 20: Prohibition on financing related to DPRK Section 21: Prohibition on financial transactions related to DPRK **Chapter IX: Administration of the Act** Section 40: Authorisations (The above are only financial measures. States primarily need to implement trade/export control measures to give effect to this requirement.)
UNSCR 2321, OP 28	Prohibition on supply, sale and transfer of copper, nickel, silver and zinc.	**Chapter IV: Other financial measures relating to DRPK** Section 20: Prohibition on financing related to DPRK Section 21: Prohibition on financial transactions related to DPRK (The above are only financial measures. States primarily need to implement trade/export control measures to give effect to this requirement.)

UN Security Council Resolution (UNSCR)/FATF Reference	Summary of Requirement	Model Provisions to Combat the Financing of the Proliferation of WMDs
UNSCR 2270, OP 30	Prohibition on supply, sale and transfer of gold, titanium ore, vanadium ore, and rare earth minerals.	**Chapter IV: Other financial measures relating to DRPK** Section 20: Prohibition on financing related to DPRK Section 21: Prohibition on financial transactions related to DPRK (The above are only financial measures. States primarily need to implement trade/export control measures to give effect to this requirement.)
Requirements Relating to Vessels		
UNSCR 2270, OP 19 UNSCR 2321, OP 8	Prohibition on leasing or chartering vessels, aircraft and crew services to DPRK; except where Committee approves on a case-by-case basis.	**Chapter IV: Other financial measures relating to DRPK** Section 30: Prohibition relating to vessels and aircraft **Chapter IX: Administration of the Act** Section 40: Authorisations
UNSCR 2270, OP 20 UNSCR 2321, OP 9	Prohibition on owning, leasing, operating or insuring a DPRK flagged vessel; except as approved by the Committee on a case-by-case basis.	**Chapter IV: Other financial measures relating to DRPK** Section 29: Prohibition relating to vessels **Chapter IX: Administration of the Act** Section 40: Authorisations
UNSCR 2321, OP 22	Prohibition on providing insurance or reinsurance to vessels owned, controlled or operated by DPRK; except as approved by the Committee on a case-by-case basis.	**Chapter IV: Other financial measures relating to DRPK** Section 29: Prohibition relating to vessels **Chapter IX: Administration of the Act** Section 40: Authorisations
UNSCR 2321, OP 23	Prohibition on procuring vessels and aircraft crew services from DPRK.	**Chapter IV: Other financial measures relating to DRPK** Section 30: Prohibition relating to vessels and aircraft

UN Security Council Resolution (UNSCR)/FATF Reference	Summary of Requirement	Model Provisions to Combat the Financing of the Proliferation of WMDs
Other Financial Measures Relating to Iran		
UNSCR 2231, Annex B, paras 2 and 4	Prohibition on certain commercial activities related to Iran without Security Council approval. Exceptions apply in relation to certain activities.	**Chapter V: Other financial measures relating to Iran** Section 33: Prohibition on commercial activities
UNSCR 2231, Annex B, paras 2, 4(b) and 5	Prohibition on making financial resources and financial services available related to the sale, supply or transfer of certain nuclear-related items, ballistic-missile related items and arms and related materiel without Security Council approval. Exceptions apply in relation to certain items.	**Chapter V: Other financial measures relating to Iran** Section 31: Prohibition on financing relating to Iran Section 32: Prohibition on financial transactions relating to Iran **Chapter IX: Administration of the Act** Section 40: Authorisations

II. Developing a Legal Framework

IN DEVELOPING LEGISLATION that meets international obligations on CPF, states should be mindful of several key legal and policy considerations that are discussed below. Gaps in legal frameworks will have a significant impact on a country's ability to combat proliferation finance, including through the successful prosecution of offenders. For example, in the Singaporean case of Chinpo Shipping (Private) Pty, prosecutors faced major challenges in securing a proliferation financing conviction due to gaps in the legal framework implementing the UN Security Council Resolutions related to North Korea. Signapore's legal framework did not adequately cover financing the shipping of conventional weapons related to WMD programs, as required by the UN Resolutions. This caused difficulties in proving that the transfer of funds (which was related to shipping costs for a vessel that carried conventional weapons) contributed to North Korea's nuclear program. Carefully drafted legislation that reflects the nuances of the various UN Security Council Resolutions on CPF can avoid difficulties with investigation and prosecution at a later stage.[1]

Identify a Legislative Framework

The international obligations on CPF contain a range of different measures, from targeted financial sanctions to activity-based prohibitions. Therefore, it is possible, depending on a country's existing laws, that more than one piece of legislation may be required to implement all international obligations. Examples of legislation that could integrate PF provisions include: AML/CTF laws; criminal or penal codes; counterterrorism or security laws; counterproliferation of WMD laws; and customs, trade or export control laws.

Some countries have taken the approach of adopting a law that implements Article 41 of the UN Charter regarding measures not involving the use of armed force, and subsequently adopting regulations that address the different requirements of each Security Council Resolution imposing sanctions. This approach creates a flexible framework that can capture all sanction obligations. Given that regulations can be amended easily, it also enables countries to keep domestic laws compliant with changing international obligations. It should be noted that while a single UN Charter law brings legal obligations under one framework, a number of agencies will nevertheless be involved in its implementation. Strong inter-agency coordination will be vital to successful implementation, as discussed further in Chapter III.

When deciding which law/s should incorporate CPF provisions and whether an entirely new law should be developed, countries should first undertake a mapping exercise to identify all relevant existing legislation.

1. Andrea Berger, 'The Chinpo Shipping Case Implodes', guest post, *Arms Control Wonk*, 15 May 2017, <http://www.armscontrolwonk.com/archive/1203164/guest-post-the-chinpo-shipping-case-implodes/>, accessed 19 July 2017.

Examples of legislative approaches to CPF adopted by countries include:

- Australia
  - Charter of the United Nations Act 1945 and related Regulations on Dealing with Assets, Democratic People's Republic of Korea, Iran, and Customs (Prohibited Exports).[2]
- France
  - Law n°2011-266 (March 14, 2011) concerning the fight against proliferation of weapons of mass destruction and their means of delivery.[3]
- Malaysia
  - Strategic Trade Act 2010 and related Strategic Trade Act (United Nations Security Council Resolutions) Regulations.[4]
- New Zealand
  - United Nations Act 1946 and related Regulations on Democratic People's Republic of Korea, and Iran – Joint Comprehensive Plan of Action.[5]
- Singapore
  - United Nations Act (Chapter 339) and related Regulations on Democratic People's Republic of Korea and Iran. Covers all persons except financial institutions and all UN sanctions resolutions.[6]
  - Monetary Authority of Singapore Act and related Regulations on Democratic People's Republic of Korea and Iran. Covers regulated financial institutions and finance-related activities.[7]
- Thailand
  - Counter-Terrorism and Proliferation of Weapons of Mass Destruction Financing Act 2016.[8]

Legislation or Regulation?

UN Security Council Resolutions are regularly amended. The 2015 and 2016 amendments to the Resolutions on Iran and North Korea made significant changes to the international obligations. It

2. 'Charter of the United Nations Act 1945 (Australia)', legislation available at <https://www.legislation.gov.au>, accessed 13 July 2017.
3. 'Law n°2011-266 (March 14, 2011) (France)'.
4. 'Strategic Trade Act 2010 (Malaysia)'. The Bill as passed is available at <http://www. parlimen.gov.my/billindex/pdf/ DR042010.pdf>, accessed 19 July 2017.
5. 'United Nations Act 1946 (New Zealand)', legislation available at <http://www.legislation.govt.nz>, accessed 13 July 2017.
6. 'United Nations Act (Chapter 339), 2001 (Singapore)', legislation available at <http://statutes.agc.gov.sg/aol/search/display/view.w3p;ident=dc537951-6037-44b6-a4a4-6652ae706deb;page=0;query=DocId%3Ac9d8ccfe-5c41-4f6f-b744-31c81f29b562%20Depth%3A0%20Status%3Ainforce;rec=0>, accessed 19 July 2017.
7. 'Monetary Authority of Singapore Act (Chapter 186), 1970 (Singapore)', legislation available at <http://statutes.agc.gov.sg/aol/search/display/view.w3p;page=0;query=DocId%3A8cde6c10-335e-4415-b97a-62aa88a1be3f%20Depth%3A0%20Status%3Ainforce;rec=0;whole=yes>, accessed 19 July 2017.
8. 'Counter-Terrorism and Proliferation of Weapons of Mass Destruction Financing Act 2016 (Thailand)'.

is recommended that countries adopt a legislative framework that covers the nuances of these sanctions regimes, and which are flexible in adapting to changes in international obligations. A key consideration is whether a broad legal framework can be implemented in principal legislation and how much of the details can be included in regulations, rules, proclamations or other subordinate legislative instruments. This will differ between countries.

For example, Australia's Charter of the United Nations Act 1945 provides a legal framework to implement a wide range of Security Council Resolutions (including, but not limited, to those relating to PF) and provides most of the details of the international obligations in its Regulations. The Regulations are made by the executive branch of government and are tabled in parliament, but do not need to be passed there. They can therefore be amended quickly to ensure timely compliance with Security Council Resolutions. A number of countries adopt this approach, particularly those that have specific legislation to implement Security Council Resolutions pursuant to Article 41 of the UN Charter.

Identify Lead Policy Agency/ies

Deciding on an appropriate legislative framework requires consideration of which government ministry, agency or department should have the policy lead for proliferation financing matters. A number of government agencies are likely to have some policy role in CPF matters, including foreign affairs, home affairs, justice, trade, customs and AML/CTF. Does a government agency in your country already have an existing mandate for proliferation financing matters either stated in law, by executive order or some other authority? If not, a lead agency will need to be nominated. This decision will have an impact on the legislative framework that is ultimately adopted since policy agencies generally administer the legislation relevant to their policy portfolio.

Inter-Governmental Coordination

The lead policy agency will have a key role in coordinating all relevant government agencies. Choosing a central agency as the policy lead can be useful as it ensures that it has both the administrative resources and the policy authority to coordinate all relevant government agencies.

Supervision and Private Sector Coordination

Countries should also nominate one or more supervisory agencies. The supervisory agency may, but need not, be the lead policy agency. In determining a supervisory agency, a key consideration is the existing regulatory or supervisory powers of the agency. As discussed in Chapter V, a wide variety of private sector actors may be involved in PF. A national risk assessment of PF will assist in identifying high-risk sectors. Choosing a supervisory agency that has existing legislative powers as well as existing practical outreach mechanisms to regulate or supervise key private sector actors will avoid the need to create new powers and mechanisms and will in turn create regulatory efficiencies. Ultimately, an effective supervisory framework for CPF may involve a combination of two or more supervisory agencies to cover different industry sectors, in addition to a lead policy agency providing overall, cross-government coordination.

Monitoring and Enforcement Powers

CPF laws will impose obligations and/or prohibit conduct. It will be necessary to ensure that appropriate supervision and enforcement powers are available to monitor and enforce CPF legislation. This is likely to include powers to request the production of documents and other property, conduct compliance checks or audits, enter premises and search for and seize documents and other property. Countries should also consider whether special investigative powers, such as phone-tapping, audio and video surveillance, and extended duration of police custody, should be included. If a law enforcement agency, such as customs, or a regulatory one, such as a central bank, is the nominated supervisory agency, it may have some of these powers provided in other legislation. If a policy agency is the nominated supervisory agency, it may have limited supervisory or enforcement powers and may need to rely on a regulatory or law enforcement agency to ensure the provisions are carried out. The legal framework should therefore ensure that the necessary powers are available to monitor and enforce compliance with CPF legislation and that any necessary links or cross-references with other legislation are made.

Penalties

Countries should ensure that failure to comply with an obligation or engaging in conduct that is prohibited attracts penalties commensurate with the serious effect of PF activity on global peace and security. The FATF Recommendations state that countries should ensure that they have a range of effective, proportionate and dissuasive sanctions to deal with both natural and legal persons. In the context of bodies corporate, sanctions should extend to their directors and senior management. To promote compliant behaviour, it is recommended that in addition to criminal offences, CPF supervisory authorities have a range of non-criminal enforcement actions available, such as the ability to impose fines, issue warning notices or call for corrective actions to be taken.

Ancillary or Inchoate Offences

Countries should ensure that ancillary or inchoate offences are provided for in their criminal law and apply to offences in their CPF law. Ancillary or inchoate offences are variously described across countries, but commonly include: attempt; participate as an accomplice in; incite; conspire to commit; organise; and direct.

Mutual Legal Assistance and Extradition

For cross-border investigations, countries need adequate legal basis as well as procedures for mutual legal assistance and extradition in the context of PF. International legal cooperation is vital in the fight against PF and following the money trail of proliferation activities. Mutual legal assistance enables countries to obtain evidence for use in court proceedings and can include executing search warrants to obtain bank, business and property records and compelling witnesses to give evidence. Extradition is the process whereby a country agrees to hand over an individual to another country to face criminal charges or for the enforcement of a sentence.

Many jurisdictions will require dual criminality – where the conduct is an offence in both countries – and coercive powers are necessary to execute the request. Countries should also ensure that mutual legal assistance is not denied on the grounds that financial insitutions are required to maintain secrecy or confidentiality.

Information-Sharing Provisions

Due to the number of government agencies that are likely to be involved in CPF, it will be important for the legislation to include provisions to enable information sharing among government agencies. In addition, given the global reach of proliferation and PF activities, the legislative authority to share information with other countries will be vital. Generally, information-sharing provisions are limited by privacy laws and come with restrictions on the use of the shared information. Countries should seek to maintain a balance between upholding privacy and data protection, and adopting efficient information-sharing mechanisms to combat PF and investigate and prosecute offenders. Information-sharing provisions should not only enable the sharing of information for law enforcement purposes, but also for regulatory and supervisory purposes.

Constitutional and Human Rights Compliance

Countries should ensure that CPF laws comply with their constitution and/or bill of rights as well as with international human rights obligations. Common law countries also protect some human rights through the judicial application of these principles. Some aspects of CPF legislation may conflict with human rights if appropriate safeguards are not built into the law. For example, provisions imposing targeted financial sanctions may bring into question the right to property. Therefore, it will be important to ensure that due process and appeal rights are protected by the legislation and that access to property is possible under limited circumstances, such as meeting basic needs (food, housing and so on).

Another common issue arising from targeted financial sanctions is the adoption of Security Council designations of persons and entities into domestic law. For constitutional compliance, some countries may require parliamentary or judicial action before Security Council designations can be implemented domestically. Several countries have found avenues for enabling automatic domestic application of Security Council designations that comply with constitutional requirements through careful legislative drafting – for example, Papua New Guinea's United Nations Financial Sanctions Act 2015.[9] Papua New Guinea has strong constitutional safeguards, but nonetheless has automatic domestic application of Security Council designations.

Asset Management

One of the international obligations on CPF is the establishment of targeted financial sanctions, which require that the assets of designated persons and entities be frozen by the holders of those assets. For example, banks are required to freeze the accounts of designated persons

9. 'United Nations Financial Sanctions Act 2015 (Papua New Guinea)'.

and entities. In some cases, the assets may be property, such as real estate or vehicles. In some countries, the government is able to assume custody and management of frozen assets, particularly where there is a danger the assets will dissipate. In such cases, countries will need to have in place legal and practical measures for frozen asset management. Under targeted financial sanctions, although the government may take custody of an asset to ensure it is not disposed of or moved to another jurisdiction, legal ownership of the asset remains with the designated person or entity. Careful asset management is necessary to avoid liabilities for destruction or loss of value of the asset. In the context of PF, assets may not always be real property but may be in the form of commitments to make expenditure at a future date, which raise complex challenges for asset management. It is recommended that countries review legal and practical asset-management frameworks and ensure that asset-management provisions cover assets managed pursuant to targeted financial sanctions.

III. Inter-Agency Coordination

THIS CHAPTER CONSIDERS best practices for inter-agency coordination during policy and legislative development as well as throughout the law's implementation. Importantly, agencies need to have the legal authority to share information regarding PF as well as effective legal and practical controls to safeguard that information. The importance of having legal provisions on information sharing was discussed in Chapter II.

Key Government Agencies Involved in CPF

A diverse range of government agencies are likely to be involved in CPF. These agencies may have pre-existing engagement with some private sector actors with whom engagement will be needed for the purposes of CPF. Engagement with private sector actors is discussed further in Chapter V. As an initial step, it is important to develop a stakeholder map of relevant government agencies that identifies their role in CPF. Of note, the range of agencies involved will be broader than in the context of AML/CTF. Countries that have AML/CTF inter-agency coordination mechanisms will need to look beyond this to ensure that all relevant agencies are identified (Table 2).

Table 2: Government Agencies Likely to be Involved in CPF

Agency	Role
Export control, customs and border control agencies	These agencies enforce compliance with export controls related to proliferation. Financial information will be useful to these agencies to detect end-users of goods. These agencies can also be sources of information for other agencies on goods and services that might be abused for proliferation and information on proliferators.
Intelligence agencies	These agencies can provide a link between dual-use items and their destination for proliferation activities. They play a key role in identifying individuals involved in or supporting proliferation financing. Intelligence from these agencies may be used by customs/border control agencies to determine the grant of export licences or to allow goods across the border. Customs agencies could use intelligence to trigger catch-all provisions to stop shipment by a profiled supplier or to profiled end-users.
Financial intelligence unit	These units play a key role in undertaking CPF risk assessments as they have access to a wide range of financial data, and they can undertake useful network analysis and generate investigative leads. While FATF does not require the filing of suspicious transaction reports (STRs) where PF is suspected, some countries include this as a requirement in their domestic AML/CTF laws. STRs can be a valuable source of information to identify suspect individuals, businesses or accounts. The requirement to report STRs for PF also assists in enabling financial intelligence units to monitor compliance of CPF laws by financial institutions.

Agency	Role
Law enforcement and prosecution agencies	These agencies are critical end-users of information for criminal enforcement of CPF laws. Investigations by law enforcement agencies can also generate additional information.
Financial supervisors and other regulatory authorities	These agencies can impose licensing requirements on private sector institutions to ensure that designated entities cannot operate in their country or that entities licensed to operate in their country cannot conduct business relationships with designated entities. These agencies play a key role in ensuring that private sector institutions are informed of PF risks and can provide a valuable link between other government agencies and private sector institutions.
Trade promotion and investment agencies	These agencies need to be aware of PF risks when considering whether to provide support for trade. These agencies may also gain information on trade approaches that may indicate patterns of illicit procurement, which can then be shared with other government agencies.
Policy agencies, such as foreign affairs, finance, home affairs or justice	These agencies can play an important role in ensuring that a country's CPF legal regime is compliant with international obligations and that practical mechanisms are robust and effective. They may also be useful in facilitating inter-agency coordination within government. Foreign affairs agencies also play a crucial role in international cooperation on CPF.
Agencies involved in implementing targeted financial sanctions	These agencies will require a variety of information to identify individuals and entities involved in or suspected of PF.

Source: Adapted by the authors from FATF, 'Sharing Among Domestic Competent Authorities Information Related to the Financing of Proliferation', Best Practices Paper, February 2012.

Inter-Agency Coordination During Policy and Legal Development

Inter-agency coordination should commence from the very beginning of the policy and legislation development stage. Convening a multi-agency forum at the outset of the process is important for developing a legal framework that is most effective for the country context and that has the support, understanding and buy-in from the wide variety of government agencies involved in CPF. Engaging a wide variety of agencies at the outset has a number of advantages. It can raise awareness of the issues for all relevant agencies, assist in identifying the most appropriate lead policy agency or agencies, uncover potential challenges to certain legal approaches at an early stage, and clarify the roles and responsibilities of different agencies. It can also assist in setting timeframes to avoid delays, ensure that necessary ministerial and senior management approvals can be sought, and identify technical assistance needs. Broad inter-agency coordination from the outset is also important in understanding PF risks and gaps in knowledge or responses to develop the necessary policy, legal and operational frameworks.

Examples of inter-agency coordination during policy and legal development include some, or a combination, of the following:

- A formal letter to each relevant government agency informing of the development of counter proliferation policy and legislation, and requesting input into the process.
- Convening a multi-agency meeting or forum for all relevant agencies.
- Engaging senior managers on the issue through formal letters or in-person meetings.
- Requesting each relevant agency to nominate an officer-level contact point for CPF issues.
- Holding one-on-one, agency-to-agency meetings on CPF.
- Establishing a task force of officers from several agencies dedicated to the development of counter proliferation policy and legislation.

It is highly recommended that a multi-agency meeting or forum be convened and supported by one or more of the suggested measures above. This would allow issues to be debated and discussed, provide an efficient process, assist in building consensus and lead ultimately to more robust policy and legislative development. Whatever measures are adopted, regular engagement with all relevant agencies should be continued throughout policy and legislative development.

Inter-Agency Coordination During Implementation

To ensure compliance with a CPF regime once it has been developed, well-established mechanisms for inter-agency coordination and information sharing are necessary. FATF Recommendation 2 states that countries should ensure that relevant government agencies at policy and operational levels have effective mechanisms to cooperate and coordinate domestically to combat the financing of WMD proliferation.[1]

As previously noted, the CPF context involves a wide range of government and private sector actors. Some government agencies may already have established mechanisms for engaging with certain private sector actors. For example, financial intelligence units (FIUs) or financial supervisors should have mechanisms for engaging with reporting entities to enforce compliance with AML/CTF laws, export control agencies may have established links to export businesses, and policy departments may have public awareness platforms, such as websites or information hotlines. To ensure that government agencies have access to all necessary information and that they provide consistent external messaging, it is important that these agencies are able to regularly coordinate effectively and efficiently.

Inter-agency coordination allows for a range of matters to be discussed, including:

- Identification and analysis of CPF risks, trends and typologies.
- Identification of intelligence gaps.
- Coordination of private sector engagement, supervision and enforcement measures.
- Coordination of investigations.

1. FATF, 'International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation: The FATF Recommendations'.

- Review of existing policy, legal and operational mechanisms for CPF.
- Sharing information on international developments and best practices.

Ongoing inter-agency coordination can be achieved through a variety of mechanisms, such as:

- Regular multi-agency meetings or forums.
- Establishment of a group of nominated officer-level contacts from each relevant agency.
- Establishment of generic CPF email addresses in relevant agencies (with several officers having access) or emergency contacts to ensure that priority or emergency issues are addressed quickly.
- Coordinating on regular briefs to senior managers or ministers.
- Formal written communication between agencies.
- Informal phone or email communication between agencies.
- Temporary secondment of officer/s from one agency to another for special projects or to share expertise between agencies.
- Periodic joint or multi-agency training sessions on proliferation financing.
- Creating a taskforce of officers from relevant agencies to work on special projects or issues.

Legal authorities for information sharing are discussed in Chapter II. These need to be coupled with practical measures to facilitate the sharing of information. Such practical measures can include entering into Memorandums of Understanding (MoUs) between government agencies. MoUs have a number of practical benefits, including creating efficiency, clarifying resources and resource sharing, building a team of experts across government, harnessing the information gathering powers and expertise of each agency to achieve mutual objectives, ensuring that information is shared legally and that procedural and physical mechanisms are in place to protect data and privacy. While MoUs can be beneficial, its absence need not impede information sharing. Building a network of officer-to-officer contacts among agencies and cultivating a culture of communication (within legal and procedural bounds) is recommended.

IV. Harnessing International Cooperation for CPF Initiatives

INTERNATIONAL COOPERATION IS a cornerstone of CPF efforts, from prevention to detection to disruption. UN Security Council Resolutions on proliferation finance call for international cooperation. For example, Resolution 1540 calls on states to cooperate to counter proliferation finance and further encourages those with greater capacities to provide implementation assistance to other countries. International cooperation is also a key component of the FATF Recommendations aimed at strengthening the financial system against illicit use, bringing offenders to justice and recovering the proceeds of crime.[1]

International cooperation can give states a greater appreciation of their risk exposure to proliferation-sensitive activity, and provide useful lessons for approaches to addressing them. Given the often transnational nature of proliferation activity and networks, international cooperation can be vital in initiating new investigations, pursuing existing investigations, gathering admissible evidence, prosecuting alleged offenders and tracing and recovering the proceeds of crime. Cooperation can also be an important mechanism for developing national capacity to comply with the FATF Recommendations and UN Resolutions aimed at addressing proliferation threats. International cooperation is essential at most stages in counter proliferation action, particularly with real-time incidents. Yet financial information, by virtue of being proprietary data regulated by national laws, is enormously difficult to share across borders. Efforts to promote bilateral and multilateral cooperation on CPF can help to address this practical challenge.

There are a range of avenues where countries can cooperate to reduce PF risks, build capacity, and take action on ongoing incidents. These avenues are mutually reinforcing; international engagements to build CPF capacity can pave the way for effective intelligence sharing and enforcement coordination at a bilateral level in response to PF incidents.

Legal and Law Enforcement Cooperation

States are encouraged to pursue both formal and informal avenues of cooperation to facilitate optimum legal and law enforcement outcomes. Formal avenues of cooperation are generally known as ‘international legal cooperation’ and include mutual legal assistance and extradition. Informal avenues of cooperation include police-to-police information sharing, either bilaterally or through multilateral bodies. Informal avenues of cooperation can be a useful precursor to formal cooperation as they enable the establishment of contacts and the clarification of domestic legal requirements between countries, greatly improving the efficiency of formal cooperation

1. FATF, ‘International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation: The FATF Recommendations’.

mechanisms. In addition, informal cooperation can enable speedy access to information in circumstances where formal channels of cooperation are not required under a state's domestic legislation. Whether pursuing formal or informal avenues for cooperation, MoUs or other arrangements can be useful tools in outlining the practical mechanisms for such cooperation to occur. They may clarify matters, such as the scope of cooperation, contact points, preferred methods of communication and data-protection measures. However, states should be careful to ensure that MoUs or similar arrangements do not become obstacles to the building of person-to-person contacts and efficient and effective communication.

International Legal Cooperation

International legal cooperation includes mutual legal assistance and extradition. Extradition is the procedure whereby a state agrees to hand over an individual to another state to face criminal charges or, if that person has already been tried and convicted, for enforcement of the sentence. Mutual legal assistance is the process countries use to provide and obtain formal government-to-government assistance to obtain evidence for use in court. The range of assistance includes executing search warrants to obtain bank, business and property records, compelling witnesses to give evidence and measures to locate, restrain, forfeit and return the proceeds of crime. Mutual legal assistance is generally required for the use of coercive powers. Subject to domestic laws, mutual legal assistance can occur on the basis of reciprocity, MOUs or bilateral or multilateral agreements.

FIU-to-FIU Cooperation

Cooperation between national FIUs can occur through reciprocity, bilateral arrangements or multilateral bodies. At the multilateral level, the Egmont Group of 152 FIUs was established to facilitate cooperation and information exchange.[2] Egmont's Principles of Information Exchange guide the efficient and effective sharing of financial intelligence and seek to break down barriers to information exchange.[3] The principles also assert stringent data protection and confidentiality controls. Egmont's Secure Web provides an avenue for contacting foreign FIUs and collecting information.[4]

Police-to-Police Cooperation

Multilateral organisations, such as Interpol, provide avenues for global police cooperation. Regional cooperation mechanisms also exist, for example, the Pacific Transnational Crime Coordination Centre (PTCCC), which involves multiple law enforcement agencies, including

2. Egmont Group of Financial Intelligence Units, <https://egmontgroup.org/en/content/about>, accessed 15 June 2017.
3. *Ibid*.
4. *Ibid*.

police, customs and immigration.[5] The PTCCC not only facilitates the sharing of information, but also collaborates to identify current and emerging crime risks in the region.

Some countries also have liaison officer networks across other countries to facilitate information exchange and to build relationships. The person-to-person contacts, the development of a shared understanding and a common purpose and the exchange of skills offered by liaison networks can prove invaluable to law enforcement efforts against serious and transnational crimes, including PF.

Joint Investigations

Due to the transnational nature and complexity of PF networks, states should also consider opportunities for conducting a joint investigation of cases, which generally requires both a legal basis and a clear operational framework.

Cooperation on Policy Development and Capacity Building

The rapid evolution of proliferation threats, trends and tactics means that sustained global attention to CPF is necessary. The global effort to combat PF thus depends on a critical mass of individual states prioritising the policy. If multilateral bodies (including FATF and the UN) are to continually invest the resources needed to keep relevant information and guidance timely and accurate, states need to be vocal in maintaining CPF as a priority policy issue in these forums.

The adoption of CPF as part of the FATF portfolio and mutual evaluation processes created an important source of international leadership on this issue, and the reports produced as part of the initial effort continue to serve as reference texts. However, the volume of non-reporting to the UN suggests that a concerning number lack either appreciation of the threat and their potential role and capacity, or both. It is therefore important that states not only implement their CPF obligations domestically and report their progress as part of FATF and UN evaluation processes, but also make an active contribution to international understanding of PF threats and lessons learned from taking action to counter them.

Conversely, international mechanisms for collaboration can help states eager to improve their CPF frameworks, particularly early in the capacity-building process. Implementing the UN and FATF frameworks into national legislation can be a complex process, with potential roles for many agencies, ministries and departments. Discussing opportunities and challenges in national policy and legislative work on CPF bilaterally or multilaterally among states generates a body of best practice. This ultimately benefits all states. Such coordination can also enable later intelligence sharing, incident response and enforcement action by helping officials become familiar with the laws and procedures of their counterparts in other countries.

5. Pacific Islands Chief of Police, 'Pacific Transnational Crime Network (PTCN)', <https://www.picp.co.nz/our-work/pacific-transnational-crime-network-ptcn/>, accessed 15 June 2017.

International cooperation can provide significant value to domestic FIs. Given the differences in CPF regulations and expectations across countries, FIs often feel they are subject to mixed messages, with inadequate guidance on whether they must meet stringent UN expectations in order to operate within those of their home government. Such confusion can lead FIs to cease doing business with (or 'de-risk') certain trade sectors or even entire countries.[6] Global engagement can clarify the relationship between international expectations and national laws, and generate more useful guidance to FIs – the organisations on the front lines of CPF efforts. Public–private partnerships on CPF are discussed further in Chapter V.

Avenues for Technical Assistance

There are numerous avenues for soliciting technical assistance on CPF, including through UN Security Council Committees, FATF and related bodies and bilaterally.

Security Council Committees

The Security Council Committee established pursuant to Resolution 1540 and its corresponding Group of Experts offer 'matchmaking' services for technical assistance related to any of the obligations imposed by the Resolution.[7] This includes obligations to impose national financial controls relating to proliferation-sensitive activity. Any state requests for technical assistance are examined by the group and forwarded to another country or multinational body that may provide the service.

Similarly, the UN Panel of Experts on North Korea has significant expertise on that particular state threat. It has conducted in-depth investigations into proliferation-linked North Korean activity since 2009, including related financial flows. Consequently, they are well placed to contribute expertise on patterns of illegal activity and the nature of the North Korean PF threat in general, and offer advice to states on approaches to implementing Security Council-imposed obligations to counter Pyongyang's illicit finance.

FATF, FATF Training and Research Institute (FATF-TREIN) and FATF-Style Regional Bodies

Regional cooperation can provide a useful link between international capacity-building and bilateral detection and response efforts. Several proliferation indicators are region specific, including geographic proximity to a country of concern. Efforts to address proliferation risks – even if undertaken unilaterally – can in these circumstances depend on a regional architecture that allows communication with policy, intelligence, finance, law enforcement, and custom and border control officials in neighbouring countries. Developing a strong regional architecture might include initiatives such as: conducting regional risk assessments of PF; formulating region-specific typologies of PF activity; establishing formal and informal channels of communication;

6. Dall, Berger and Keatinge, 'Out of Sight, Out of Mind?', p. 24.
7. UN, 1540 Committee, 'General Information', <http://www.un.org/en/sc/1540/assistance/general-information.shtml>, accessed 14 July 2017.

undertaking periodic joint training sessions or exercises; and creating task forces to work on special regional issues.

FATF guidance can also provide a useful common ground for countries to cooperate with international partners on CPF efforts. Its 2008 typologies report, for example, outlines past examples of PF activity, including cross-jurisdictional cases.[8] Additionally, FATF's new training and research institute (FATF-TREIN), in Busan, South Korea, may be able to provide support and capacity building for member states on CPF issues. Member states should ensure that their officials working in CPF-related capacities take full advantage of any training opportunities provided by FATF-TREIN.

FATF-style regional bodies, such as the Asia/Pacific Group on Money Laundering (APG), have also offered an ideal venue for these types of discussion. APG has on several occasions held regional training workshops on CPF, focusing on local risks and state experiences in implementing national frameworks or addressing real-time PF cases. These workshops often actively involve the private sector, including FIs and non-governmental experts, in order to bring together the breadth of actors working on CPF in the region.

Bilateral Technical Assistance

A number of foreign governments, including the US, have demonstrated their willingness to provide bilateral technical assistance. As with internationally coordinated technical outreach, bilateral collaboration can help to build a country's capacity to prevent, detect and respond to PF incidents. Other countries may in future offer their own expertise for this purpose.

8. FATF, 'Typologies Report on Proliferation Financing'.

V. Building an Effective Public–Private Partnership on CPF

SUCCESS IN CPF ultimately depends on the extent to which the private sector organisations at the front line of implementation are able to proactively and reactively take relevant action. The capability of private sector actors in CPF is central to overall efforts to stem the flow of finance in support of illicit proliferation: it is FIs that will need to detect and reject proliferation-linked payments, freeze the assets of persons or entities designated on proliferation-related grounds, and carry out due diligence procedures that can help to prevent proliferators from directly or indirectly accessing the formal financial system.

At the same time, private sector actors also have access to a wealth of information that can contribute to a fuller picture of ongoing cases and solidify the legal basis for enforcement action. Financial information relating to specific clients and individual transactions can be combined with other information – including that provided by foreign governments – to aid ongoing investigations. In a broader sense, financial information is also critical to better understanding a country's risk exposure to PF, and the challenges local FIs may face in identifying this particular form of illicit activity. Domestic FIs should thus be viewed as an important partner in any government's efforts to counter PF. Other private sector organisations can play an important role in CPF initiatives too, whether they are logistical providers, exporters or company incorporation secretaries. Each of these may at one point be exposed to PF risks, and it is vital to ensure that they are properly equipped to mitigate and counter this risk.

In order to foster effective public–private partnerships, governments should first understand which domestic private sector organisations are relevant to their CPF initiatives. Their regulated financial sector will be the most important stakeholder, including the insurance industry, which, in many countries, receives less attention than banks in the course of CPF conversations. However, other private sector stakeholders should be considered and involved. As with other forms of financial crime, Designated Non-Financial Businesses and Professions (DNFBPs), such as lawyers, accountants and casinos have the potential to play a role in facilitating PF. Raising their awareness of PF risks and involving them in relevant action to combat them is therefore worthwhile.

Similarly, many countries offer shipping flags of convenience, passports of convenience or the possibility of registering companies with little regulatory oversight – all of which tend to be actively exploited by proliferators. The private sector actors involved in administering and offering such licences therefore need to form an active part of CPF efforts. Equally, as indicated previously, logistical providers, which may make and receive payments related to the physical movement of proliferation-sensitive goods, can also be important to consider from a PF viewpoint, rather than simply an export control perspective. Governments therefore need

to conduct a 'mapping' exercise to determine the domestically registered private sectors that should form part of their public–private outreach.

A comparable exercise should be undertaken to analyse the extent to which domestic CPF regulations apply to relevant private sector organisations. Any gaps, including in regulatory oversight, should be clearly noted and prioritised for further inter-agency action and regulatory development. Approaches to developing legal and regulatory frameworks for CPF are discussed in Chapter II.

An understanding of the landscape of domestic private sector stakeholders should form the core of a national engagement strategy for CPF. Although any public–private engagement strategy on CPF should be tailored to a country's unique circumstances, it should nevertheless feature three key components: general awareness-raising; engagement around legal and regulatory development; and engagement concerning the implementation of CPF requirements.

Recent FATF Mutual Evaluations have shown that in many jurisdictions, financial institutions remain unaware of proliferation threats and uneducated about the need to counter PF. A RUSI study found that even in jurisdictions that have been repeatedly involved in PF, FIs have fundamental misconceptions about the nature of proliferation and related finance.[1] This finding also likely applies to DNFBPs and other relevant sectors. Many continue to conflate the issue with conventional arms trade, or believe that scanning trade documentation for obvious dual-use goods will mitigate all risk. Financial institutions also believe that they are countering PF simply by focusing on sanctions risk, or relying on tools and guidance communicated by governments on other forms of financial crime, such as money laundering or terrorist financing. Consequently, their internal procedures for detecting, analysing and reporting activity specific to PF are deficient.

A core component of public–private engagement strategies should therefore be general awareness-raising around proliferation and the trends and tactics used by those facilitating it. Robust, detailed PF typologies and case studies are likely to be requested by FIs and other private sector organisations that will wish to understand how PF signatures compare with other forms of financial crime. FATF typology and guidance documents on PF serve as a useful starting point,[2] as do reports by independent think tanks and universities.

In some countries, such as Norway and the US, government or law enforcement agencies offer PF training and outreach, including detailed typologies. Several not-for-profit think tanks, universities and private experts also hold extensive expertise in this field and are able to provide

1. Dall, Berger and Keatinge, 'Out of Sight, Out of Mind?', p. 19.
2. FATF typology and guidance documents on PF share many features with typologies covering other forms of financial crime. While some overlap between different forms of financial crime is to be expected, as proliferators will inevitably employ some of the same tactics and evasion techniques, the specific signatures which sets PF apart from these risks should be appreciated.

training for FIs.[3] Where governments conduct their own awareness-raising or issue their own guidance on CPF, they should ensure that it is distinct and separate from that which relates to other financial crimes, that it avoids duplication and that it is useful for financial audiences beyond the banking community.

A second feature of any engagement strategy should involve a two-way dialogue with FIs at the legal and regulatory development phase. When formulating new laws and regulations or amending existing ones, governments should ensure they clearly communicate the need to develop such regulations to relevant financial institutions and private sector organisations. They should also solicit comments and feedback on the proposed legal and regulatory changes to address any potential deficiencies, areas lacking in clarity or possible challenges in implementation that the private sector might face. If potential practical difficulties are identified at the policy design stage, steps can be taken to address them and enhance the overall effectiveness of the CPF regime proposed.

Once an appropriate legal and regulatory framework is in place, governments should conduct extensive outreach surrounding implementation. As a first step, the relevant national agency, such as the FIU, should notify financial institutions of any legal or regulatory changes concerning CPF, including notifications of the adoption of new Security Council Resolutions relating to proliferation. When communicating these developments to FIs, the FIU should ensure all relevant aspects of the change are mentioned. In most recent proliferation-related UN Resolutions, for example, new targeted financial sanctions have been imposed alongside activity-based restrictions on finance. Omission of any aspect can result in significant cases of national non-compliance. It will also be useful for governments to liaise with national banking associations or similar sectoral associations, which may take on the role of communicating new developments in regulatory requirements and guidance to their member organisations.

Rather than identifying individual cases of PF during more comprehensive efforts to mitigate risk, financial institutions need to be able to focus their attention on a systematic effort that is more likely to get to the heart of PF. Broader implementation-focused guidance and training for the private sector is therefore likely to be necessary. Governments and regulators should encourage their FIs to understand PF as an activity that goes beyond sanctions evasion and is not just contained within shortlists of UN-designated entities and individuals. A better understanding of PF at an activity level therefore depends on specific and active outreach from government and a two-way conversation between the public and private sectors.

To promote this conversation, especially in light of the pervasive belief among FIs that they do not have the resources needed to counter PF except through list-based screening, jurisdictions should consider encouraging their financial institutions to take a few relatively simple steps,

3. RUSI has an ongoing research project aiming to further the capability of financial institutions to effectively counter PF. Other institutions include the James Martin Center for Nonproliferation Studies, King's College London and the Center for a New American Security.

which will enhance their overall understanding of PF risk, and provide the building blocks for an effective CPF approach. These measures include:

- Incorporating CPF-related due diligence at the 'on-boarding' stage of a client relationship to promote greater understanding of the nature of the client's business and customers, and in turn enhance the financial institution's understanding of where their potential exposure to PF risk lies within the business.
- Devoting resources to conducting network analysis to better understand individuals and entities linked to designated parties or to parties that the financial institution has already identified as being suspicious for PF reasons.

Regardless of the form of outreach, jurisdictions should be clear and consistent about what they expect their FIs to do in respect to CPF. This includes clarifying which approaches are required elements of a CPF response and which are at the discretion of the institution in accordance with their own risk profile and appetite. For example, jurisdictions could elaborate upon whether and how FIs should determine if a particular item is within the technical capability of the importing nation – a FATF indicator for proliferation finance.[4] Similarly, if they have not already done so, governments should specify that FIs are expected to file STRs when they encounter transactions they suspect are proliferation-related, and that they should outline those suspicions in a particular way.

In recognition of the importance of STRs as a tool to detect and counter PF, national FIUs should evaluate those reports that have contributed to the identification of proliferation-linked transactions. Understanding why FIs flagged these transactions and whether an institution successfully identified a possible connection to proliferation will help to identify outstanding gaps and challenges, as well as areas where current approaches are proving effective. It would also allow relevant government agencies to identify wider proliferation specific trends that could be fed back to FIs for implementation.

This would promote a more detailed public–private discussion of good practices at a time when information sharing on financial crimes, especially PF, is lacking. Due to constraints on the sharing of propriety client information, FIs have access only to the part of a transaction involving their own clients. It may be difficult for FIs to ascertain whether a transaction is related to PF without knowing the full picture. For example, if a UK-based client received a payment from China, the UK bank will have access only to this single transaction. They will not be able to gain further details about the Chinese sender, the nature of their business or what other transactions they have performed. It is such information-sharing limitations which hinder FIs from being more closely involved in efforts to counter financial crime risks in general, and PF specifically. A policy framework for public–private outreach serves as an important starting point to build an effective domestic partnership on CPF that harnesses the potential of the private sector and overcomes this information disconnect.

4. FATF, 'Typologies Report on Proliferation Financing'.

Conclusion

GLOBAL COLLECTIVE ACTION by states is necessary if CPF risks are to be mitigated. Proliferators have proved adept in exploiting gaps in national legal and institutional frameworks to achieve their illicit aims. Their networks can be complex and sophisticated and their methods fluid and shrewd. Meanwhile, governments have struggled with understanding their proliferation risks and coordinating institutional efforts, both domestically and internationally, to combat the crime. As highlighted in this paper, gaps in legal frameworks pose serious obstacles in achieving the successful prosecution of proliferation financiers.

With careful attention to policy development and domestic coordination mechanisms, governments can develop legal frameworks that are effective in implementing international CPF obligations and relevant FATF Recommendations. The practical guidance in this paper, together with the model legislative provisions contained in the Annex, aims to provide governments with the building blocks of an effective and comprehensive CPF regime.

Financial institutions have also shown vulnerabilities in their understanding of proliferation financing, resulting in the limited adoption of institutional mitigation measures. RUSI's two complementary guidance papers on CPF have sought to equip governments and financial institutions alike with the tools they need to strengthen their responses to CPF. Together, the guides also highlight and encourage the strong public–private collaboration that is necessary to give effect to international CPF obligations and safeguard the financial sector against abuse.

Annex: Model Provisions to Combat the Financing of the Proliferation of Weapons of Mass Destruction

Notes on Using These Model Provisions

These model provisions are aimed at assisting states to develop or amend their legislative framework to comply with international obligations and standards to implement financial measures to combat the proliferation of weapons of mass destruction. The provisions are based on relevant UN Security Council resolutions and the Financial Action Task Force (FATF) Recommendations.

The model provisions are intended to be a legal policy and legislative drafting resource. The provisions are drafted in a style that will be familiar to common law jurisdictions. However, the model provisions are nevertheless useful for civil law jurisdictions in understanding the legal requirements. States should take care to adapt the underlying concepts and specific language to accord with constitutional and fundamental legal principles in their legal systems. Specific notes are included throughout this text (in text boxes) to provide further guidance or to highlight issues for consideration. Where there is text in brackets, states need to insert relevant domestic references.

The international obligations on proliferation financing contain a range of different measures, from targeted financial sanctions, to activity-based prohibitions, to vigilance measures. Therefore, it is probable – depending on a state's existing laws – that more than one piece of legislation may be required to implement the various international obligations. Examples of legislation that could integrate proliferation financing provisions include: anti-money laundering/counterterrorist finance (AML/CTF) laws; criminal or penal codes or laws; UN sanctions laws; counterterrorism or security laws; counter proliferation of WMD laws; and customs, trade or export control laws.

Some countries have taken the approach of adopting a law that implements Article 41 of the UN Charter regarding measures not involving the use of armed force and subsequently adopting regulations that address the different requirements of each UN Security Council Resolution imposing sanctions. This approach creates a flexible framework that can capture all sanctions obligations under one umbrella. Given that regulations can be easily amended, it also enables countries to keep their domestic laws in compliance with changing international obligations. It should be noted that while a single UN Charter law brings legal obligations under one umbrella,

a number of agencies will nevertheless be involved in its implementation. Strong inter-agency coordination will be vital to successful implementation.

When deciding which law/s should incorporate counter proliferation financing provisions or whether an entirely new law should be developed, countries should first undertake a mapping exercise to identify all relevant existing legislation.

We welcome feedback on these model provisions in order to continue to improve them. Feedback can be directed to:

Anagha Joshi: anniej@poetic.com

Tom Keatinge: TomK@rusi.org

List of Provisions

Chapter I: Preliminary **46**
1. Object of the Act 46
2. Entry into force 46
3. Application 46
4. Application of the [criminal code] 47
5. Act to bind the State 47
6. Definitions 47

Chapter II: Proliferation financing **57**
7. Offence of Proliferation financing 57

Chapter III: Targeted financial sanctions **59**

Part I: Designation Process **59**
8. Designations by the United Nations Security Council relating to Iran 59
9. Designations by the United Nations Security Council relating to DPRK 59
10. Designation by the [minister] relating to DPRK 60
11. Duration of [minister's] designation 61
12. Revocation of [minister's] designation 61
13. Judicial review 61
14. Notification of designations and revocations 62
15. Notice of designation to a designated person or entity 63

Part II: Prohibitions **64**
16. Prohibition against dealing with assets 64
17. Prohibition against making assets available 65
18. Prohibition on joint ventures with designated persons and entities of DPRK 66

Part III: Seizure of frozen assets **67**
19. Court may grant order for seizure of frozen assets 67

Chapter IV: Other financial measures relating to DPRK **68**
20. Prohibition on financing related to DPRK 68
21. Prohibition on financial transactions related to DPRK 69
22. Prohibition on trade with DPRK 70
23. Prohibition on relationships with DPRK financial institutions 71
24. Prohibition on maintaining offices in DPRK 71
25. Prohibition on maintaining offices in [State] 72
26. Prohibition on accounts related to DPRK missions 72
27. Prohibition against financial transactions related to professional or commercial activities 73
28. Prohibition against use of real property 73

29. Prohibition relating to vessels 74
30. Prohibition relating to vessels and aircraft 74

Chapter V: Other financial measures relating to Iran 76
31. Prohibition on financing related to Iran 76
32. Prohibition on financial transactions related to Iran 77
33. Prohibition on commercial activities 78

Chapter VI: Cross-border transportation of cash, precious metals and precious stones 79

Chapter VII: Preventative measures for financial institutions and DNFBPs 80

Chapter VIII: Reporting obligations 81
34. Reporting obligations not limited 81
35. Request to verify 81
36. Obligation to report the assets of a designated person or entity 81
37. Obligation to report suspicious transactions 82
38. Prohibition against disclosing report, information or suspicion 84
39. Enhanced reporting obligations related to DPRK 85

Chapter IX: Administration of the Act 87

Part I: Functions and powers of the [minister] 87
40. Authorisations by the [minister] 87
41. Annual report 90
42. Report to United Nations Security Council or its Committees 90
43. Power to request information and documents 90
44. Production of documents 91
45. Failure to comply with a request for information or documents 91
46. Information to be confidential 92
47. Disclosure of information by the [minister] 92
48. Communications from foreign governments 92
49. Power to make regulations 92
50. Delegation of authority 93

Part II: Sanctions Secretariat 93
51. Sanctions Secretariat 93

Part III: National Coordinating Committee 94
52. [National coordinating committee] on counter-proliferation financing 94
53. Functions of the [national coordinating committee] 95

Chapter X: Supervision and enforcement **96**

Part I: Supervision **96**
54. Appointment of supervisors 96
55. Functions of supervisors 96
56. Delegation of authority 97

Part II: Powers of supervisors **97**
57. Power to request information and documents 97
58. Production of documents 97
59. Power to conduct on-site inspections 98
60. Failure to comply with a request for information or documents 98
61. Information to be confidential 99
62. Disclosure of information by a supervisor 99

Part III: Enforcement **100**
63. Enforcement measures 100
64. Infringement notice 100
65. Enforceable undertaking 101
66. Enforcement of undertaking 101
67. Performance injunctions 101

Chapter XI: Miscellaneous **103**
68. Protection from liability for acts done in good faith 103
69. Immunity of State 103
70. Imputing conduct to bodies corporate 103
71. Liability of officers of bodies corporate 103

Schedule 1: United Nations Security Council Resolutions **105**

Schedule 2: United Nations Security Council Resolutions related to Iran **106**

Schedule 3: United Nations Security Council Resolutions related to DPRK **107**

AN ACT

Entitled

Counter Proliferation Financing Act [year]

Being an Act to provide for financial measures to prevent the proliferation of weapons of mass destruction,

Made by the [name of enactor/method of enactment].

Chapter I: Preliminary

1. Object of the Act

The object of this Act is to:

(a) protect the national interest and promote the security of [State] and its citizens by preventing the proliferation of weapons of mass destruction; and
(b) give effect to Article 41 of the Charter of the United Nations by implementing financial measures arising from United Nations Security Council Resolutions listed in Schedule 1 or prescribed by Regulations; and
(c) protect fundamental rights and freedoms through robust procedural safeguards.

States should insert their country name in Paragraph (a).

2. Entry into force

This Act shall enter into force on [date/gazettal].

3. Application

This Act applies:

(a) in [State]; and
(b) to all citizens of [State] and bodies corporate incorporated under a law of [State] wherever located; and
(c) to a vessel flying the flag of [State]; and
(d) to an aircraft registered in [State]; and
(e) to an offence committed on board a vessel flying the flag of [State] or an aircraft registered in [State] wherever located.

States should ensure that the Act applies to any external territories.

States should ensure that they are able to apply this Act to vessels, which are flagged, and aircraft, which are registered, by the state. In some states, this may be implicit in Paragraph (a) and therefore Paragraphs (c) and (d) are not required.

Paragraph (e) may not be required where the extension of enforcement jurisdiction is already provided by the criminal or penal law of the state and therefore covered by Section 4. Where the criminal or penal law of a state does not extend such enforcement jurisdiction over vessels and aircraft, states should include Section 3(1)(e). Section 3(1)(e) extends jurisdiction over offences committed on board a state's flagged vessel or registered aircraft wherever located. This is mainly relevant to situations where the vessel or aircraft is on or over the high seas to ensure that there is not a gap in legal coverage. It should be noted that where a vessel or aircraft that is flagged/registered by one state is located in the territory of another state, the other state will have concurrent jurisdiction. The jurisdiction of the flag-state or state of registration is not exclusive. These issues of jurisdiction are governed by international law and states may wish to seek specific legal advice on this point to clarify the application of laws.

4. Application of the [criminal code]

The [criminal code] applies to all offences under this Act.

States should insert a reference to the relevant criminal or penal law.

The broader framework of a state's criminal or penal law should apply to offences under this Act. In particular, states should ensure that ancillary offences are provided for each offence in this Act. Ancillary offences are variously described across different states but should include the equivalent of 'attempt', 'participate as an accomplice in', 'incite', 'conspire to commit' and 'direct'.

Given the transnational nature of proliferation of WMD activities and their financing, states should also ensure that broad heads of jurisdiction apply to criminal offences under this Act. Note, in particular, the comment above regarding extending jurisdiction to cover offences on-board vessels and aircraft.

5. Act to bind the State

This Act binds the State.

6. Definitions

(1) The following definitions apply for the purpose of this Act:

"account" includes:

(a) any facility or arrangement under which a financial institution:
  (i) accepts deposit of an asset; or
  (ii) allows withdrawal or transfer of an asset; or
  (iii) pays, collects or draws on a bearer negotiable instrument on behalf of any other person; or
  (iv) supplies a safety deposit box or any other form of safe deposit; and
(b) any account that is closed or inactive, or that has a nil balance;

"aircraft" means any machine or craft that can derive support in the atmosphere from the reactions of the air, other than the reactions of the air against the earth's surface;

States should ensure that the definition of 'aircraft' corresponds with their national aviation legislation.

"arms or related materiel" includes:

(a) weapons; and
(b) ammunition; and
(c) military vehicles and equipment, including:
  (i) battle tanks; and
  (ii) armoured combat vehicles; and
  (iii) large calibre artillery systems; and
  (iv) combat aircraft; and
  (v) attack helicopters; and
  (vi) warships; and
  (vii) missiles and missile systems,

which have the same meanings as they have for the purposes of reports by member States to the United Nations Register of Conventional Arms established under United Nations General Assembly Resolution A/RES/46/36L of 6 December 1991; and

(d) spare parts and accessories for the items mentioned in Paragraph (a), (b) or (c); and
(e) paramilitary equipment, including:
  (i) batons, clubs, riot sticks and similar devices of a kind used for law enforcement purposes; and
  (ii) tear gas and other riot control agents; and
  (iii) body armour, bullet resistant apparel and helmets; and
  (iv) handcuffs, leg-irons and other devices used for restraining prisoners; and
  (v) riot protection shields; and
  (vi) whips; and
  (vii) parts and accessories designed or adapted for use in, or with, equipment mentioned in Paragraphs (i) to (vi);

"asset" means funds, property, financial resources and economic resources of every kind, whether tangible or intangible, corporeal or incorporeal, moveable or immovable, actual or potential, however acquired, including:

(a) currency, precious metals, precious stones and other financial resources; and
(b) real property, chattels and vessels; and
(c) natural resources, human resources and other economic resources that may be used to obtain funds, goods or services; and
(d) legal documents or instruments in any form, including electronic or digital, evidencing title to, or interest in, or right to claim such asset, including bank credits, travellers cheques, bank cheques, money orders, shares, securities, bonds, drafts, and letters of credit; and
(e) any interest, dividends, income or value accruing from, generated by, or derived from such asset;

In relation to the reference to 'vessels' in Paragraph (b), states should note that Annex III of UN Security Council Resolution 2270 on DPRK provides a list of Ocean Maritime Management Co (OMM) vessels that must be covered by the prohibition against dealing with assets in Section 16.

"authorisation" means a permission granted by the [minister] to undertake an act or make an omission that is otherwise prohibited by this Act and can include conditions imposed on the permission;

"ballistic missile-related goods" means items, materials, equipment or technology:

(a) listed in Security Council document S/2015/546; or
(b) that could contribute to ballistic missile-related programmes or weapons of mass destruction delivery systems and are prescribed by Regulations;

References are made throughout this Act to documents produced by international organisations that provide a list of goods. These documents are regularly updated. It is recommended that states consider listing these documents in subsidiary legal instruments, for example, by prescribing them in Regulations, to allow them to be quickly updated as needed. The documents are listed on the face of this Act only for ease of reference.

UN Security Council Resolutions on Iran and DPRK require states to determine other items that could contribute to ballistic missile or WMD-related programmes. Paragraph (b) allows a state to list additional such items in Regulations.

"basic expense" means an expense necessarily incurred for any of the following purposes:

(a) obtaining foodstuffs;
(b) paying rent or mortgage;

(c) obtaining medicine or medical treatment;
(d) paying taxes;
(e) paying insurance premiums;
(f) paying utility charges;
(g) paying reasonable professional fees;
(h) paying reasonable expenses associated with the provision of legal services;
    (i) paying fees or service charges that are in accordance with the laws of [State] for the routine holding or maintenance of a frozen asset;
    (ii) any other similar purpose;

"biological weapon" means any agent, toxin, weapon, equipment, or means of delivery mentioned in Article 1 of the Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on their Destruction, of 10 April 1972;

"chemical weapon" has the same meaning as in Article II of the Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their Destruction, of 3 September 1992;

Note that the definition in Article II of the Convention includes components of chemical weapons and means of delivery, together or separately.

"Consolidated List" means the list of all designated persons and entities maintained by the Sanctions Secretariat under Paragraph 51(2)(b);

"consular officer" has the same meaning as in Article 1(1)(d) of the Vienna Convention on Consular Relations, of 24 April 1963;

"contractual obligation" means an obligation whereby a payment is required under a contract or agreement made before the date of the designation and where the payment required does not violate the requirements of a United Nations Security Council Resolution listed in Schedule 1;

"control" means exercising influence, authority or power over decisions about financial or operating policies, and includes control as a result of, or by means of, trusts, agreements, arrangements, understandings or practices, whether or not having legal or equitable force and whether or not based on legal or equitable rights, and "controlled" has a corresponding meaning;

"correspondent relationship" means a relationship that involves the provision of banking or currency or value transfer services by one financial institution (the "**correspondent"**) to another financial institution (the "**respondent"**) where:

(a) the correspondent carries on a banking or currency or value transfer business at or through a permanent place of business in one country; and

(b) the respondent carries on a banking or currency or value transfer business at or through a permanent place of business in another country; and
(c) the relationship between the correspondent and the respondent relates, in whole or in part, to the provision of banking or currency or value transfer services between those permanent places of business;

"court" means the [relevant court];

States should specify a court of competent jurisdiction.

"crew service" means a service providing:
(a) flight or cabin crew for a vessel or aircraft; or
(b) a person to travel on board a vessel or aircraft for any purpose relating to the vessel or aircraft's operation; or
(c) a person to travel on board a vessel or aircraft to examine the qualifications or competency of flight or cabin crew;

States should ensure that the definition of 'crew service' corresponds with their national maritime and aviation legislation.

"deal" includes sale, supply, lease, transfer, conversion, disposition, movement or use, and "dealing" and "dealt" have the same meaning;

"designated person or entity" means a person or entity:
(a) designated by the [minister] under Section 10; or
(b) whose designation has been extended by the [minister] under Section 11; or
(c) designated by the United Nations Security Council or its Committees pursuant to a Resolution listed in Schedule 2 or 3 or prescribed by Regulations;

"diplomatic agent" has the same meaning as in Article I(e) of the Vienna Convention on Diplomatic Relations, of 18 April 1961;

"DNFBP" means a designated non-financial business or profession in [State], that is:
(a) a person or entity that conducts any of the following activities:
    (i) providing a gaming, junket or other related casino service;
    (ii) acting as a professional intermediary in a real estate transaction;
    (iii) dealing in precious metals;
    (iv) dealing in precious stones;
    (v) providing a trust or company service; or

(b) an accountant, a lawyer, a notary public, or other independent legal professional when preparing for, engaging in, or carrying out a transaction for a client concerning any of the following activities:
  (i) buying or selling real estate;
  (ii) managing client currency, securities or other assets;
  (iii) managing a bank, savings or securities account;
  (iv) organising contributions for the creation, operation or management of a body corporate;
  (v) creating, operating or managing a body corporate or unincorporated entity;
  (vi) buying and selling businesses;

States should ensure that the definition of 'DNFBP' is consistent with the definition of the same in each state's anti-money laundering and counterterrorist finance (AML/CTF) legislation.

"DPRK" means the Democratic People's Republic of Korea;

"DPRK financial institution" means a person or entity, wherever located, that conducts an activity listed in Paragraphs (a) to (m) of the definition of financial institution and that is:
(a) regulated, registered, incorporated or licensed under any law of DPRK; or
(b) owned or controlled by DPRK;

Paragraph (a) of the definition of "DPRK financial institution" should cover a range of persons and entities that are in some way regulated, registered, incorporated or licensed under any DPRK law where that person or entity conducts any of the activities listed in the definition of "financial institution". For example, Paragraph (a) would cover a company (not necessarily a bank) incorporated in DPRK that conducts any of the activities listed in the definition of "financial institution".

"DPRK flagged vessel" means a vessel:
(a) regulated, registered or licensed under a law of DPRK; or
(b) owned or controlled by DPRK;

"entity" includes any unincorporated body, group, association, organisation, institution or arrangement;

"extraordinary expense" means any payment which is not a basic expense or a contractual obligation that the [minister] considers:
(a) to be necessary; and
(b) does not violate the requirements of a United Nations Security Council Resolution listed in Schedule 1 or prescribed by Regulations;

"financial institution" means any person or entity that conducts in [State] any of the following activities for or on behalf of a customer:

(a) acceptance of deposits and other repayable funds from the public, including private banking;
(b) lending, including consumer credit, mortgage credit, factoring (with or without recourse), and financing of commercial transactions, including forfeiting;
(c) financial leasing other than in respect of arrangements relating to consumer products;
(d) the transfer of currency or value;
(e) issuing or managing means of payment, including credit and debit cards, cheques, travellers' cheques, money orders and bankers' drafts, and currency in non-physical form;
(f) issuing financial guarantees or commitments;
(g) trading in:
    (i) money market instruments;
    (ii) bearer negotiable instruments;
    (iii) foreign exchange;
    (iv) exchange, interest rate or index instruments;
    (v) transferable securities;
    (vi) commodity futures;
(h) participation in securities issues or the provision of financial services related to such issues;
(i) individual or collective portfolio management;
(j) safekeeping or administration of physical currency, bearer negotiable instruments or liquid securities on behalf of other persons;
(k) investing, administering or managing assets on behalf of other persons;
(l) providing an insurance service;
(m) currency changing;

The definition of 'financial institution' should be consistent with the definition of the same in each state's AML/CTF legislation.

"financial service" means any activity listed in:

(a) Paragraphs (a) to (m) of the definition of financial institution; or
(b) Paragraphs (a)(i) to (v) of the definition of DNFBP; or
(c) Paragraphs (b)(i) to (vi) of the definition of DNFBP; or
(d) the provision of consultancy, training or advisory services related to the activities in Paragraph (a), (b) or (c);

"frozen asset" means an asset which cannot be dealt with due to the prohibition imposed under Section 16;

"insurance service" means a service providing an undertaking or commitment under which a person is obliged, in return for payment, to provide another person, in the event of materialisation of a risk, with an indemnity or a benefit as determined by the undertaking or commitment, and includes underwriting insurance, placement of insurance and providing an insurance brokerage or other insurance intermediation service;

"Iran" means the Islamic Republic of Iran;

"Joint Comprehensive Plan of Action" means the Joint Comprehensive Plan of Action that is attached as Annex A to United Nations Security Council Resolution 2231;

"joint venture" means an arrangement between two or more persons or entities to cooperate on a project, initiative, business or activity, whether or not that arrangement has legal or equitable force or is based on legal or equitable rights;

"[minister]" means [relevant minister];

> The powers given to the minister, particularly the power to designate persons and entities, has a significant impact on the rights of persons. As such, it is recommended that the relevant authority is a minister or other senior official. Another option to protect against possible abuse of power could be to nominate a committee or council of senior officials so that the power is not vested in a single person, so long as the committee or council can operate and make decisions efficiently.

"nuclear weapon" means any weapon that derives its destructive force from nuclear reactions and any explosive device capable of releasing nuclear energy, irrespective of the purpose for which it could be used, whether assembled, partly assembled, or unassembled;

> The definition seeks to cover component parts of nuclear weapons and means of delivery of nuclear weapons, regardless of the purpose of the item and whether the items are assembled or unassembled.

"own" means having a legal entitlement, either directly or indirectly, to 25% or more of a body corporate or entity, and "owned", "ownership" and "owning" have corresponding meanings;

"person" means any natural person or body corporate;

"representative office" means a business office that is established by a body corporate in a foreign country, where the body corporate is not licensed to operate, to conduct marketing operations;

"Sanctions Secretariat" means the Sanctions Secretariat established under Section 51;

"subsidiary" means a body corporate with voting stock that is owned or controlled by another body corporate;

"vessel" means any kind of vessel used in navigation by water, however propelled or moved, and includes the following:

(a) a barge, lighter or other floating craft; and
(b) an air-cushion vehicle, or other similar craft, used wholly or primarily in navigation by water;

States should ensure that the definition of 'vessel' corresponds with their national maritime legislation.

"weapons of mass destruction related material" means items, materials, equipment, goods, or technology:

(a) listed in any of the following documents:
    (i) Security Council document S/2006/814;
    (ii) Security Council document S/2006/815;
    (iii) Security Council document S/2006/853;
    (iv) Security Council document S/2006/853/CORR.1;
    (v) Security Council document S/2009/205;
    (vi) Security Council document S/2013/136;
    (vii) International Atomic Energy Agency document INFCIRC/254/Rev.9/Part 1a;
    (viii) International Atomic Energy Agency document INFCIRC/254/Rev.7/Part 2a;
    (ix) Annex III to United Nations Security Council Resolution 2321; or
(b) that could contribute to DPRK's nuclear-related, ballistic missile-related or weapons of mass destruction-related programmes and are the subject of a determination made by the United Nations Security Council or its Committees under Paragraph 8(a)(ii) of United Nations Security Council Resolution 1718 that has not ceased to have effect; or
(c) that are dual-use conventional arms and are the subject of a determination made under Paragraph 7 of United Nations Security Council Resolution 2321; or
(d) that could contribute to weapons of mass destruction-related programmes and are prescribed by Regulations.

UN Security Council Resolutions on DPRK require states to determine other dual-use items that could contribute to WMD programmes. Paragraph (d) allows a state to list or specify additional items in Regulations. Paragraph (d) also implements catch-all provisions of UN Security Council Resolutions on Iran that cover items that have been prohibited from transfer by states under UN Security Council Resolutions that specify such action is required on the basis of possession of information that provides reasonable grounds to believe they are intended for a prohibited program.

(2) For the purpose of a "DNFBP" defined in this section, a **"trust or company service"** includes any of the following:
   (a) forming, registering or managing a body corporate or unincorporated legal entity;
   (b) acting as, or arranging for another person to act as, a director or secretary of a company, the partner of a partnership or a similar position in relation to a body corporate or unincorporated legal entity;
   (c) providing a registered office, business address, correspondence address or accommodation for a body corporate or unincorporated legal entity;
   (d) acting as, or arranging for another person to act as, a trustee of an express trust or the equivalent function for another unincorporated legal entity;
   (e) acting as, or arranging for another person to act as, a nominee shareholder for another person.

(3) For the purpose of a "trust or company service" mentioned in Subsection (2), an **"unincorporated legal entity"** includes any unincorporated foundation, association, partnership, undertaking, or legal arrangement, such as a trust, that has certain legal rights and obligations.

Chapter II: Proliferation financing

7. Offence of Proliferation financing

(1) A person must not engage in conduct specified in Subsection (5) knowing that, or reckless as to whether, the conduct relates to an activity specified in Subsection (7).

(2) A person who contravenes Subsection (1) is guilty of an offence.

Penalty:

(a) if the offender is a natural person – a fine not exceeding [xx] or imprisonment for a period not exceeding [xx] or both; or
(b) if the offender is a body corporate – a fine not exceeding [xx].

(3) A person commits an offence under Subsection (2) even if an activity specified in Subsection (7) does not occur or is not attempted.

(4) Subsection (2) does not apply if the person has engaged in conduct for which an authorisation has been granted under Section 40.

(5) The following conduct is specified for the purpose of Subsection (1):

(a) collecting, providing or managing an asset; or
(b) providing advice related to the activities in Paragraph (a); or
(c) providing a financial service; or
(d) conducting a financial transaction.

(6) For the purpose of Paragraph 5(d):

(a) a person conducts a financial transaction if the person is a party to the transaction or procures or facilitates the transaction; and
(b) a transaction can be made by any means, including electronic or physical transfer of an asset.

(7) For the purpose of Subsection (1), the activities specified are:

(a) the manufacture, production, possession, acquisition, stockpiling, storage, development, transportation, sale, supply, transfer, export, transhipment or use of:
    (i) nuclear weapons; or
    (ii) chemical weapons; or
    (iii) biological weapons; or
    (iv) materials related to nuclear weapons, chemical weapons or biological weapons that are prescribed by Regulations; or
(b) the provision of technical training, advice, service, brokering or assistance related to any of the activities in Paragraph (a).

This provision seeks to implement the financial aspects of Operative Paragraphs (OP) (2) and (3)(d) of UN Security Council Resolution 1540. These provisions extend the prohibitions against financing to cover the proliferation activities of non-state actors.

The terms 'nuclear weapons', 'chemical weapons' and 'biological weapons' used in Subsection (7) are each defined terms in this Act. States should note that each definition includes not only the weapons themselves, but also their component parts and means of delivery. States should give careful attention to all materials captured by these definitions.

OP 3(d) of UN Security Council Resolution 1540 requires the implementation of export controls, which extends beyond nuclear, biological and chemical weapons to also cover "related materials". In the absence of an export control regime in these model provisions, Subsection (7)(d) includes a reference to "related materials prescribed by Regulations", which should specify the range of export-controlled items.

States should ensure that the offences in this Act constitute predicate offences to money laundering. States have different approaches to specifying predicate offences to money laundering. Some states list specific offences as predicate offences, other states apply a threshold penalty approach, that is, all offences above a certain penalty threshold constitute predicate offences to money laundering. States should use the appropriate legal method in their jurisdiction to capture the offences in this Act as a predicate offences.

Chapter III: Targeted financial sanctions

The requirements for implementing targeted financial sanctions relating to proliferation of WMD are very similar to those relating to terrorism. States may consider combining targeted financial sanctions for both terrorism and proliferation into a single regime.

Part I: Designation Process

8. Designations by the United Nations Security Council relating to Iran

(1) A designation of a person or entity by the United Nations Security Council or its Committees under a Resolution listed in Schedule 2 or prescribed by Regulations shall:
    (a) have immediate application in [State]; and
    (b) have the immediate effect of imposing the prohibitions in Sections 16 and 17; and
    (c) shall continue in force until:
        (i) it expires under Subsection (2); or
        (ii) it is revoked by the United Nations Security Council or its Committees.

(2) A designation under Subsection (1) shall expire on 18 October 2023 unless otherwise decided by the United Nations Security Council.

The date of 18 October 2023 is eight years after the Joint Comprehensive Plan of Action Adoption Day. This time limit is imposed by UN Security Council Resolution 2231, OP 6(c). States should note that two potential decisions could occur at the international level that would impact on this timeframe. Firstly, the UN Security Council could find that there has been a failure by Iran to comply with the Joint Comprehensive Plan of Action, in which case the targeted financial sanctions would continue to apply indefinitely. Alternatively, the International Atomic Energy Agency (IAEA) could find that all nuclear activities in Iran remain peaceful, in which case, the IAEA would provide a report to the UN Security Council which would need to make a determination that the targeted financial sanctions would no longer continue to apply. States should monitor decisions of the UN Security Council and IAEA to determine whether changes to the legislation are required to implement those decisions if they are made.

9. Designations by the United Nations Security Council relating to DPRK

(1) A designation of a person or entity by the United Nations Security Council or its Committees under a Resolution listed in Schedule 3 or prescribed by Regulations shall:
    (a) have immediate application in [State]; and
    (b) have the immediate effect of imposing the prohibitions in Sections 16, 17 and 18; and

(c) shall continue in force until it is revoked by the United Nations Security Council or its Committees.

10. Designation by the [minister] relating to DPRK

(1) The [minister] must designate an entity where there are reasonable grounds to believe that:
  (a) the entity is any of the following:
    (i) an entity of the Government of DPRK;
    (ii) an entity of the Workers' Party of DPRK;
    (iii) is owned or controlled, directly or indirectly, by an entity mentioned in Subparagraph (i) or (ii);
    (iv) is acting on behalf of, or at the direction of, an entity mentioned in Subparagraph (i) or (ii); and
  (b) the entity is or has been involved in an activity listed in Subsection (2).

(2) The following activities are specified for the purpose of Subsection (1):
  (a) activities prohibited under Chapter IV; or
  (b) activities related to DPRK's weapons of mass destruction or ballistic missile-related programmes; or
  (c) other activities prohibited by a United Nations Security Council Resolution listed in Schedule 3 or prescribed by Regulations; or
  (d) attempting, participating in or facilitating activities in Paragraphs (a), (b) or (c).

(3) The [minister] must take into consideration any relevant communication from a foreign government or the United Nations Security Council or its Committees when deciding whether an entity should be designated.

(4) The [minister's] designation of an entity has immediate application in [State].

(5) The [minister's] designation of an entity has the immediate effect of imposing the prohibitions under Sections 16, 17 and 18.

This section gives effect to OP 32 of UN Security Council Resolution 2270. The domestic designation process is very similar to the domestic designation process required by Resolution 1373 related to terrorism, although the grounds for designation here are far more specific and relate only to DPRK. States should consider whether the domestic designation process for DPRK, and the subsequent notification and other procedural requirements for DPRK, should be contained in one piece of legislation together with the domestic designation process for terrorism pursuant to Resolution 1373. This would enable states to utilise authorities and mechanisms already in placed and implemented for the purposes of Resolution 1373.

11. Duration of [minister's] designation

(1) A designation made by the [minister] under Section 10 shall continue in force until:
    (a) it expires under Subsection (2); or
    (b) it is revoked by the [minister] under Section 12.

(2) A designation expires [3] years after the date on which it was made.

(3) The [minister] may extend the duration of a designation at any time before the designation expires if the Minister continues to be satisfied that the grounds for designation in Section 10 are met.

(4) A designation that has been extended by the [minister] under Subsection (3) expires [3] years after the date on which the extension was made.

(5) There is no limit to the number of times the [minister] can extend a designation.

States should choose a time period for expiry of a designation. The expiration of designations forces periodic reconsideration of the grounds for designation. This is a procedural safeguard to protect individual rights.

12. Revocation of [minister's] designation

(1) The [minister] may revoke a designation prior to its expiry if the [minister] reasonably believes that the grounds for designation under Section 10 are no longer met.

(2) The revocation of a designation shall have immediate application in [State].

13. Judicial review

(1) Nothing in this Act limits a person's right to seek [judicial review] of a designation by the [minister].

(2) The [court] may consider material in closed proceedings, and in the absence of the designated person or entity and their legal representative, where disclosure of the material would prejudice national security.

In relation to the reference to 'judicial review', it is recommended that states identify the relevant terminology for a review enabling a court to consider whether a legal error has been made.

In relation to Paragraph (2), states should adopt language consistent with the powers of the relevant court to consider material in closed proceedings, taking into account human rights and constitutional protections.

14. Notification of designations and revocations

(1) The [minister] must, without delay, use any necessary means to notify persons specified in Subsection (2) if:
   (a) a designation or revocation is made by the United Nations Security Council or its Committees under United Nations Security Council Resolutions listed in Schedule 2 or 3 or prescribed by Regulations; or
   (b) a designation is made by the [minister] under Section 10; or
   (c) a revocation is made by the [minister] under Section 12; or
   (d) a designation has expired under Section 11(2) or (4).

(2) The following persons are specified for the purpose of Subsection (1):
   (a) a financial institution or DNFBP who has a reporting obligation under this Act [or the law on anti-money laundering and counter-terrorist financing]; and
   (b) any other person or entity considered necessary by the [minister], other than the designated person or entity.

The reference in Paragraph (a) to 'the law on anti-money laundering and counter-terrorist financing' refers to a state's legislation regulating financial institutions and DNFBPs for compliance with AML/CTF requirements.

Depending on whether you choose to put reporting obligations for financial institutions and DNFBPs in this Act or in AML/CTF legislation, the reference here should be to the appropriate law. Refer to comments on 'reporting obligations' below.

(3) The [minister] must, as soon as reasonably practicable, publish in any manner considered appropriate:
   (a) a designation or revocation made by the United Nations Security Council or its Committees under a United Nations Security Council Resolution listed in Schedule 2 or 3 or prescribed by Regulations; or
   (b) a designation made by the [minister] under Section 10; or
   (c) a revocation made by the [minister] under Section 12; or
   (d) the expiry of a designation under Section 11(2) or (4).

States should note that pursuant to Sections 8, 9 and 10, decisions of the UN Security Council or the [minister] to designate persons or entities have the immediate effect of imposing the prohibitions in Sections 16, 17 and 18. No other administrative process is required for those decisions to have legal effect. Section 14 recognises that in practice some form of communication of the UN Security Council or the [minister's] decision should take place and therefore outlines a possible communication process. However, legal obligations are imposed by the making of the decision, not by the communication of that decision. To promote compliance with the legal obligations, FATF recommends that these decisions are notified 'without delay' to financial institutions and DNFBPs.

15. Notice of designation to a designated person or entity

(1) The [minister] must, within a reasonable time, make reasonable efforts to give written notice of their designation to:
    (a) a person or entity designated by the [minister] under Section 10; and
    (b) a person or entity designated by the United Nations Security Council or its Committees under a United Nations Security Council Resolution listed in Schedule 2 or 3 or prescribed by Regulations if that person or entity is located within the territory of [State]; and
    (c) a person designated by the United Nations Security Council or its Committees under United Nations Security Council Resolutions listed in Schedule 2 or 3 or prescribed by Regulations if that person is a national of [State]; and
    (d) a person designated by the United Nations Security Council or its Committees under United Nations Security Council Resolutions listed in Schedule 2 or 3 or prescribed by Regulations if that person is a body corporate incorporated under a law of [State].

(2) The notice in Subsection (1) must contain the following matters as applicable:
    (a) the grounds for designation; and
    (b) the information relied on in making the designation, with the exception of information that, in the opinion of the [minister] acting reasonably, should not be disclosed on the grounds that [it would prejudice national security]; and
    (c) the duration of the designation; and
    (d) details of the prohibitions imposed; and
    (e) avenues to appeal the designation; and
    (f) the right to seek [judicial review] of the designation; and
    (g) information on the procedure for making an application for an authorisation under Section 40.

The language in Paragraph (2)(b) should reflect the legal basis on which your government can withhold information from the public. The phrase 'prejudice national security' is used in a number of states.

A three-stage process for notification is contemplated by Section 15. Firstly, without delay financial institutions, DNFBPs and any other person that is suspected of holding the asset of a designated person or entity should be notified. This notification should be carried out in a manner that does not alert the designated person or entity or allow the assets to dissipate. Secondly, it is recommended that information regarding designations and revocations is publicly available in some form, for example on an official website of the Sanctions Secretariat. This should take place only after the specific notice to financial institutions, DNFBPs and other relevant persons. Thirdly, and lastly, reasonable efforts should be made to notify persons and entities designated by the [minister], or designated by the UN Security Council or its Committees and who are located in your state or are nationals of your state. Where a designated person or entity is located in your state, the state has obligations to inform designated persons or entities of their rights – for example, the right to authorised access to assets or a right to judicial review of the [minister's] decision, among others. This is the basis of the third limb of the notification process.

Part II: Prohibitions

For all offences in this Act, 'knowledge' should be able to be inferred from objective factual circumstances. This is a common law principle that exists in many states. However, it may be the practice in some states that a provision needs to be included in every offence that knowledge can be inferred from objective factual circumstances. Without this principle, this mental element of the offence would be very difficult to prove.

16. Prohibition against dealing with assets

(1) A person must not deal with an asset knowing that, or reckless as to whether, the asset is owned, controlled or held, directly or indirectly, wholly or jointly, by:
    (a) a designated person or entity; or
    (b) on behalf of a designated person or entity; or
    (c) at the direction of a designated person or entity.

(2) A person who contravenes Subsection (1) is guilty of an offence.

    Penalty:

(a) if the offender is a natural person – a fine not exceeding [xx] or imprisonment for a term not exceeding [xx] years or both; or
(b) if the offender is a body corporate – a fine not exceeding [xx] or an amount equivalent to the value of the asset, whichever is greater.

(3) For the avoidance of doubt, Subsection (1) applies to any and all assets of persons and entities listed in Subsection (1) and is not limited to assets related to a specific act, plot or threat.

(4) Subsection (2) does not apply if the person has an authorisation under Section 40(2), (3) or (4).

(5) It is not a defence to Subsection (2) that a response from the [police] verifying a suspicion under Subsection 35(4) was not received.

The prohibition against dealing with assets implements the obligation to "freeze assets". It clarifies what is meant by freezing an asset by articulating that this means you can no longer deal with the asset. "Deal" is a defined term. It means that you can no longer sell, supply, transfer, move, convert, dispose of or use the asset. However, the prohibition against dealing with assets does not give rise to an entitlement to confiscate those assets. Ownership of the asset does not change as a result of this provision.

The recklessness test in Subsection (1) is the broadest implementation of the prohibition against dealing with assets. This ensures that a person cannot continue to transact with assets even though they may also file an STR at the point when a suspicion is raised. This means that when a person has a suspicion that an asset is owned, controlled or held by or on behalf of or at the direction of a designated person or entity, then two obligations are invoked: first, the obligation to file an STR under Section 37(4), and second, the prohibition against dealing with the asset pursuant to Section 16(2).

The proliferation of weapons of mass destruction has serious consequences for global, regional and national security and the safety of a state's citizens. States should insert penalties commensurate with the gravity of the offences in this Act.

Fines for bodies corporate should generally be higher than fines for natural persons in order for the penalty to have a sufficient deterrent effect.

17. Prohibition against making assets available

(1) A person must not make an asset available knowing that, or reckless as to whether, it is being made available, directly or indirectly, wholly or jointly:
(a) to a designated person or entity; or
(b) to a person or entity owned or controlled by a designated person or entity; or

(c) to a person or entity acting on behalf of a designated person or entity; or
(d) for the benefit of a designated person or entity.

(2) A person who contravenes Subsection (1) is guilty of an offence.

Penalty:
(a) if the offender is a natural person – a fine not exceeding [xx] or imprisonment for a term not exceeding [xx] years or both; or
(b) if the offender is a body corporate – a fine not exceeding [xx] or an amount equivalent to the value of the asset, whichever is greater.

(3) For the purpose of Subsection (1), it is immaterial whether the asset is located inside or outside [State].

(4) Subsection (2) does not apply if:
(a) the person has an authorisation under Section 40(2), (3) or (4); or
(b) a payment, including by way of interest or other earnings, is made to an account containing frozen assets and that payment is also frozen.

18. Prohibition on joint ventures with designated persons and entities of DPRK

(1) A person must not establish or maintain a joint venture with a person or entity knowing that, or reckless as to whether, that person or entity is designated by:
(a) the United Nations Security Council or its Committees under a United Nations Security Council Resolution listed in Schedule 3 or prescribed by Regulations; or
(b) the [minister] under Section 10.

(2) A person who contravenes Subsection (1) is guilty of an offence.

Penalty:
(a) if the offender is a natural person – a fine not exceeding [xx] or imprisonment for a term not exceeding [xx] years or both; or
(b) if the offender is a body corporate – a fine not exceeding [xx].

References are made in various offence provisions in this Act to "maintaining" certain things, for example, see the reference in Subsection (1) above to "maintaining a joint venture". States should consider whether these references to "maintaining" are better encapsulated in transitional provisions according to their domestic practices so that upon entry into force of this Act, existing joint ventures or accounts (and so on) as applicable must be terminated and no new joint ventures or account as applicable can be established.

Part III: Seizure of frozen assets

19. Court may grant order for seizure of frozen assets

(1) An [enforcement authority] may apply to the court for an order for an [authorised officer] to search for and seize a frozen asset.

(2) An [enforcement authority] may make an application to the court under Subsection (1) at the [enforcement authorities'] own instigation or upon the request of the holder of a frozen asset.

(3) On application by the [enforcement authority], the court may make an order for [an authorised officer] to search for and seize a frozen asset in the following circumstances:
    (a) the seizure is necessary in order to preserve the asset; or
    (b) there is a reasonable risk that the asset will dissipate.

(4) If during the course of a search under an order granted under Subsection (3), an [authorised officer] finds an asset that he or she has reasonable grounds to believe could have been included in the order had its existence been known at the time of application of the order, the [authorised officer] may seize that asset and the seizure order shall be deemed to authorize such seizure.

(5) An asset seized under an order granted under Subsection (3) may only be retained so long as the asset remains frozen under this Act.

Due to the fact that an asset freeze may continue for several years, this provision allows the state to seize and maintain frozen assets. States should ensure that this provision is adapted to reflect domestic legal authorities and processes for the seizure of assets. States should also ensure that they have effective asset management systems in place so that frozen assets are preserved. States should consider any liabilities that may arise is relation to assets under its management – for example, where an asset is de-valued, damaged or destroyed. Provisions for seizing assets can be particularly useful where states have banking rules that prohibit dormant bank accounts to remain open past a certain period of time.

States should note that, in general, the seizure of frozen assets does not create a right to confiscation of those assets. The exception to this rule is OP 14 of UN Security Council Resolution 1874 regarding the DPRK, which allows states to dispose of designated vessels in a manner not inconsistent with obligations under relevant UN Security Council Resolutions. In this context, disposal includes storage, destruction or transfer to another state. This exception in relation to vessels recognises the financial and practical difficulties faced by states in maintaining a vessel that is subject to an asset freeze.

Chapter IV: Other financial measures relating to DPRK

20. Prohibition on financing related to DPRK

(1) A person must not make available an asset or financial service related to an activity specified in Subsection (4) knowing that, or reckless as to whether, the asset or financial service is being made available to a person or entity specified in Subsection (6).

(2) A person who contravenes Subsection (1) is guilty of an offence.

Penalty:

(a) if the offender is a natural person – a fine not exceeding [xx] or imprisonment for a term not exceeding [xx] or both; or
(b) if the offender is a body corporate – a fine not exceeding [xx].

(3) Subsection (2) does not apply if the person has an authorisation under Section 40(6).

(4) For the purpose of Subsection (1), the activities specified are:

(a) the manufacture, production, possession, acquisition, stockpiling, storage, development, transportation, transfer or use of a item specified in Subsection (5); or
(b) the provision of technical training, advice, services, brokering or assistance related to any of the activities in Paragraph (a).

(5) For the purpose of Subsection (4), the following items are specified:

(a) arms or related materiel; or
(b) weapons of mass destruction related material; or
(c) ballistic missile-related goods; or
(d) items, materials, equipment, goods or technology that could contribute to the operational capabilities of DPRK armed forces and are prescribed by Regulations; or
(e) coal, iron, or iron ore; or
(f) gold, titanium ore, vanadium ore, copper, silver, nickel, or zinc; or
(g) rare earth minerals prescribed by Regulations; or
(h) aviation fuel prescribed by Regulations; or
(i) any other items prescribed by Regulations.

(6) For the purpose of Subsection (1), the following persons and entities are specified:

(a) a person in the territory of DPRK; or
(b) a national of DPRK; or
(c) a body corporate incorporated under a law of DPRK; or
(d) the government of DPRK; or
(e) a public body, corporation or agency of the government of DPRK; or

(f) an entity owned or controlled by a person or entity mentioned in Paragraphs (a) to (e); or
(g) a person acting on behalf of, or at the direction of, a person or entity mentioned in Paragraphs (a) to (e).

21. Prohibition on financial transactions related to DPRK

(1) A person must not conduct a financial transaction related to an activity specified in Subsection (5), knowing that, or reckless as to whether, a person or entity specified in Subsection (7) is a party to the financial transaction.

(2) A person who contravenes Subsection (1) is guilty of an offence.

Penalty:
(a) if the offender is a natural person – a fine not exceeding [xx] or imprisonment for a term not exceeding [xx] or both; or
(b) if the offender is a body corporate – a fine not exceeding [xx].

(3) Subsection (2) does not apply if the person has an authorisation under Section 40(6).

(4) For the purpose of Subsection (1):
(a) a person conducts a financial transaction if the person is a party to the transaction, or procures or facilitates the transaction; and
(b) a transaction can be made by any means, including electronic or physical transfer of an asset.

(5) For the purpose of Subsection (1), the activities specified are:
(a) the manufacture, production, possession, acquisition, stockpiling, storage, development, transportation, sale, supply, transfer or use of an item specified in Subsection (6); or
(b) the provision of technical training, advice, services, brokering or assistance related to any of the activities in Paragraph (a).

(6) For the purpose of Subsection(5), the following items are specified:
(a) arms or related materiel; or
(b) weapons of mass destruction related material; or
(c) ballistic missile-related goods; or
(d) items, materials, equipment, goods or technology that could contribute to the operational capabilities of DPRK armed forces and are prescribed by Regulations; or
(e) coal, iron, or iron ore; or
(f) gold, titanium ore, vanadium ore, copper, silver, nickel, or zinc; or
(g) rare earth minerals prescribed by Regulations; or
(h) aviation fuel prescribed by Regulations; or

(i) any other items prescribed by Regulations.

(7) For the purpose of Subsection (1), the following persons and entities are specified:
(a) a person in the territory of DPRK; or
(b) a national of DPRK; or
(c) a body corporate incorporated under a law of DPRK; or
(d) the government of DPRK; or
(e) a public body, corporation or agency of the government of DPRK; or
(f) an entity owned or controlled by a person or entity mentioned in Paragraphs (a) to (e); or
(g) a person acting on behalf of, or at the direction of, a person or entity mentioned in Paragraphs (a) to (e).

For the purpose of Subsection (6) in both the Section 20 and Section 21 offence provisions, states may choose to add 'luxury goods' to that list. While there is no specific requirement in the UN Security Council Resolutions prohibiting financing the sale, supply or transfer of luxury goods, OP 11 of Resolution 2094 requires states to prohibit the transfer of financial services or financial or other assets or resources to DPRK in relation to "other activities prohibited by" UN Security Council Resolutions relating to DPRK. Resolution 1718 prohibits the sale, supply or transfer of luxury goods to DPRK. A list of luxury goods is specified by the UN Resolutions, however, states are required to add other items they determine to be luxury goods. This could be done in Regulations to these model provisions.

The materials in Subsection (6)(e) to (h) have been included since prohibiting financing of these materials is consistent with the intention of the UN Security Council Resolutions and is an effective method of bolstering the implementation of export controls related to these materials.

22. Prohibition on trade with DPRK

(1) A person must not provide public or private financial support for trade with DPRK.

(2) For the purpose of Subsection (1), financial support includes the granting of export credits, guarantees or insurance related to trade.

(3) A person who contravenes Subsection (1) is guilty of an offence.

Penalty:
(a) If the offender is a natural person – a fine not exceeding [xx] or imprisonment for a term not exceeding [xx] or both; or
(b) if the offender is a body corporate – a fine not exceeding [xx].

(4) Subsection (3) does not apply if the person has an authorisation under Section 40(6).

The UN Security Council Resolutions use the term 'financial support' in relation to this obligation and provide an inclusive list of three examples of such financial support (export credits, guarantees and insurance). By comparison, other financial measures in the UN Security Council Resolutions relating to DPRK use to the terms "funds, other financial assets and economic resources" and "financial services", which have been implemented in these model provisions through the defined terms "assets" and "financial services". States may wish to give greater clarity to the private sector on what is captured by the term "financial support" by instead using the defined terms "assets" and "financial services" and amending the definitions to clarify that export credits, guarantees and insurance are clearly captured.

23. Prohibition on relationships with DPRK financial institutions

(1) A financial institution must not:
- (a) establish or maintain a joint venture with a DPRK financial institution; or
- (b) obtain or maintain ownership or control of a DPRK financial institution; or
- (c) establish or maintain a correspondent relationship with a DPRK financial institution.

(2) A person who contravenes Subsection (1) is guilty of an offence.

Penalty:
- (a) if the offender is a natural person – a fine not exceeding [xx]; or
- (b) if the offender is a body corporate – a fine not exceeding [xx].

(3) Subsection (2) does not apply if the financial institution has an authorisation under Section 40(6).

(4) The offence under Subsection (2) is a strict liability offence.

24. Prohibition on maintaining offices in DPRK

(1) A financial institution must not establish or maintain a representative office, branch, subsidiary or account in the territory of DPRK.

(2) A person who contravenes Subsection (1) is guilty of an offence.

Penalty:
- (a) if the offender is a natural person – a fine not exceeding [xx]; or
- (b) if the offender is a body corporate – a fine not exceeding [xx].

(3) Subsection (2) does not apply if the financial institution has an authorisation under Section 40(6).

(4) The offence under Subsection (2) is a strict liability offence.

25. Prohibition on maintaining offices in [State]

(1) A DPRK financial institution must not establish or maintain a representative office, branch, subsidiary or account in the territory of [State].

(2) A person who contravenes subsection (1) is guilty of an offence.

Penalty:
- (a) if the offender is a natural person – a fine not exceeding [xx]; or
- (b) if the offender is a body corporate – a fine not exceeding [xx].

(3) The offence under Subsection (2) is a strict liability offence.

26. Prohibition on accounts related to DPRK missions

(1) A financial institution must not open or maintain an account in [State] knowing that, or reckless as to whether, the account holder is a person or entity specified in Subsection (3) without authorisation from the [minister] under Section 40(6).

(2) A person who contravenes Subsection (1) is guilty of an offence.

Penalty:
- (a) if the offender is a natural person – a fine not exceeding [xx]; or
- (b) if the offender is a body corporate – a fine not exceeding [xx].

(3) For the purpose of Subsection (1), the following persons and entities are specified:
- (a) a DPRK diplomatic mission or consular post; or
- (b) a DPRK diplomatic agent or consular officer; or
- (c) a person or entity owned or controlled by a person or entity in Paragraphs (a) or (b); or
- (d) a person acting on behalf of, or at the direction of, a person or entity in Paragraphs (a), (b) or (c).

This prohibition is to implement OP 16 of UN Security Council Resolution 2321, which limits DPRK diplomatic missions, consular posts, accredited diplomats and consular officers to only one bank account per mission, post, diplomat and officer. The intention is that in order to regulate the number of bank accounts DPRK missions and diplomats have in your state, financial institutions have to seek authorisation to open or maintain a bank account for a person specified in this provision. A single financial institution may not know whether a specified person has an account with another financial institution. However, a state's financial intelligence unit, regulatory or law enforcement authority would be able to obtain this information. Therefore, an obligation is imposed to obtain an authorisation to establish or maintain an account for a specified person.

27. Prohibition against financial transactions related to professional or commercial activities

(1) A person must not conduct a financial transaction relating to professional or commercial profit-making activities knowing that, or reckless as to whether, the financial transaction is with, or for, a DPRK diplomatic agent.

(2) A person who contravenes Subsection (1) is guilty of an offence.

Penalty:

(a) if the offender is a natural person – a fine not exceeding [xx] or imprisonment for a term not exceeding [xx] or both; or
(b) if the offender is a body corporate – a fine not exceeding [xx].

(3) For the purpose of Subsection (1):

(a) a person conducts a financial transaction if the person is a party to the transaction, or procures or facilitates the transaction; and
(b) a transaction can be made by any means, including electronic or physical transfer of an asset.

28. Prohibition against use of real property

(1) A person must not use, lease, sub-lease or hire real property for any activity other than a diplomatic or consular activity knowing that, or reckless as to whether, the real property is owned or leased:

(a) by the government of DPRK; or
(b) a public body, corporation or agency of the government of DPRK; or
(c) a DPRK diplomatic mission or consular post; or
(d) a DPRK diplomatic agent or consular officer; or
(e) a person or entity owned or controlled by a person or entity in Paragraphs (a) to (d).

(2) A person who contravenes Subsection (1) is guilty of an offence.

Penalty:

(a) if the offender is a natural person – a fine not exceeding [xx] or imprisonment for a term not exceeding [xx] or both; or
(b) if the offender is a body corporate – a fine not exceeding [xx].

29. Prohibition relating to vessels

(1) A person must not:
(a) deal with a DPRK flagged vessel; or
(b) provide an insurance service in relation to a DPRK flagged vessel.

(2) A person who contravenes Subsection (1) is guilty of an offence.

Penalty:

(a) If the offender is a natural person – a fine not exceeding [xx] or imprisonment for a term not exceeding [xx] or both; or
(b) if the offender is a body corporate – a fine not exceeding [xx].

(3) Subsection (2) does not apply if the person has an authorisation under Section 40(6).

(4) The offence under Subsection (2) is a strict liability offence.

30. Prohibition relating to vessels and aircraft

(1) A person must not lease or charter a vessel or aircraft, or provide a crew service to a person or entity knowing that, or reckless as to whether, the person or entity is:
(a) the government of DPRK; or
(b) a public body, corporation or agency of the government of DPRK; or
(c) owned or controlled by an entity mentioned in Paragraphs (a) or (b); or
(d) acting on behalf of, or at the direction of, an entity mentioned in Paragraphs (a) or (b).

(2) A person who contravenes Subsection (1) is guilty of an offence.

Penalty:

(a) If the offender is a natural person – a fine not exceeding [xx] or imprisonment for a term not exceeding [xx] or both; or
(b) if the offender is a body corporate – a fine not exceeding [xx].

(3) Subsection (2) does not apply if the person has an authorisation under Section 40(6).

This Section is intended to implement OP 19 of UN Security Council Resolution 2270 and OP 8 of Resolution 2321. Note that where the person or entity is a designated person or entity, this prohibition is also covered by the targeted financial sanctions prohibition against making assets available to designated persons and entities under Section 17.

Chapter V: Other financial measures relating to Iran

31. Prohibition on financing related to Iran

(1) A person must not make available an asset or financial service related to an activity specified in Subsection (4) knowing that, or reckless as to whether, the asset or financial service is being made available to a person or entity specified in Subsection (6).

(2) A person who contravenes Subsection (1) is guilty of an offence.

Penalty:

(a) if the offender is a natural person – a fine not exceeding [xx] or imprisonment for a term not exceeding [xx] or both; or
(b) if the offender is a body corporate – a fine not exceeding [xx].

(3) Subsection (2) does not apply if the person has an authorisation under Section 40(5).

(4) For the purpose of Subsection (1), the activities specified are:

(a) the manufacture, production, possession, stockpiling, storage, development, transportation, supply, sale, transfer or use of an item listed in Subsection (5); or
(b) the provision of technical training, advice, services, brokering or assistance related to any of the activities in Paragraph (a).

(5) For the purpose of Subsection (4)(a) the items listed are:

(a) materials, equipment, goods or technology listed in the following International Atomic Energy Agency documents:
    (i) INFCIRC/254/Rev.12/Part 1; or
    (ii) INFCIRC/254/Rev.9/Part 2; or
(b) arms or related materiel; or
(c) ballistic missile-related goods; or
(d) materials, equipment, goods or technology that could contribute to reprocessing or enrichment-related or heavy water-related activities and that are prescribed by Regulations.

(6) For the purpose of Subsection (1), the following persons and entities are specified:

(a) the government of Iran; or
(b) a public body, corporation or agency of the government of the Iran; or
(c) an entity owned or controlled by an entity mentioned in Paragraphs (a) or (b); or
(d) a person or entity acting on behalf of, or at the direction of, an entity mentioned in Paragraphs (a), (b) or (c).

32. Prohibition on financial transactions related to Iran

(1) A person must not conduct a financial transaction related to an activity listed in Subsection (5), knowing that, or reckless as to whether, a person or entity specified in Subsection (7) is a party to the financial transaction.

(2) A person who contravenes Subsection (1) is guilty of an offence.

Penalty:

(a) if the offender is a natural person – a fine not exceeding [xx] or imprisonment for a term not exceeding [xx] or both; or
(b) if the offender is a body corporate – a fine not exceeding [xx].

(3) Subsection (2) does not apply if the person has an authorisation under Section 40(5).

(4) For the purpose of Subsection (1):

(a) a person conducts a financial transaction if the person is a party to the transaction or procures or facilitates the transaction; and
(b) a transaction can be made by any means, including electronic or physical transfer of an asset.

(5) For the purpose of Subsection (1), the activities specified are:

(a) the manufacture, production, possession, acquisition, stockpiling, storage, development, transportation, transfer or use of an item listed in Subsection (6); or
(b) the provision of technical training, advice, services, brokering or assistance related to any of the activities in Paragraph (a).

(6) For the purpose of Subsection (5)(a) the items listed are:

(a) materials, equipment, goods or technology listed in the following International Atomic Energy Agency documents:
    (i) INFCIRC/254/Rev.12/Part 1; or
    (ii) INFCIRC/254/Rev.9/Part 2; or
(b) arms or related materiel; or
(c) ballistic missile-related goods; or
(d) materials, equipment, goods or technology that could contribute to reprocessing or enrichment-related or heavy water-related activities and that are prescribed by Regulations.

(7) For the purpose of Subsection (1), the following persons and entities are specified:

(a) the government of Iran; or
(b) a public body, corporation or agency of the government of the Iran; or
(c) an entity owned or controlled by an entity mentioned in Paragraphs (a) or (b); or
(d) a person or entity acting on behalf of, or at the direction of, an entity mentioned in Paragraphs (a), (b) or (c).

33. Prohibition on commercial activities

(1) A person must not sell, or otherwise make available, ownership in or control of, a commercial activity specified in Subsection (4), knowing that, or reckless as to whether, the sale or availability is to a person or entity specified in Subsection (5).

(2) A person who contravenes Subsection (1) is guilty of an offence.

Penalty:

(a) if the offender is a natural person – a fine not exceeding [xx] or imprisonment for a term not exceeding [xx] or both; or

(b) if the offender is a body corporate – a fine not exceeding [xx].

(3) Subsection (2) does not apply if the person has an authorisation under Section 40(5).

(4) For the purpose of Subsection (1), the following commercial activities are specified:

(a) uranium mining; or

(b) uranium production; or

(c) manufacturing, producing, possessing, acquiring, stockpiling, storing, developing, transporting, supplying, selling, transferring or using:

(i) materials, equipment, goods, or technology that are listed in International Atomic Energy Agency document INFCIRC/254/Rev.12/Part 1; or

(ii) ballistic missile-related goods.

(5) For the purpose of Subsection (1), the following persons and entities are specified:

(a) a national of Iran; or

(b) a body corporate incorporated under a law of Iran; or

(c) the government of Iran; or

(d) a public body, corporation or agency of the government of the Iran; or

(e) an entity owned or controlled by an entity mentioned in Paragraphs (a) to (d); or

(f) a person acting on behalf of or at the direction of an entity mentioned in Paragraphs (a) to (e).

Chapter VI: Cross-border transportation of cash, precious metals and precious stones

The physical transportation of bulk cash and gold are well-documented proliferation financing methods, particularly in relation to DPRK. UN Security Council Resolutions highlight the importance of monitoring the cross border transportation of cash, precious metals and precious stones. FATF Recommendation 32 also includes requirements for states to implement an effective regime for the declaration of cross-border transportation of 'currency and bearer negotiable instruments'. States should ensure that they have an effective system of declaration of cross border transportation of cash and that the system also covers precious metals, such as gold, and precious stones.

Chapter VII: Preventative measures for financial institutions and DNFBPs

The FATF Recommendations require financial institutions and DNFBPs to implement a range of preventative measures relating to AML/CTF. While not specifically required by UN Security Council Resolutions or FATF Recommendations, states should ensure that these preventative measures cover counter-proliferation financing in addition to AML/CTF. Doing so ensures the effective implementation of UN Security Council Resolutions and may also assist states in complying with FATF's 'effectiveness criteria', in particular Immediate Outcome 11. Requirements related to preventative measures for financial institutions and DNFBPs include: (a) obligations to undertake a risk assessment; (b) obligations for external audits; (c) obligations to adopt internal programmes; (d) obligations to perform customer due diligence; (e) obligations to conduct enhanced due diligence in relation to high risk jurisdictions, high risk business activities, and where the risk of [proliferation financing] is high; (f) obligations for due diligence in relation to correspondent banking relationships; and (g) obligations around record-keeping and transmittal of wire transfer information.

Chapter VIII: Reporting obligations

34. Reporting obligations not limited

Nothing in this Act limits the reporting obligations on a financial institution or DNFBP imposed by the [law on anti-money laundering and counter-terrorist financing].

35. Request to verify

(1) A person who holds an asset which he or she suspects is, or may be, owned, controlled or held on behalf of, or at the direction of, a designated person or entity may make a request in writing to the [police] to verify that suspicion.

(2) The request must be accompanied by details of the asset and the owner or controller of the asset as known to the person making the request.

(3) The [police] must use their best endeavours to assist a person who has made a request under Subsection (1).

(4) As soon as is reasonably practicable after receiving a request under Subsection (1), the [police] must respond in writing stating that:
    (a) it is likely that the property is owned or controlled by a designated person or entity; or
    (b) it is unlikely that the property is owned or controlled by a designated person or entity; or
    (c) it is unknown whether the property is owned or controlled by a designated person or entity.

States should nominate a first point of contact to assist with verification of identity requests. This may be a law enforcement agency, financial intelligence unit or regulatory authority responsible for proliferation financing. The reference is made to 'police' in this provision because it is generally law enforcement agencies, which have the skills and access to relevant information necessary to help verify whether there is a match against the Consolidated List of designated persons and entities. Alternatively, states may also nominate the Sanctions Secretariat as the first point of contact.

36. Obligation to report the assets of a designated person or entity

(1) A person who holds an asset of a designated person or entity must report the holding of that asset to the [Sanctions Secretariat OR relevant supervisor] as soon as reasonably practicable and in any event within [5 working days] from:
    (a) the date that person received notification of the designation under Section 14(1); or

(b) the date of publication of the designation under Section 14(3); or
(c) the date the asset came into the possession or control of that person.

(2) The report must include the following information, if available:
(a) details of the asset; and
(b) name and address of the owner or controller of the asset; and
(c) details of any attempted transaction involving the asset, including:
(i) the name and address of the sender; and
(ii) the name and address of the intended recipient; and
(iii) the purpose of the attempted transaction; and
(iv) the origin of the asset; and
(v) where the asset was intended to be sent.

(3) The report must be in accordance with any form or procedure specified by the [Sanctions Secretariat OR relevant supervisor].

(4) For the avoidance of doubt, the obligation to make a report under Subsection (1) is in addition to the obligation to make a suspicious transaction report under Section 37(4).

(5) A person who intentionally, or by negligence, fails to make a report under Subsection (1) is guilty of an offence.

Penalty:
(a) if the offender is a natural person - a fine not exceeding [xx]; or
(b) if the offender is a body corporate – a fine not exceeding [xx].

Depending on the proliferation financing risks in your state, it may be that it is primarily financial institutions that may hold assets required to be frozen under this Act. If this is the case, states may wish to consider whether the relevant authority for the purpose of reporting obligations should be the financial intelligence unit. This would take advantage of the existing relationship and lines of communication between financial institutions and the financial intelligence unit. Alternatively, states could also consider whether reports should be provided to the relevant supervisor appointed under this Act.

37. Obligation to report suspicious transactions

(1) This section applies where a financial institution or DNFBP has reasonable grounds to suspect that information that is known to it may:
(a) be relevant to the detection, investigation or prosecution of a person for money laundering, terrorist financing, an offence under this Act or any other indictable offence; or

(b) be relevant to the detection, investigation or prosecution of a person for a foreign indictable offence; or
(c) concern proceeds of crime.

Descriptions of the categories of offences in Subsection (1) should be adapted to suite the terminology adopted in each state's domestic legislation on those matters, particularly the criminal or penal law, money laundering offence and proceeds of crime/criminal asset recovery legislation.

(2) For the avoidance of doubt, Subsection (1) applies where a suspicion is formed after this Act enters into force, but that suspicion may be based on information obtained before this Act entered into force.

(3) Where Subsection (1) applies, a financial institution or DNFBP must take reasonable measures to ascertain the following information:
(a) the purpose of the transaction; and
(b) the origin of the funds; and
(c) where the funds will be sent; and
(d) the name and address of the person who will receive the funds; and
(e) any other information that may be relevant to:
(i) the prosecution or investigation of an offence of the kind mentioned in Paragraph (1)(a); or
(ii) any proceedings under this Act or [the law on anti-money laundering and counter-terrorist financing]; or
(iii) a proceeds of crime law of [State].

(4) Where Subsection (1) applies, a financial institution or DNFBP must make a suspicious transaction report to the [financial intelligence unit] as soon as is reasonably practicable and in any event within [5 working days] from the date the suspicion first arose.

States should ensure their AML/CTF legislation enables the financial intelligence unit to share information relating to proliferation financing with the relevant authorities for proliferation financing matters mentioned in this Act (the Sanctions Secretariat, the [minister], supervisors).

(5) A report under Subsection (4) must include:
(a) such information mentioned in Subsection (3) that is known to the financial institution or DNFBP; and
(b) any other information required by the [financial intelligence unit] that is known to the financial institution or DNFBP; and
(c) the basis on which the suspicion has arisen.

(6) A financial institution or DNFBP must provide a report under Subsection (4) in accordance with any form and procedure specified by the [financial intelligence unit].

(7) A financial institution or DNFBP that has made a report in accordance with Subsection (4) must, if requested to do so by the [financial intelligence unit], provide to the [financial intelligence unit] any further information that it has relating to the suspicion.

(8) A person who intentionally, or by negligence, fails to make a report under Subsection (4) is guilty of an offence.

Penalty:
(a) if the offender is a natural person – a fine not exceeding [xx]; or
(b) if the offender is a body corporate – a fine not exceeding [xx].

(9) Nothing in this section precludes a financial institution or DNFBP from communicating to the [financial intelligence unit] any suspicion it may have prior to the making of a report under Subsection (4).

This is an example of provisions on 'suspicious transaction reporting' that includes a requirement to make an STR where offences related to proliferation financing are suspected. Neither the UN Security Council Resolutions, nor the FATF Recommendations, require proliferation financing to be included in STR obligations. However, doing so is recommended in order to effectively implement the Resolutions and may also be a measure that is considered in the context of the FATF's 'effectiveness criteria' (IO 11). States should note that the FATF Recommendations require a range of other measures around suspicious transaction reporting obligations. These would equally apply where the STR is made in relation to a proliferation financing offence under this Act. These other provisions are not included in this Act. Suspicious transaction reporting obligations and related provisions are ideally located within a state's AML/CTF legislation. The example provisions are given here to encourage inclusion of proliferation financing in suspicious transaction reporting obligations.

FATF Recommendations require DNFBPs that undertake certain types of activities to make STRs. States should consider their domestic AML/CTF legislation on the circumstances under which DNFBPs are required to comply with reporting obligations and amend this provision accordingly.

38. Prohibition against disclosing report, information or suspicion

(1) Where Sections 35(1), 36(1), 37(1) or 37(4) apply, a person must not, unless required to do so under this Act, disclose to anyone else:
(a) that a suspicion has been formed under Section 35(1) or Section 37(1); or
(b) a request has been made under Section 35(1); or
(c) that a report has been made under Section 36(1) or Section 37(4); or

(d) that a suspicion has been or may be communicated to the [financial intelligence unit] under Section 37(9); or
(e) any other information from which a person could reasonably infer any of the matters in Paragraphs (a), (b) or (c).

(2) Subsection (1) does not apply to disclosures made by the person to:
(a) the [financial intelligence unit], [police] or [Sanctions Secretariat OR relevant supervisor] in accordance with this Act; or
(b) a police officer for any law enforcement purpose; or
(c) an officer, employee or agent of a financial institution for any purpose connected with the performance of that person's anti-money laundering/counter-terrorist financing duties; or
(d) a lawyer for the purpose of obtaining legal advice or representation in relation to the matter.

(3) Subsection (1) does not apply where a court is satisfied that disclosure is necessary in the interests of justice.

(4) A person who intentionally, or by negligence, discloses information in contravention of Subsection (1) is guilty of an offence.

Penalty:
(a) if the offender is a natural person – a fine not exceeding [xx] or imprisonment for a term not exceeding [xx] years, or both; or
(b) if the offender is a body corporate – a fine not exceeding [xx].

39. Enhanced reporting obligations related to DPRK

(1) A financial institution or DNFBP must make a report to the [financial intelligence unit] where it has reasonable grounds to believe that:
(a) a financial transaction exceeding [USD 10,000] was made or attempted and that financial transaction involves DPRK, a national of DPRK or a person or entity owned or controlled by DPRK; or
(b) an account was opened or attempted to be opened by DPRK, a national of DPRK or a person or entity owned or controlled by DPRK; or
(c) an asset of a value exceeding [USD 10,000] came under management or was requested to come under management and that asset is owned or controlled by DPRK, a national of DPRK or a person or entity owned or controlled by DPRK; or
(d) a front company, shell company, joint venture or other ownership or control structure exists and could be used to evade a prohibition in Chapter IV or any other measure contained in a United Nations Security Council Resolution listed in Schedule 3 or prescribed by Regulations.

(2) The report must include the following information, if applicable and available:
    (a) details of the parties to the transaction or attempted transaction; and
    (b) details of the account holder; and
    (c) name and address of the owner or controller of the asset; and
    (d) the origin of the asset; and
    (e) details of ownership and control structures; and
    (f) details of the transaction or attempted transaction, including:
        (i) the name and address of the sender; and
        (ii) the name and address of the intended recipient; and
        (iii) the purpose of the transaction or attempted transaction; and
        (iv) where the asset was intended to be sent.

(3) A financial institution or DNFBP must provide a report under Subsection (1) in accordance with any form and procedure specified by the [financial intelligence unit].

(4) A person who intentionally, or by negligence, fails to make a report under Subsection (1) is guilty of an offence.

Penalty:
    (a) if the offender is a natural person – a fine not exceeding [xx]; or
    (b) if the offender is a body corporate – a fine not exceeding [xx].

(5) Nothing in this section precludes a financial institution or DNFBP from communicating to the [financial intelligence unit] any suspicion it may have prior to the making of a report under Subsection (1).

(6) For the avoidance of doubt, the obligation to make a report under Subsection (1) is in addition to the obligation to make a suspicious transaction report under Section 37(4).

The UN Security Council Resolutions on DPRK extend beyond suspicious transaction reporting by requiring enhanced monitoring. These additional reporting obligations on financial institutions and DNFBPs are aimed at facilitating this enhanced monitoring in accordance with OP 11 of Resolution 2094, OP 6 of Resolution 2087, and OP 16 and OP 38 of Resolution 2270.

States should define “front company” and “shell company” as used in Section 39(1) in accordance with their corporations law. For the purpose of these model provisions, the terms refer to organisational structures used to shield a “parent” company from liability or scrutiny.

Chapter IX: Administration of the Act

Part I: Functions and powers of the [minister]

40. Authorisations by the [minister]

(1) A person may apply in writing to the [minister] for authorisation to act in contravention of a prohibition in this Act.

(2) In relation to a prohibition in Chapter III, Part II, the [minister] may grant an authorisation if the action contravening a prohibition is required to meet:
   (a) a basic expense; or
   (b) a contractual obligation; or
   (c) an extraordinary expense; or
   (d) a judicial, administrative or arbitral lien or judgement entered into prior to [the designation of the person or entity *OR* 23 December 2006], and the asset is necessary to satisfy that lien or judgement.

The date of 23 December 2006 is the date of adoption of UN Security Council Resolution 1737, which originally imposed the asset freezing obligations. This date is specified in the obligation in Resolution 2231, Annex B, OP 6(d)(iv), which specifically refers to the date of adoption of Resolution 1737, and which Paragraph (d) seeks to implement. States should note that adopting this exact wording of OP 6(d)(iv) means that where a person or entity was designated after 23 December 2006 and a judicial, administrative or arbitral lien was entered into prior to designation but after 23 December 2006, an authorisation cannot be granted to satisfy that lien or judgement. Therefore, two options have been provided in these model provisions, states should seek advice from the UN Security Council in implementing this provision.

(3) In relation to persons and entities designated by the United Nations Security Council or its Committees under United Nations Security Council Resolutions listed in Schedule 2 or prescribed by Regulations relating to Iran, the [minister] may also grant an authorisation if the action contravening a prohibition is:
   (a) necessary for a civil nuclear cooperation project described in Annex III of the Joint Comprehensive Plan of Action; or
   (b) necessary for any activity required for the implementation of the Joint Comprehensive Plan of Action.

(4) In relation to persons and entities designated by the United Nations Security Council or its Committees under United Nations Security Council Resolutions listed in Schedule 3 or prescribed by Regulations relating to DPRK, the [minister] may also grant an authorisation if the action contravening a prohibition is:

(a) necessary to carry out activities of DPRK's missions to the United Nations and its specialized agencies and related organisations or other diplomatic and consular missions of DPRK; or
(b) necessary for the delivery of humanitarian assistance; or
(c) necessary for denuclearisation.

(5) In relation to a prohibition in Chapter V relating to Iran, the [minister] may also grant an authorisation if the action contravening a prohibition:
    (a) is related to:
        (i) equipment covered by B.1 of International Atomic Energy Agency document INFCIRC/254/Rev.12/Part 1 that is for light water reactors; or
        (ii) low-enriched uranium covered by A.1.2 of International Atomic Energy Agency document INFCIRC/254/Rev.12/Part 1 that is incorporated in assembled nuclear fuel elements for light water reactors; or
        (iii) materials, equipment, goods or technology listed in International Atomic Energy Agency document INFCIRC/254/Rev.9/Part 2 that is for exclusive use in light water reactors; or
        (iv) materials, equipment, goods or technology that is directly related to:
            (ivA) the modification of two cascades at the Fordow facility for stable isotope productions; or
            (ivB) the modernisation of the Arak reactor based on the conceptual design agreed in the Joint Comprehensive Plan Of Action; or
            (ivC) the export of Iran's enriched uranium in excess of 300 kilograms in return for natural uranium; or
    (b) has been approved by the United Nations Security Council or its Committees; or
    (c) is consistent with any other exception provided by a United Nations Security Council Resolution listed in Schedule 2 or prescribed by Regulations.

UN Security Council Resolution 2231 does not prohibit the sale, supply or transfer of the items listed in Subsection 5(a), nor does it require UN Security Council approval for the sale, supply or transfer of these items. Nonetheless, states should note that they have obligations to ensure that: (a) the requirements, as appropriate, of the Guidelines as set out in the relevant INFCIRC documents have been met; (b) they have obtained and are in a position to exercise a right to verify the end-use and end-use location of any supplied item; (c) they notify the UN Security Council within ten days of the supply, sale or transfer; and (d) in relation to items listed in the relevant INFCIRC documents, they also notify the International Atomic Energy Agency within ten days of the supply, sale or transfer. Therefore, these model provisions include requirements to obtain authorisation to finance the sale, supply or transfer of these items so that states are in a position to meet the verification and notification requirements.

States should note that in relation to Paragraph (b), the UN Security Council can approve nuclear materials as well as arms or related materiel and ballistic missile-related goods.

(6) In relation to a prohibition in Chapter IV relating to DPRK, the [minister] may also grant an authorisation if the action contravening a prohibition is:
    (a) necessary for the delivery of humanitarian assistance; or
    (b) necessary for livelihood purposes; or
    (c) has been approved by the United Nations Security Council or its Committees; or
    (d) is consistent with any other exception provided by a United Nations Security Council Resolution listed in Schedule 3 or prescribed by Regulations.

(7) The [minister] may not grant an authorisation if the authorisation would violate a provision of a United Nations Security Council Resolution listed in Schedule 1 or prescribed by Regulations.

(8) The [minister] may impose any conditions on an authorisation.

(9) Prior to granting an authorisation, the [minister] must:
    (a) seek any approvals required by, and make any notifications required to, the United Nations Security Council or its Committees, and
    (b) consider any communication from a foreign government relevant to the authorisation.

(10) Where an application is made under Subsection (1) the [minister] must determine the application within a reasonable time and respond to the applicant in writing to:
    (a) grant the authorisation, including any conditions attached to the authorisation; or
    (b) deny the authorisation.

41. Annual report

(1) The [minister] must cause to be published an annual report by regarding the administration of this Act.

(2) The report shall include information regarding:
   (a) designations and revocations made under this Act by the [minister]; and
   (b) designations and revocations made by the United Nations Security Council or its Committees relating to citizens of [State], bodies corporate incorporated under a law of [State] or persons located in [State]; and
   (c) international cooperation on matters relating to the administration of this Act; and
   (d) investigations and prosecutions for offences under this Act.

(3) Nothing in Subsection (2) requires the [minister] to disclose information that would [prejudice national security].

42. Report to United Nations Security Council or its Committees

(1) The [minister] must periodically provide a report to the United Nations Security Council or its Committees in writing.

(2) The report must contain information relevant to the implementation of United Nations Security Council Resolutions listed in a Schedule to this Act or prescribed by Regulations, including:
   (a) information regarding the evasion or attempted evasion of a prohibition under this Act; and
   (b) information that the [minister] believes would assist the United Nations Security Council or its Committees to carry out their functions under a United Nations Security Council Resolution listed in a Schedule to this Act or prescribed by Regulations.

43. Power to request information and documents

(1) Where the [minister] believes that it is necessary for the purpose of carrying out their functions under this Act, the [minister] may request, in writing, any person to provide information or produce documents in their possession or subject to their control.

(2) The [minister] may specify the manner in which, and the period within which, information or documents are to be provided.

(3) A request made under Subsection (1) may include a continuing obligation to keep the [minister] informed as circumstances change, or on such regular basis as the [minister] may specify.

(4) Notwithstanding any other Act or any contractual obligation imposing confidentiality obligations, a person must comply with a request made under Subsection (1).

(5) For the avoidance of doubt, Subsection (4) does not affect [legal professional privilege].

44. Production of documents

Where a request is made for the production of documents, the [minister] may:

(a) take copies of or extracts from any document so produced; and
(b) request any person producing a document to give a written explanation of it.

45. Failure to comply with a request for information or documents

(1) A person who:

(a) (a) fails to comply with a request made under Section 43(1); or
(b) (b) gives information, or produces a document, knowing it is false in a material particular in response to a request made under Section 43(1); or
(c) (c) destroys, mutilates, defaces, conceals or removes a document with the intention of evading a request made under Section 43(1), is guilty of an offence.

Penalty:

(a) if the offender is a natural person – a fine not exceeding [xx] or imprisonment for a term not exceeding [xx] years or both; or
(b) is the offender is a body corporate – a fine not exceeding [xx].

Offences for failure to comply with requests for information are not as severe as the offences relating to proliferation financing, and should therefore attract lesser penalties.

(2) It is a defence to a prosecution under Paragraph (1)(a) that the person has reasonable excuse for failing to comply with the request for information or documents.

(3) A person who gives information, or produces a document, reckless as to whether it is false in a material particular in response to a request made under Section 43(1) is guilty of an offence.

Penalty:

(a) if the offender is a natural person – a fine not exceeding [xx] or imprisonment for a term not exceeding [xx] years or both; or
(b) if the offender is a body corporate – a fine not exceeding [xx].

(4) Where a person is convicted of an offence under this Section, the [court] may make an order requiring that person, within such period as may be specified in the order, to comply with the request.

46. Information to be confidential

Information obtained by the [minister] under this Act is confidential information and can only be disclosed in accordance with Section 47.

47. Disclosure of information by the [minister]

The [minister] may disclose any information obtained under this Act to any agency or body, including an international agency or body or an agency or body of a foreign government, for any of the following purposes:

(a) detecting, investigating or prosecuting an indictable offence;
(b) enforcing a [proceeds of crime law];
(c) promoting, monitoring or enforcing compliance with this Act or the financial sanctions law of another State;
(d) enabling or assisting an official trustee to discharge his functions under enactments relating to insolvency;
(e) monitoring or enforcing compliance with enactments relating to anti-money laundering and counter-terrorist financing;
(f) monitoring or enforcing compliance with [trade, export, or customs laws];
(g) enabling or assisting international law enforcement cooperation under police to police cooperation mechanisms, [mutual legal assistance laws] or other relevant mechanisms and laws;
(h) enabling or assisting any State or territory outside [State] to exercise functions corresponding to those of the [minister] under this Act;
(i) enabling or assisting the United Nations Security Council or its Committees in implementing United Nations Security Council Resolutions listed in Schedule 1 or prescribed by Regulations.

48. Communications from foreign governments

The [minister] may either directly or through diplomatic channels transmit, receive and respond to communications from foreign governments or the United Nations Security Council or its Committees with regard to the powers exercisable under this Act.

49. Power to make regulations

(1) The [minister] may make Regulations consistent with this Act prescribing all matters which are:
(a) required or permitted to be prescribed by this Act; or
(b) necessary or convenient to be prescribed for giving effect to this Act.

(2) Without limiting subsection (1), the Regulations may prescribe additional United Nations Security Council Resolutions.

50. Delegation of authority

The [minister] may delegate, in writing, to an officer of the Sanctions Secretariat the exercise of any or all of his or her powers and functions under this Act, other than the power of delegation conferred by this section, the designation power under Section 10, the power to extend a designation under Section 11(3) and the revocation power under Section 12.

Part II: Sanctions Secretariat

51. Sanctions Secretariat

(1) There is established a Sanctions Secretariat.

(2) The Sanctions Secretariat may exercise functions and powers necessary to support the [minister] in the administration of this Act, including:
   (a) maintaining an up-to-date Consolidated List of all designated persons and entities; and
   (b) specifying such forms and notices as are necessary in the implementation of this Act; and
   (c) receiving reports under [Section 36(1) of this Act OR Section X of the law on anti-money laundering and counter terrorist financing]; and
   (d) facilitating the sharing of information with other agencies or bodies in accordance with Section 47; and
   (e) publishing information on procedures for disputing a prohibition under Section 16, 17 or 18 on the basis of a false match against the Consolidated List; and
   (f) publishing information on procedures for appealing a designation to the [minister] or to the United Nations Security Council or its Committees.

You may wish to nominate an existing agency to undertake the functions under this Section. For the purpose of these model provisions, a 'Sanctions Secretariat' has been created and so named to support the [minister] and receive delegations of functions and powers from the [minister]. In some states, it may be that the [minister] is already able to delegate functions to their department and that department is already administratively required to support the [minister]. If that is the case, you may not need to establish a 'Sanctions Secretariat'; the functions of the Sanctions Secretariat under Subsection 51(2) can simply be attributed to the [minister] and delegated by the [minister] as appropriate to their department under Section 50.

States may choose to use the Consolidated List of designations by UN Security Council Committees available at this website <https://www.un.org/sc/suborg/en/sanctions/un-sc-consolidated-list> and add designations by the [minister] under this Act.

Amend Subsection 2(d) as necessary to reflect the legislation, which contains the reporting obligations. If reporting obligations are contained in other legislation, ensure that the other legislation enables the reports to be shared with the Sanctions Secretariat. This should include the sharing of STRs related to financial sanctions.

Part III: National Coordinating Committee

52. [National coordinating committee] on counter-proliferation financing

(1) There is established a [national coordinating committee] on counter-proliferation financing.

(2) The [national coordinating committee] on counter-proliferation financing shall consist of a representative from:
    (a) the [ministry of foreign affairs]; and
    (b) the [ministry of justice/home affairs/attorney-general/public prosecutor]; and
    (c) the [customs/border control]; and
    (d) every supervisor appointed under this Act; and
    (e) the [police]; and
    (f) the [financial intelligence unit]; and
    (g) the [central bank]; and
    (h) the [trade/export/investment authority]; and
    (i) the [intelligence agency]; and
    (j) the Sanctions Secretariat; and
    (k) such other persons as are invited from time to time by the [minister].

(3) The chair of the [national coordinating committee] shall be the [minister].
(4) The [national coordinating committee] must be convened on a regular basis as determined by the [minister].

This section provides an indicative list of ministries or departments that may be involved in a state's counter-proliferation financing system. If states wish to expand an existing AML/CTF national coordinating committee to include counter-proliferation financing, states should note that the range of ministries or departments involved in counter-proliferation financing will be broader than those involved in AML/CTF. Note that the [committee] does not need to be held at the ministerial level. The Act allows the [minister] to delegate this function to the Sanctions Secretariat. Indeed, it is recommended that this [committee] is held at the officer or senior officer level to facilitate the exchange of information and maintain flexibility.

53. Functions of the [national coordinating committee]

The functions of the [national coordinating committee] on counter-proliferation financing are to:

(a) facilitate necessary information sharing between supervisors, the [minister], and other agencies involved in the operation of the counter-proliferation financing system; and
(b) facilitate the production and dissemination of information on the risks of proliferation financing in order to give advice and make decisions on counter-proliferation financing requirements and the risk-based implementation of those requirements; and
(c) facilitate co-operation amongst supervisors and consultation with other agencies in the development of counter-proliferation financing policies and legislation; and
(d) facilitate consistent and co-ordinated approaches to the development and dissemination of counter-proliferation financing guidance materials and training initiatives by supervisors; and
(e) facilitate good practice and consistent approaches to supervision of this Act; and
(f) provide a forum for examining any operational or policy issues that have implications for the effectiveness or efficiency of the counter-proliferation financing system.

Chapter X: Supervision and enforcement

Part I: Supervision

54. Appointment of supervisors

(1) The following supervisors are appointed for monitoring and enforcing compliance with this Act:
- (a) …….
- (b) …….
- (c) …….

(2) If the products or services provided by a person or entity are covered by more than one supervisor:
- (a) the supervisors concerned will agree on the relevant supervisor for that person or entity; and
- (b) the relevant supervisor will notify the person or entity accordingly.

States may wish to appoint a single supervisor, for example, the Sanctions Secretariat or the financial intelligence unit. Alternatively, states may wish to appoint several supervisors. These supervisors may be regulatory authorities with responsibility to regulate specific sectors.

Subsection (2) is recommended to avoid confusion where several supervisors are appointed.

55. Functions of supervisors

The functions of a supervisor appointed under Section 54 are to:
- (a) monitor and assess the level of risk of proliferation financing across all of the persons and entities that it supervises; and
- (b) monitor the persons and entities that it supervises for compliance with this Act, and for this purpose to develop and implement a risk-based supervisory programme; and
- (c) provide guidance and feedback to the persons and entities it supervises in order to assist those persons and entities to comply with this Act; and
- (d) produce codes of practice for compliance with this Act; and
- (e) receive reports under [Section 36(1) of this Act OR Section X of the law on anti-money laundering and counter terrorist financing]; and
- (f) enforce compliance with this Act; and
- (g) co-operate through the Sanctions Secretariat and the [national coordinating committee for counter-proliferation financing] (or any other mechanism that may be appropriate) with domestic and international counterparts to ensure the consistent, effective, and efficient implementation of this Act.

States should consider whether compliance with a code of practice can be considered by a court in criminal proceedings when determining whether a person has acted in contravention of a prohibition under this Act. States may need to adopt special provisions enabling a court to consider codes of practice.

States should amend Paragraph (e) as necessary to reflect the legislation, which contains the reporting obligations. If reporting obligations are contained in other legislation, ensure that the other legislation enables the reports to be shared with the Sanctions Secretariat and supervisor/s, as appropriate.

56. Delegation of authority

A supervisor may delegate, in writing, to a suitable officer the exercise of any or all of the supervisor's powers and functions under this Act.

Part II: Powers of supervisors

57. Power to request information and documents

(1) Where a supervisor believes that it is necessary for the purpose of monitoring compliance with or detecting evasion of this Act, the supervisor may request, in writing, any person to provide information or produce documents in their possession or subject to their control.

(2) A supervisor may specify the manner in which, and the period within which, information or documents are to be provided.

(3) A request made under Subsection (1) may include a continuing obligation to keep the supervisor informed as circumstances change, or on such regular basis as the supervisor may specify.

(4) Notwithstanding any other Act or any contractual obligation imposing confidentiality obligations, a person must comply with a request made under Subsection (1).

(5) For the avoidance of doubt, Subsection (4) does not affect [legal professional privilege].

58. Production of documents

Where a request is made for the production of documents, a supervisor may:

(a) take copies of or extracts from any document so produced; and
(b) request any person producing a document to give a written explanation of it.

59. Power to conduct on-site inspections

(1) A supervisor may, at any reasonable time, enter and remain at any place (other than a [residential dwelling]) for the purpose of conducting an on-site inspection of a person or entity that it supervises.

(2) During an inspection, a supervisor may require any employee, officer, or agent of the person or entity that it supervises to answer questions relating to its records and documents and to provide any other information that the supervisor may reasonably require for the purpose of the inspection.

(3) A person is not required to answer a question asked by a supervisor under this section if the answer would or could incriminate the person.

(4) Before a supervisor requires a person to answer a question, the person must be informed of the right specified in Subsection (3).

(5) Nothing in this section requires a lawyer to disclose a [privileged communication].

In relation to Subsection (5), states should adopt terminology that corresponds with domestic rules around legal professional privilege.

60. Failure to comply with a request for information or documents

(1) A person who:
- (a) fails to comply with a request made under Section 57(1) or Section 59; or
- (b) gives information, or produces a document, knowing it is false in a material particular in response to a request made under Section 57(1) or Section 59; or
- (c) destroys, mutilates, defaces, conceals or removes a document with the intention of evading a request made under Section 57(1) or Section 59, is guilty of an offence.

Penalty:
- (a) if the offender is a natural person – a fine not exceeding [xx] or imprisonment for a term not exceeding [xx] years or both; or
- (b) is the offender is a body corporate – a fine not exceeding [xx].

(2) It is a defence to a prosecution under Paragraph (1)(a) that the person has reasonable excuse for failing to comply with the request for information or documents.

(3) A person who gives information, or produces a document, reckless as to whether it is false in a material particular in response to a request made under Section 57(1) or Section 59 is guilty of an offence.

Penalty:

(a) if the offender is a natural person – a fine not exceeding [xx] or imprisonment for a term not exceeding [xx] years or both; or
(b) if the offender is a body corporate – a fine not exceeding [xx].

(4) Where a person is convicted of an offence under this Section, the [court] may make an order requiring that person, within such period as may be specified in the order, to comply with the request.

61. Information to be confidential

Information obtained by a supervisor under this Act is confidential information and must only be disclosed in accordance with Section 62.

Where a supervisor is also a regulatory authority, states should consider whether information obtained under this Act by a supervisor can be used for the purposes of carrying out its functions as a regulatory authority under the regulatory law; and vice versa. If this is the case, states should adopt provisions giving effect to this right. States should also consider whether the supervisor is required to inform a person of the purpose for which the information is sought and the fact that the information may be used for another purpose.

62. Disclosure of information by a supervisor

A supervisor may disclose any information obtained under this Act to any agency or body, including an international agency or body or an agency or body of a foreign government, for any of the following purposes:

(a) detecting, investigating or prosecuting an indictable offence;
(b) enforcing a [proceeds of crime law];
(c) promoting, monitoring or enforcing compliance with this Act or the financial sanctions law of another State;
(d) enabling or assisting an official trustee to discharge his functions under enactments relating to insolvency;
(e) monitoring or enforcing compliance with enactments relating to anti-money laundering and counter-terrorist financing;
(f) monitoring or enforcing compliance with [trade, export, or customs laws];
(g) enabling or assisting international law enforcement cooperation under police to police cooperation mechanisms, [mutual legal assistance laws] or other relevant mechanisms and laws;

(h) enabling or assisting any State or territory outside [State] to exercise functions corresponding to those of a supervisor under this Act;
(i) enabling or assisting the [minister] in implementing United Nations Security Council Resolutions listed in Schedule 1 or prescribed by Regulations.

Part III: Enforcement

63. Enforcement measures

(1) A supervisor may do one or more of the following where it has reasonable grounds to believe that a person or entity that it supervises has contravened a prohibition under this Act:
(a) issue a formal warning; or
(b) issue an infringement notice under Section 64; or
(c) accept an enforceable undertaking under Section 65 and seek an order from the court for breach of that undertaking under Section 66; or
(d) seek a performance injunction from the court under Section 67.

(2) This Act does not affect a power of a regulatory authority to suspend, revoke or impose conditions upon or amend the conditions of a license, practising certificate, registration or other equivalent permission granted to a person or entity by that regulatory authority or to exercise any of its other powers or functions.

Supervisors should have a range of non-criminal enforcement measures available to them and should also be able to refer matters to the prosecution authority where appropriate for criminal prosecution.

Subsection (2) highlights the point that states should ensure that relevant regulatory authorities have the power in their respective laws to suspend or revoke a license or registration for contravention of a prohibition under this Act.

64. Infringement notice

(1) A supervisor may serve an infringement notice, in writing, to a person or entity that it supervises where the supervisor has reasonable grounds to believe that the person or entity has contravened a prohibition or failed to meet an obligation under this Act.

(2) A person or entity to whom an infringement notice has been served must, within [30 days] of the date the notice was served, pay a penalty not exceeding:
(a) [xx] for an individual; or
(b) [xx] for a body corporate.

(3) A supervisor may publish in any manner considered appropriate an infringement notice issued to a person or entity.

Where states have civil penalty regimes, it is recommended that civil penalties be included.

65. Enforceable undertaking

(1) A supervisor may request a written undertaking from a person or entity in connection with compliance with this Act.

(2) Without limiting Subsection (1), a written undertaking may relate to an activity of a person or entity or to an officer, employee, agent or a group of officers, employees or agents of the person or entity.

(3) A person or entity may give the supervisor a written undertaking in connection with compliance with this Act.

(4) The terms of an undertaking under this Section must be lawful and in compliance with this Act.

66. Enforcement of undertaking

(1) If the supervisor considers that a person or entity has breached one or more of the terms of an undertaking it provided under Section 65, the supervisor may apply to the court for an order under Subsection (2).

(2) If the court is satisfied that:
    (a) the person or entity has breached one or more of the terms of its undertaking; and
    (b) the undertaking was relevant to the person or entity's obligation under this Act, the court may make an order directing the person or entity to comply with any of the terms of the undertaking.

67. Performance injunctions

(1) A supervisor may apply to the court for an injunction requiring a person or to do an act in order to comply with this Act.

(2) Further to an application under Subsection (1), the court may grant an injunction requiring a person to do an act if it is satisfied that:
    (a) a person has refused or failed, or is refusing or failing, or is proposing to refuse or fail, to do an act; and
    (b) the refusal or failure was, is or would be a contravention of this Act.

(3) An injunction granted by the Court under Subsection (2) may relate to an officer, employee or agent, or a group of officers, employees or agents of the person or entity

the subject of the performance injunction.

(4) An application made under Subsection (1) may be made ex parte and the court may grant an interim injunction under Subsection (2) without the defendant being heard when the court considers it appropriate to do so.

(5) Where the court has granted an injunction under Subsection (2), a supervisor may publish a notice outlining the details of the person or entity's non-compliance and any remedial action ordered by the court.

Chapter XI: Miscellaneous

68. Protection from liability for acts done in good faith

No person is subject to any civil or criminal liability, action, claim or demand for anything done or omitted to be done in good faith in accordance with this Act.

This Section aims to protect all persons, including financial institutions and DNFBPs, against liability for actions or omissions in pursuance of complying with any or all requirements of this Act.

69. Immunity of State

No minister or official of the government of [State] and no person acting at the direction of a minister or official of the government of [State] is subject to any civil or criminal liability, action, claim or demand for anything done or omitted to be done in good faith for the purpose of discharging a duty, performing a function or exercising a power under this Act.

70. Imputing conduct to bodies corporate

For the purpose of the Act, any conduct engaged in on behalf of a body corporate by an employee, agent or officer of the body corporate acting within the actual or apparent scope of his or her employment, or within his or her actual or apparent authority, is conduct also engaged in by the body corporate.

71. Liability of officers of bodies corporate

(1) If a body corporate contravenes a provision of this Act and the contravention is attributable to an officer of the body corporate failing to take reasonable care, the officer is guilty of an offence and liable to a fine not exceeding the maximum for an offence constituted by a contravention by a natural person of the provision contravened by the body corporate.

(2) In determining whether an officer of a body corporate is guilty of an offence, regard must be had to:
    (a) what the officer knew about the matter concerned; and
    (b) the extent of the officer's ability to make, or participate in the making of, decisions that affect the body corporate in relation to the matter concerned; and
    (c) whether the contravention by the body corporate is also attributable to an act or omission of any other person; and
    (d) any other relevant matter.

(3) An officer of a body corporate may be found guilty of an offence in accordance with Subsection (1) whether or not the body corporate has been convicted or found guilty of the crime committed by it.

(4) For the purpose of this section, an **"officer"** of a body corporate includes a person who makes or participates in the making of decisions that affect the whole or a substantial part of the body corporate's business and a person who has the capacity to affect significantly the body corporate's financial standing.

Schedule 1: United Nations Security Council Resolutions

United Nations Security Council Resolutions on the proliferation of nuclear, chemical and biological weapons and their means of delivery:
Resolution 1540 (2004) of the Security Council, adopted on 28 April 2004
Successor resolutions to the above Resolution

United Nations Security Council Resolutions on Democratic People's Republic of Korea:
Resolution 1718 (2006) of the Security Council, adopted on 14 October 2006
Resolution 1874 (2009) of the Security Council, adopted on 12 June 2009
Resolution 2087 (2013) of the Security Council, adopted on 22 January 2013
Resolution 2094 (2013) of the Security Council, adopted on 7 March 2013
Resolution 2270 (2016) of the Security Council, adopted on 2 March 2016
Resolution 2321 (2016) of the Security Council, adopted on 30 November 2016
Successor resolutions to any of the above Resolutions

United Nations Security Council Resolutions on Iran:
Resolution 1737 (2006) of the Security Council, adopted on 27 December 2006
Resolution 2231 (2015) of the Security Council, adopted on 20 July 2015
Successor resolutions to any of the above Resolutions

Schedule 2: United Nations Security Council Resolutions related to Iran

Resolution 1737 (2006) of the Security Council, adopted on 27 December 2006
Resolution 2231 (2015) of the Security Council, adopted on 20 July 2015
Successor resolutions to any of the above Resolutions

Schedule 3: United Nations Security Council Resolutions related to DPRK

Resolution 1718 (2006) of the Security Council, adopted on 14 October 2006
Resolution 1874 (2009) of the Security Council, adopted on 12 June 2009
Resolution 2087 (2013) of the Security Council, adopted on 22 January 2013
Resolution 2094 (2013) of the Security Council, adopted on 7 March 2013
Resolution 2270 (2016) of the Security Council, adopted on 2 March 2016
Resolution 2321 (2016) of the Security Council, adopted on 30 November 2016
Successor resolutions to any of the above Resolutions

About the Authors

Andrea Berger is an Associate Fellow at RUSI and a Senior Research Associate and Senior Program Manager at the James Martin Center for Nonproliferation Studies. She was previously Deputy Director of the Proliferation and Nuclear Policy team at RUSI, where she also co-headed the Institute's programme on the design and implementation of economic sanctions. In addition to her research work on sanctions policy and non-proliferation, Andrea directed the UK Project on Nuclear Issues (UK PONI), a network of over 600 emerging and established nuclear professionals in the UK.

Anagha Joshi is an Associate Fellow at RUSI and undertakes research projects for RUSI's Centre for Financial Crime and Security Studies. She also works as an independent consultant delivering projects to strengthen legal and policy responses to transnational crime and terrorism. Prior to joining RUSI, Anagha worked for the Australian government as a director in the International Legal Assistance Branch, where she led teams to work with governments across Africa, Asia and the Pacific to strengthen transnational crime and terrorism legal frameworks. Anagha has specialist knowledge on AML/CTF, border management and international crime cooperation. She has also worked as a government lawyer, providing advice on international law relating to aviation and maritime security and law enforcement issues.