HM Treasury

National risk assessment of proliferation financing

September 2021

This publication is available at www.gov.uk/government/publications

Any enquiries regarding this publication should be sent to us at public.enquiries@hmtreasury.gov.uk

ISBN 978-1-913635-87-9 PU 3020

Contents

Foreword

As set out in the UK's 2021 Integrated Review of Security, Defence, Development and Foreign Policy, the proliferation of chemical, biological, radiological and nuclear (CBRN) weapons and their delivery systems greatly destabilises counter-proliferation efforts worldwide and poses a significant threat to UK national security. Actors involved in the financing of this proliferation look to exploit the UK's position in the global economy and international financial system to raise funds to develop CBRN programmes which counter UK national security objectives and threaten international peace and security. A key component of the UK's economic strength and prosperity is our openness to investment and trade, as well as our status as a global financial centre. However, as with other economic threats facing the UK – such as money laundering and terrorist financing – these qualities also make the UK economy vulnerable to proliferation financing and threaten the integrity of the UK financial system.

The UK has a robust counter-proliferation regime in place to protect the UK from counter-proliferation threats, including financial sanctions legislation targeting CBRN proliferation and our export control regime. Additionally, the UK plays a leading role in driving international efforts to tackle proliferation financing, at fora such as the United Nations Security Council and the Financial Action Task Force (FATF). In 2018, FATF provided the UK with the best rating of any country assessed so far in this round of its evaluations, including a highly effective rating on the proliferation financing-focused element of the assessment. Nonetheless, in order to ensure that our domestic and international efforts are sufficient to meet the challenge posed by proliferation financing, the UK continuously reviews, identifies and assesses the threats and vulnerabilities this activity presents to the UK. In December 2020, the government published an updated National Risk Assessment of Money Laundering and Terrorist Financing. We are now furthering the UK's understanding of illicit finance risks with the first National Risk Assessment of Proliferation Financing.

This assessment – published by HM Treasury, using input from a wide range of government, private sector and academic partners – highlights the key proliferation financing threats facing the UK today, as well as the specific vulnerabilities in the UK economy and financial system which actors may target to gain financing for their proliferation activities. Only by outlining where these threats and vulnerabilities lie will we be better able to strengthen the UK government's domestic and international efforts in tackling PF. This work will also raise awareness among the private sector and encourage private sector partners to continue and improve their investigations of proliferation financing activity. As the UK's first national risk assessment on proliferation financing, this is an initial step in an enhanced effort by the UK in tackling this activity. Future versions of this assessment – developed in coordination with relevant partners – will continue to identify and highlight these threats and vulnerabilities to protect UK national security.

John Glen MP
Economic Secretary to the Treasury

Chapter 1

Aim, scope and methodology

Background to counter-proliferation financing

1.1 The financing of the proliferation of chemical, biological, radiological and nuclear (CBRN) weapons[1] has increasingly attracted international attention in recent years, largely due to the high-profile actions of proliferation actors such as the Democratic People's Republic of Korea (DPRK) and Iran. At its core, proliferation financing (PF) focuses on the risks associated with financial products and services which are directly linked to the trade in proliferation-sensitive items.

1.2 A range of international organisations monitor PF and examine the wider risk that it poses to the global community. The United Nations (UN), through bodies such as the UN Panel of Experts which support sanctions committees under each UN sanctions regime, works with UN Member States to improve their understanding of PF and its continually evolving methods. The UN has in place extensive sanctions measures targeting DPRK's nuclear programme. These measures include financial sanctions, transport sanctions and export/import controls which aim to restrict North Korean access to vital funds and resources which could contribute to their CBRN activities. The UN also has a sanctions regime targeting Iran's nuclear and ballistic missile programme.

1.3 Additionally, the Financial Action Task Force (FATF) – the international standard setter on countering money laundering (ML) and terrorist financing (TF) – also recommends measures which aim to facilitate implementation of the relevant UN Security Council Resolutions (UNSCRs) relating to PF. However, its mandate in relation to PF is currently limited to the implementation of the UN's DPRK and Iran sanctions regimes – specifically designations under those regimes. In particular, while the FATF requires reporting on actions undertaken to ensure compliance with the prohibitions in relevant UNSCRs, it does not monitor implementation of the activity-based provisions[2] in the UN DPRK regime. The UK also has in place numerous

[1] 'CBRN' is commonly used to describe the malicious use of chemical, biological, radiological and nuclear materials and weapons with the intention to cause significant harm or disruption. The UK has obligations under a number of international treaties, conventions and export control regimes to tackle CBRN proliferation, such as the Nuclear Non-Proliferation Treaty, the Chemical and Biological Weapons Conventions and the Missile Technology Control Regime.

[2] As explained by the Financial Action Task Force, activity-based provisions aim to prevent the provision of financial services, financial resources or financial assistance through active implementation of measures such as identifying high-risk customers and transactions and applying enhanced scrutiny to such customers and transactions.

autonomous measures to tackle PF under the Sanctions and Anti-Money Laundering Act (SAMLA) which will be covered in the following chapter.

1.4 In 2018, the FATF first began pursuing work to strengthen its standards on countering PF. This signalled a shift towards assessing PF risk as a key component of a robust regime to combat ML, TF and PF, rather than primarily focussing on ML/TF and considering PF within broader sanctions assessments. In October 2020, the FATF agreed revisions to its Recommendation 1 to require both countries and the private sector to identify, assess, manage and mitigate the risks of potential breaches, non-implementation or evasion of targeted financial sanctions relating to PF. As a global leader in counter-proliferation efforts and one of the original co-chairs of the FATF project, the UK has been a strong supporter of these new requirements. Publishing this first national risk assessment (NRA) on PF is an important step towards strengthening our national response to the threat posed by this activity, particularly given the potential vulnerability of the UK – as a global financial centre – to a broad range of activities which could facilitate PF.

Aims of the UK's PF national risk assessment

1.5 Risk assessments have become a central feature of national responses to the dual threats posed by ML and TF. A sound understanding of PF risk is critical to policy development for the public as well as being vital for effective implementation of counter-PF measures for both public sector (particularly in prioritisation and allocation of law enforcement resource) and private sector groups.

1.6 The UK was one of the first countries to publish an ML/TF NRA and is widely recognised internationally as a leader in this field. The UK's ML/TF NRA, however, has not previously included an assessment of PF risk. The UK's 2021 Integrated Review of Security, Defence, Development and Foreign Policy (the Integrated Review 2021) highlighted PF's importance to the UK's broader counter-proliferation efforts. Internationally, several countries, including the United States and South Africa, have moved to conduct their first national PF risk assessment as we committed to doing in the Economic Crime Plan 2019.

1.7 Recognising this opportunity to further strengthen our counter-proliferation system, we have now conducted and published the UK's first PF NRA to complement the December 2020 update to the ML/TF NRA.

The national risk assessment's scope

1.8 The FATF's understanding of PF activity[3] provides a comprehensive insight into the kind of activities which should be considered as contributors to PF,

[3] The Financial Action Task Force states that PF activity includes 'the act of providing funds or financial services which are used, in whole or in part, for the manufacture, acquisition, possession,

such as a company providing internet banking services to a government shipping agency to facilitate them importing dual-use items in breach of UN sanctions requirements. However, in only referring to activities which can be *directly* linked, we risk excluding all types of *indirect* financing which can still contribute to CBRN proliferation. While activities which undermine a certain UN sanctions regime may not be specifically designed to provide the financing of weapons acquisition to the targets of the regime, these activities could also indirectly provide the targets of the regime with financing which could ultimately be used to develop its CBRN programme. For example, this could include providing funding to a charity whose Senior Executive has privately sympathetic views towards an extremist organisation with proliferation ambitions. The donor could have genuine intentions and simply be donating to a charity, but the funds could indirectly be transferred by the Senior Executive for CBRN development. While indirect, as well as other economic crime types such as embezzlement and a potential breach of charity rules the funding would amount to a significant PF risk.

1.9 Another example of facilitating PF indirectly could be through the establishment of front companies to mask the true parties involved in specific transactions. To address this issue, the NRA's scope includes activities carried out by actors which directly or indirectly finance the procurement of CBRN technology. These examples all demonstrate the importance of carrying out appropriate checks on all persons involved in transactions – and the transactions themselves – particularly where higher-risk jurisdictions, such as the ones noted in this assessment, are involved.

1.10 In summary, this NRA's scope covers the following activities, all of which must have a UK nexus and threaten the UK financial system and/or UK national security to be included:

- Activities which directly or indirectly finance an actor's procurement of CBRN technology.

1.11 In future iterations of our PF NRA, we will endeavour to continue to broaden the evidence base to include a broad spectrum of actors within scope of the NRA where there is evidence of risks arising from PF.

Methodology

1.12 The methodology used for this NRA is broadly in line with that used in the ML/TF NRA and international best practice. It follows three key stages – identification, assessment and evaluation of evidence.

1.13 The first stage of this NRA established the parameters of the assessment's scope and the activities which should be included, as set out above, in the absence of a universally accepted definition of PF. To develop this scope, we

development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials (including both technologies and dual-use goods used for non-legitimate purposes), in contravention of national laws or, where applicable, international obligations'. Financial Action Task Force, 'Combating Proliferation Financing', 2010, p.5.

reviewed relevant material on PF – such as papers and reports published by the FATF and other publicly available national risk assessments – and obtained evidence of PF activity with a UK nexus from both public and private sector partners. The information gathering phase involved UK government departments, private sector partners – including financial institutions and insurance firms – the academic sector and non-governmental organisations. These organisations provided evidence on PF threats and trends they were aware of, and information was obtained in written form at roundtables and via bilateral meetings.

1.14 Following this, we assessed this evidence and determined the threats, vulnerabilities and consequences of the activities impacting the UK – including those impacting UK government interests and the private sector – and reviewed possible mitigation strategies to address them. These terms, which have been used throughout the NRA, have been defined below:

- Threat - the intent and capability of people to cause harm, and the activities they conduct to do so. PF threats include financing of CBRN procurement, such as the use of trade finance services in procurement of proliferation-sensitive items.
- Vulnerability – these are inherent things that can be exploited by threat actors. See below for the full list of vulnerabilities we refer to throughout the NRA.
- Consequence – the impact or harm that results from PF activity, including the development of CBRN programmes or the reputational effect of the PF activity taking place in the UK financial system.
- Mitigations – these are the actions that are taken to reduce the risk. This includes the effectiveness, capability and capacity of the UK government, law enforcement and the private sector.

1.15 The assessments were systematically reviewed by UK government departments to ensure they represented a holistic view of the PF threat from the UK government's perspective.

1.16 This publication is a first iteration of the UK's PF NRA. As has been the case for the ML/TF NRA, ongoing review, identification and assessment of PF threats to the UK will continue going forward with potential for additional threats, vulnerabilities and consequences, as well as the corresponding mitigation strategies, to be identified.

Chapter 2

The UK's strategic, regulatory and operational framework for combatting proliferation finance

The UK's approach to counter-proliferation financing

2.1 The UK has a long-standing commitment to counter-proliferation (CP) and has been active in disrupting those seeking to procure proliferation-sensitive items and those funding such activity in the UK and globally. The Integrated Review 2021 underlined the UK's commitment to remaining at the forefront of international efforts to tackle proliferation through the imposition of our responsibilities as set out in United Nations Security Council Resolutions (UNSCRs) focused on CP

2.2 The UK maintains a whole of government approach to CP work with a focus upon co-operation and collaboration. As part of its strategic CP objectives, the UK government created the Counter Proliferation and Arms Control Centre (CPACC) in July 2016. It consolidated, in a single location, expertise and policy making on international CP and arms control issues, drawing together personnel from the Foreign, Commonwealth and Development Office (FCDO), Ministry of Defence (MOD), Department for International Trade (DIT) and the Department for Business, Energy and Industrial Strategy (BEIS). This unit is the co-ordinating body for CP and arms control policy and activity, including PF, ensuring that all relevant cross government partners are operating in a coordinated manner to achieve common objectives.

2.3 At the strategic level, direction on CP issues is set in a collective way involving input from across HMG's CP and PF community which discusses ongoing issues with CP treaties and regimes and ensures joint working across CP and PF stakeholders in government. There are also cross-government structures which provide direction, prioritisation and strategic coherence on HMG sanctions policy and strategy, bringing together all relevant departments involved in HMG sanctions work including FCDO, HMT (including the Office of Financial Sanctions Implementation), DIT, Home Office and the Department for Transport. These provide policy and enforcement oversight of the various CP sanctions regimes within the UK's sanctions framework.

2.4 HM Treasury is represented at relevant groups as appropriate, bringing focus and expertise on PF and the implementation of financial sanctions.

Regulatory framework

2.5 The UK has a robust, bespoke regulatory framework in place to combat the threat posed by PF. A key focus is the implementation of UK and UN sanctions regimes on DPRK, Iran and chemical weapons activity. The sanctions measures apply to anyone in the UK's jurisdiction, action taken by a UK national outside of the UK and to companies incorporated in the UK. Obligations under the measures imposed by the UN are set out in the relevant UNSCRs and relevant counter-PF (CPF) measures set out in UK legislation, such as CPF sanctions regimes implemented under SAMLA.

The Democratic People's Republic of Korea

2.6 The UK has in place an autonomous DPRK sanctions regime, The Democratic People's Republic of Korea (Sanctions) (EU Exit) Regulations 2019. The purposes of the regime are to restrict the ability of North Korea to carry on banned programmes and to promote the abandonment of these, as well as the decommissioning of the DPRK's banned weapons, and otherwise promote peace, security and stability on the Korean peninsula. The Regulations ensure the UK complies with UN obligations under the following UN Security Council Resolutions:

- Resolution 1718 in 2006 which first imposed prohibitions on North Korea and demanded it to refrain from developing its CBRN capability and reversing its CBRN programmes;
- Resolution 1874 of 2009. This developed several measures under Resolution 1718, such as expanding the arms embargo;
- Resolutions 2087 and 2094 in 2013 which – among other measures – imposed restrictions on the development of technology in relation to DPRK's CBRN capabilities and also expanded on these technological measures and added luxury goods to the list of banned imports;
- Resolutions 2270 and 2321 in 2016. These Resolutions further expanded measures from previous Resolutions, such as those in relation to inspections on cargo destined to or originating from North Korea;
- Resolutions 2356, 2371, 2375 and 2397 in 2017. These Resolutions again expanded previous UN measures on DPRK. These measures included financial restrictions, restrictions on the export of energy resources to North Korea and required countries to expel North Korean workers.

Iran

2.7 The UK implements two autonomous sanctions regimes that target specific activities carried out by actors in Iran: The Iran (Sanctions) (Nuclear) (EU Exit) Regulations 2019 and The Iran (Sanctions) (Human Rights) (EU Exit) Regulations 2019. The former's purposes are to ensure UK compliance with UNSCR 2231 and to promote the abandonment by Iran of nuclear weapons programmes, restrict the ability of Iran to develop nuclear weapons and nuclear weapons delivery systems, and promote implementation of the Joint Comprehensive Plan of Action. The

Regulations impose sanctions measures on Iranian individuals and entities involved in this activity.

Chemical weapons

2.8 The UK implements an autonomous sanctions regime on chemical weapons, The Chemical Weapons (Sanctions) (EU Exit) Regulations 2019. Individuals and entities from Syria and Russia have been designated under this regime, the purposes of which are to deter the proliferation and use of chemical weapons, including encouraging the effective implementation of the Chemical Weapons Convention.

Strategic military and dual-use items[4]

2.9 The UK's comprehensive sanctions regime is complemented by robust restrictions on the export of proliferation-sensitive items. The Export Control Act (2002) and the Export Control Order (2008) provide the legal framework for export controls. The Order has been subject to frequent amendment. The UK has also retained a significant body of relevant European Union legislation.

Anti-money laundering (AML) and counter-terrorist financing (CTF) regime

2.10 The UK has had regulations intended to prevent money laundering in place for nearly thirty years. Over time, these have evolved in line with international standards set by the FATF and multiple EU Money Laundering Directives. The most substantial recent revision was in June 2017, transposing the European Fourth Money Laundering Directive and the Funds Transfer Regulation, which were themselves heavily informed by a substantial rewrite of the FATF's international standards in 2012. Since 2017, the Money Laundering Regulations (MLRs) have been amended, most significantly through the transposition of the Fifth Money Laundering Directive in January 2020. The government launched a consultation in July 2021 on further updates and changes to the MLRs.

2.11 Additionally, SAMLA enables the UK to implement United Nations (UN) sanctions regimes and to use autonomous UK sanctions to meet national security and foreign policy objectives. It also allows the UK to keep its anti-money laundering and counter-terrorist financing measures updated. This helps to protect the security and prosperity of the UK and to continue to align the UK with international standards.

[4] Dual-use items are goods, software, technology, documents and diagrams which can be used for both civil and military applications. They can range from raw materials to components and complete systems, such as aluminium alloys, bearings, or lasers. They could also be items used in the production or development of military goods, such as machine tools, chemical manufacturing equipment and computers.

2.12 The Proceeds of Crime Act 2002 (POCA) also contains the single set of money laundering offences applicable throughout the UK to the proceeds of all crimes. Additionally, the Criminal Finances Act 2017 amends POCA, the Terrorism Act 2000, and the Anti-Terrorism Crime & Security Act 2001, and provides additional powers to enable law enforcement and prosecution agencies to identify and recover corrupt and criminal funds from those seeking to hide, use or move them in the UK. The Anti-Terrorism Crime & Security Act also includes offences relating to the development, procurement and use of CBRNs.

2.13 Moreover, the Terrorism Act 2000 includes key provisions criminalising the financing of terrorism (sections 15-18). These include inviting, providing, or receiving money or property with the intention or reasonable suspicion that it will be used for the purposes of terrorism and using or intending to use money or other property for the purposes of terrorism. Section 17A within the Act was amended by the Counter Terrorism and Security Act 2015, to explicitly criminalise the making of insurance payments in response to terrorist demands. In addition, the UK counter-terrorist sanctions regimes meet obligations placed on the UK by UN Security Council Resolutions (UNSCRs). These are implemented by the ISIL (Da'esh) and Al-Qaida (United Nations Sanctions) (EU Exit) Regulations 2019, the Counter Terrorism (International Sanctions) (EU Exit) Regulations 2019 and the Counter Terrorism (Sanctions) (EU Exit) Regulations 2019.

Operational framework

2.14 The UK used all possible tools available to it to undertake this assessment with efforts to counter PF being closely integrated with wider cross-government CP efforts.

2.15 OFSI is the lead for the implementation of financial sanctions (including those related to CP) and leverages significant contributions from other agencies and government departments to ensure that financial sanctions are properly implemented in the UK. The creation of OFSI in 2016 significantly increased the resource dedicated to ensuring and monitoring compliance with financial sanctions. In 2019-2020, OFSI received 140 reports of potential financial sanctions breaches worth £982.34 million[5].

2.16 Supervisors for Financial Institutions (FIs) and Designated Non-Financial Businesses and Professions (DNFBPs) monitor sanctions compliance to some degree, including PF compliance, as part of their risk-based inspections, desk-based reviews, and other monitoring of their regulated sector, and will expect to see firms considering this as part of their own risk assessments. OFSI works closely with the AML/CTF supervisors such as the FCA (including the Office for Professional Body Anti-Money Laundering Supervision - OPBAS), HMRC and professional body supervisors through the AML Supervisors Forum (AMLSF) on issues such as publicising OFSI guidance to their regulated population.

5 These relate to all financial sanctions regimes and not just proliferation-related regimes.

OFSI financial sanctions compliance strategy

2.17 OFSI's functions are broader than just enforcement. It takes a holistic approach to helping ensure compliance with the CP sanctions regimes, rather than simply waiting until a breach occurs, and a response is required. Deciding whether to impose a monetary penalty is informed by OFSI's overall approach to financial sanctions compliance. This approach covers the whole lifecycle of compliance. OFSI's

approach is summarised by its compliance and enforcement model: promote, enable, respond, change:

- OFSI promotes compliance, publicising financial sanctions and engaging with the private sector. It applies an effective compliance approach, which promotes compliance by reaching the right audiences, through multiple channels, with messages they respond to;

- OFSI enables compliance by providing customers with guidance and alerts to help them fulfil their own compliance responsibilities. An effective compliance approach enables cost-effective compliance, makes it easy to comply and minimises by design the opportunities for non-compliance. This is demonstrated by OFSI reporting requirements, where the facilitation of suspected breach reporting and the use of tightly drafted and bespoke reporting conditions serves to promote increased reporting and ensure more effective oversight of potentially higher-risk licences;

- OFSI responds to non-compliance by intervening to disrupt attempted breaches and by tackling breaches effectively. It applies an effective compliance approach, by responding to non-compliance consistently, proportionately, transparently and effectively, taking into account the full facts of the case, and learns from experience to continuously improve the UK's response;

- OFSI does these things to change behaviour, directly preventing future non-compliance by the individual and more widely through the impact of compliance and enforcement action.

Cross-government monitoring in support of compliance

2.18 Gathering and analysing information in support of countering PF is undertaken by a wide number of government departments. Intelligence from a variety of sources is drawn upon by entities across government who scrutinise it for activity that is in breach of UK and UN Sanctions regimes:

- While DIT is the UK export licensing authority and export control policy holder, HMRC is the UK's enforcement authority for export control activity. HMRC's Customs arm monitors a number of information feeds to counter the proliferation of those items that are controlled under the UK's Strategic Export Controls regime;

- The NCA, which conducts its own monitoring activity, assesses intelligence to identify significant breaches that are then referred to relevant partners;

- The Ministry of Defence also undertake analysis in support of the UK's CP objectives.

2.19 The co-ordination of activities and exchange of information that result from these monitoring efforts occurs through the various government co-ordination mechanisms relating to sanctions and counter proliferation.

Allies and partners

2.20 OFSI works with a wide range of international partners and allies on financial sanctions implementation, engaging – for example – with colleagues in the US and European partners on a regular basis. Liaison with these partners is wide-ranging, and includes multijurisdictional casework, best practice sharing and identification of common priorities to aid better enforcement and vigilance.

2.21 The UK also actively assists the Crown Dependencies (CDs) and British Overseas Territories (OTs) with guidance on financial sanctions, including in a proliferation context. The UK is fostering greater cooperation between the UK, CDs and OTs, with greater best practice sharing and exchanges of experience on operational sanctions policy. Departments across government regularly collaborate on guidance on sanctions-related issues for OTs Governors' Offices and public officials, including best practice around processing of licence applications and communicating new listings to the public. OFSI has assisted OTs directly with capacity building, individually and collectively, and presented to FATF-Style Regional Bodies, including in the Caribbean region, on targeted financial sanctions in a proliferation context.

Chapter 3

Proliferation financing threats facing the United Kingdom

3.1 This section of the risk assessment outlines the direct and indirect PF threats facing the UK. The UK financial system is particularly susceptible to PF threats given its role in the global financial system and the openness and transparency of the UK economy.

3.2 The PF threats that the UK is most likely to be exposed to relate to the UK's central role as a global provider of financial and corporate services in support of the legitimate trade in sensitive items, even items that are not procured from the UK, as well as the ability for actors to establish shell companies in the UK to conceal a wider network of PF-related activity. To a lesser extent, the UK may also face PF threats as a jurisdiction where proliferators can raise revenue and procure proliferation sensitive and other dual-use items.[1]

3.3 This chapter divides PF threats facing the UK into three sub-categories:

(i) direct PF activity;
(ii) indirect PF activity; and
(iii) PF activity undertaken by state actors

Direct proliferation financing

3.4 Direct financing is well documented as a strand of PF elsewhere, particularly in UNSCR 1540 and publications by the FATF. Direct financing can be thought of as activity which directly contributes to the development of CBRN capability, such as providing funding to a state nuclear agency or procurement of dual-use items. Many of the PF threats facing the UK today can be understood as direct. While there may be some indirect elements to the activity – such as procurement networks including front companies – the case studies and the broader analysis in this section of the assessment focuses on PF activity where there is a clear link between finance and proliferating actors. This section focuses on two main areas of direct PF activity impacting the UK: (i) direct procurement of proliferating or dual-use items and (ii) evasion of financial sanctions regimes.

[1] Please see the Royal United Services Institute's three categories of PF threats in 'Guide to Conducting a National Proliferation Financing Risk Assessment', 13 May 2019, p. 13-15, https://rusi.org/publication/other-publications/guide-conducting-national-proliferationfinancing-risk-assessment.

Direct procurement of proliferating or dual-use items

3.5 Direct procurement of dual-use items in a PF context typically involves a procurement network seeking to export controlled items out of the UK to a high-risk jurisdiction. The example below covers this type of activity. The UK's role as a major arms manufacturer and supplier, as well as producer of dual-use items – such as nuclear-related material – increases the attractiveness of the UK to proliferation actors involved in these procurement networks, and therefore increases risks to the UK. Many UK industrial sectors can be procurement targets, including goods which can be used in the nuclear industry which are also used in everyday items or for use in commercial industry, such as carbon fibre, vacuum pumps, electronic components and testing equipment. Chemical weapon precursors are also considered to be dual-use items which can be vulnerable to PF actors, an example being those chemicals used as flame retardant. UK-manufactured electronic components, for example, were found in the debris of a 2012 North Korean missile test.[2]

Case Study 1 – procurement of dual-use items from UK company

- A UK manufacturer/exporter was approached by a company based in a foreign jurisdiction. The company was seeking to purchase high specification dual-use items for deployment in a non-military project in an area which was local to that country's boundaries. The financial structure used to conceal the real 'end user' involved several overseas companies with limited trading histories which had been set up specifically for this procurement.
- This structure was explained by the customer as being required for client/agent confidentiality and to enable the specific project to be financially ring-fenced from the customer's other business interests. These are accepted business practices in certain transactions and consequently they did not cause suspicion during the UK exporter's due diligence processes. It was on a more detailed examination of the technical requirements for the items by HMRC that it became apparent that the items were ultimately destined for a military project controlled by a totally separate country which was subject to international sanctions.
- This case study highlights the importance of undertaking sufficient levels of customer due diligence to ensure end users are legitimate and not linked to illicit actors. The evidence of illicit actors masking participants in transactions or financial networks increases the necessity of carrying out these checks.

Evasion of financial sanctions regimes and export controls

3.6 The UK implements both autonomous UK and UN financial sanctions regimes, some of which are designed to prevent financing being obtained by proliferating actors globally. Many proliferation threats facing the UK in

[2] United Nations Security Council Resolution 1718 Committee, S/2014/147, 6 March 2014, p. 22, https://www.undocs.org/S/2014/147.

respect of financial sanctions evasion involve actors with links to DPRK and Iran. However, proliferation financing also seeks to evade export controls. One example below highlights the threat from those seeking to subvert export controls on dual-use items by masking the financial mechanisms used to pay for these items.

Case study 2 – re-insurance products for North-Korean designated entity

- A UK-registered specialist underwriter provided a re-insurance policy for a vessel which had links to North Korea. Through a subsidiary based in a third country of a major insurance market, the underwriter provided cover for an insurer in that same third country, who in turn insured the vessel.
- After the vessel was initially insured, both it and its owning company became designated by the UN (and were subsequently designated by the UK) for reported involvement in ship-to-ship petroleum transfers with a DPRK-flagged vessel. The underwriter was then informed by a regulatory organisation of the re-insurance policy's link to a designated entity. Following this the policy was cancelled and OFSI was notified and investigated further.
- As neither the vessel nor its owning company were designated at the date the policy was facilitated (as the reported proliferation activity had apparently occurred after that point), sanctions checks undertaken by the underwriter and third country insurance subsidiary on the vessel had not highlighted potential North Korean links; whilst no premium payments were received by the underwriter following cancellation of the policy. Consequently, no sanctions breach was deemed to have occurred. The original reporting party were urged to freeze any designated entity-related premium payments received in the future and the case was closed.
- Had the re-insurance policy not been cancelled, it would have posed a proliferation financing risk, by providing a designated vessel with insurance cover, which would then have facilitated the transport of proliferation-sensitive items and materials, thereby generating funds in support of the North Korean regime and furthering proliferation. Both the UK-based specialist underwriter and the ultimately UK-based major insurance market (whose subsidiary was referred to above) could also have been subject to proportionate enforcement action by OFSI (following investigation). This could have involved a range of actions; up to and including the imposition of a monetary penalty (of up to £1 million or 50% of the value of the breach, whichever is higher) or referral to law enforcement agencies for possible criminal prosecution.
- This case study outlines the importance of monitoring changes to designations under UK sanctions regimes. Legitimate business activity with an entity that later becomes designated needs to result in the termination of the relevant activity prohibited under the sanctions regime, unless certain permissions apply.

Case study 3 – export of controlled items to the Middle East

- A procurement network operating in the Middle East sought high specification military items from a UK manufacturer and exporter. An application for a UK export licence was supported by what appeared to be a genuine End User Certificate from a foreign government. The export was interdicted and examined prior to leaving the UK. The accompanying export documents indicated the involvement of an intermediary company also based in the same Middle Eastern country, which prompted further HMRC enquiries.

- Investigations revealed questionable authenticity of the End User Certificate and banking transaction details indicating payments made for the items to the UK manufacturer originating from a third-party bank account in a different jurisdiction to the declared consignee. The invoice supplied in support of the financial transaction also mis-described the items being supplied and funds were transferred via a client sub-account operated by a professional enabler. HMRC's assessment is that these steps were taken to conceal the real end user and final destination from scrutiny by the competent UK export licensing authority, and financial institutions. The items were subsequently seized by HMRC.
- This case study outlines the importance of undertaking sufficient due diligence on parties involved in transactions to minimise the risk of illicit actors being involved.

Case study 4 – masking of dual-use machinery shipments to Iran

- An EU resident Iranian national operated a local company specialising in the sourcing of industrial production equipment new and second hand, capable of producing items restricted under EU dual-use items controls. For this reason, the machinery itself is controlled. The Iranian procurer sourced those machines from the UK where there is a good supply on the second-hand market at more competitive prices.
- Due to the high volumes, much of this type of machinery is usually sold in open auction, both with physical bidders as well as being opened to other bidders which may be based overseas. Successful bids are sold "ex works", where the buyer has title to the items on payment of the successful bid price. The buyer is then responsible for the removal of the items and if to be exported, organises one's own freight movement. Payment is made using the EU bank account of the buyer.
- As an auctioneer, the UK seller may carry out checks prior to the admission of bidders, but usually to ensure they are able to pay for the items rather than to carry out Counter Proliferation related checks. The amounts involved are usually low and therefore do not routinely arouse suspicions from the sellers' bank, and likewise for the buyer's bank. Due to UK, EU and US sanctions, not all Iranian banks have banking relationships with Western banks, so the Iranian buyer explained away third country payments from the UAE or Turkey. As the payer may be a local entity, the real Iranian purchaser was never revealed. As the buyer organises the freight movement independently, the usual routing is through Turkey or the UAE. The former for ease of movement of items from the UK and a land border to Iran, and the latter as a Freeport / free trade zone in the heart of the Middle East. Furthermore, as the items are declared as being consigned for local entities, the real end user is not declared.
- This case study highlights the importance of raising awareness of sanctions regimes, proliferation risks and goods and items which can be exploited by proliferators. Doing so here would have ensured that the individual's ability to purchase the goods was constrained due to relevant robust counter-proliferation due diligence perspective.

Indirect proliferation financing

3.7 While direct PF can be regarded as PF activity where there is a clearer link between the proliferating actor and their financial activities, there are also cases where these actors use more indirect methods to fund their proliferation ambitions. While the FATF rightly highlights the threats posed

by more direct PF activity, this section will demonstrate that the UK also faces threats from indirect PF. This will raise awareness of this type of activity. Indirect PF can be considered as activity where there are more steps between finance and the proliferating actor – typically, the role played by front companies and intermediaries is more obvious in these types of cases.

Networks of front companies designed to mask participants

3.8 While front companies have been mentioned in previous examples in more direct case studies, their role in indirect PF activity is more prominent. In these examples, there are usually more complex networks of companies designed to mask the end recipient of proliferation-related items. This will be highlighted in the 'Vulnerabilities' chapter, but the same factors that make our companies framework successful, such as ease of incorporation, also make it attractive to exploitation, including to those of proliferating actors seeking to establish entities here.

Case study 5 – the purchase of aircraft parts for an Iranian procurer

- HMRC recently carried out an investigation of individuals linked to the purchase of US and Russian aircraft parts for Iran. The procurement was refined over several years to disguise the key individuals within the network and the financial channels used to facilitate the activity.
- In 2007, the principal UK actor worked for a Singaporean company that bought aircraft parts from the US, imported them into Singapore and diverted them to Iran. The directors of the company were indicted, with one eventually prosecuted and imprisoned in the US. Between 2008-2010 however, the UK national in question and his associates set up front companies in the UK, Dubai, Malaysia and the British Virgin Islands (BVI) to re-establish this illicit procurement network.
- The UK company ultimately received payment from a Cypriot bank account opened by the company based in BVI. The Malaysian-based company then exported the aircraft parts from Malaysia to Iran. Many of the Iranian entities were designated under UN and EU sanctions and payments appear to have been made through 3rd party Iranian entities to money exchanges in other Middle Eastern jurisdictions, before being sent to Malaysia. Despite there being several Malaysian front companies, the principal remained the signatory for all bank accounts. Following a thorough investigation, HMRC successfully prosecuted the UK national involved in 2018.
- This case study illustrates the steps proliferating actors may take to obscure their activity and the importance of obtaining accurate beneficial ownership information when undertaking customer due diligence checks.

The role of intermediaries

Case study 6 – establishment of a Scottish Limited Partnership

- An Eastern European business operator used a professional gatekeeper in one of the Baltic states to set up a Scottish Limited Partnership (SLP) to conduct business activity. Unlike traditional brass plate companies, the SLP declared a limited income for the purpose of tax assessment and to satisfy legal requirements. A

representative resident in Scotland signed all SLP filings and returns on behalf of the SLP but was completely unconnected with the SLP or the business operator, thereby reducing the likelihood that they had knowledge of the Eastern European's dealings.

- The representative was paid per item signed. The payment came from the professional gatekeeper's business account in the Baltics and at no point was there any link back to the physical person behind the SLP. The SLP's role was to act as an intermediary for defence related contracts, and for receipt of funds for the contracts. The SLP's bank accounts used for such transactions were based offshore.
- The establishment of the SLP – and its management of payments going to the Eastern European actor – posed a PF risk. A key reflection from this case study, like previous cases, is that the representative in Scotland likely had no knowledge of the potential proliferation activity occurring. As stated previously, it is vital that checks are carried out on all actors involved in a transaction network, particularly where defence-related contracts are the subject.

Case study 7 – the use of intermediary jurisdictions to mask the involvement of designated entities

- An international bank with a UK footprint reported that its customer, the pre-eminent shipping company in its country, had attempted to transfer funds to a non-designated Egyptian shipping and marine supply company via an intermediary bank. That attempted transaction was in connection with services provided by that company relating to a non-designated bulk carrier. The intermediary bank froze the funds as they had ascertained a link between the Egyptian company and a North Korean designated entity. This entity had previously embedded employees in the Egyptian company, which had historically acted as an agent, branch office and vessel manager. The Egyptian company essentially became a front company for the North Korean entity. This link had not initially been apparent to the original reporting bank, with no relevant regulatory licence being in place to permit such a transfer.
- Had the transfer been allowed to continue, it would have potentially posed a proliferation financing risk as the funds would have been made available to a company with historical links to a designated entity involved in proliferation financing and procurement of proliferation-sensitive items. Additionally, this activity involved the use of front and shell companies, foreign intermediaries, indirect payment methods, nationals of proliferating states and shipping companies located in non-proliferating states.
- It was assessed that there was no evidence of sanctions harm in this case, as the funds were not made available to a designated entity and the intermediary bank took effective remedial action. OFSI satisfied itself that the original reporting bank had made and implemented improvements to their compliance processes to prevent similar incidents happening in the future.
- This case study highlights the importance of carrying out sanctions checks against parties involved in transactions, and entities they have links to. Establishing front companies, or even embedding North Korean workers in companies from other jurisdictions, is a tactic used by North Korean proliferators as they seek to evade sanctions regimes. Increased awareness of these PF typologies and robust customer due diligence are therefore key to undermining these sanctions evasion efforts.

The role of state actors in facilitating proliferation financing

3.9 State actors – particularly from the DPRK and Iran – have featured prominently in the previous sections as the key actors behind PF networks impacting the UK financial system. This section will further discuss the role played by these states and others in this activity. While Iran and DPRK feature heavily, the role played by states, including China, in global PF should not be understated and is often not addressed. This section will raise the awareness of the role played by these states to widen the scope of future policy development both by the UK and international partners.

3.10 The case studies and ongoing investigations emphasise the importance of effective implementation, as well as the need to carry out sufficient due diligence on parties in a transaction, and the transaction itself, to ensure that proliferation activity is not taking place. The complicated proliferation networks – such as those outlined in the above examples – highlight the need to not take a transaction at face value and properly assess the risks of illicit actors participating in the transaction, particularly where higher-risk jurisdictions are involved.

The Democratic People's Republic of Korea

3.11 The DPRK's efforts to finance its CBRN programme has been increasingly targeted by the UN Security Council through targeted financial sanctions, aimed at restricting North Korean access to the global financial system. Given this limited access, the DPRK is therefore the primary PF state actor and the UK's role in the global financial system increases the threat posed to the UK by North Korean and North Korean-affiliated proliferating actors. A case study provided above outline specific examples of North Korean PF activity impacting the UK. The role of DPRK actors in the financial sector are addressed in the following section, but there are also other threats which both the UK government and private sector should be aware of:

- North Korean embassies and diplomatic staff have been known to engage in PF activities – generating revenue though extra-diplomatic means, identifying business opportunities for North Korean entities and helping them access the formal financial system (or move cash/goods in diplomatic bags) in violation of UNSC sanctions. North Korean diplomatic property has also been used in some countries to generate revenue.[3] The UK hosts a DPRK embassy in London, which may pose an inherent PF risk for the reasons identified above, although strong controls will mitigate this. Hosting of an embassy and diplomatic staff comes with UN Security Council Resolution requirements as relates to the provision of bank accounts. Whilst awareness of these requirements may exist in the large high-street banks, the full range of banks available in the UK may be less attuned to these UN restrictions.

- The presence of North Korean workers in a country – a practice now banned by the UNSC – also comes with significant risk. Recent work by the Royal

[3] "Berlin court rules hostel at North Korean Embassy must close", DW, 28 January 2020, https://www.dw.com/en/berlin-court-rules-hostel-at-north-korean-embassy-must-close/a-52177730.

United Services Institute (RUSI) showed how North Korean nationals in Malaysia exploited their visa status while working for a UN designated and military-linked entity to raise revenue for the regime in Pyongyang, while procuring items for transport back home.[4] More generally, despite UNSCR 2397 (2017) requiring the repatriation of North Korean workers by December 2019, almost 2 years later these workers continue to generate revenue, much of which returns to the North Korean state. While the UK does not host any North Korean workers, the latest UNSCR 1718 Panel of Experts report highlighted the presence of North Korean nationals in the UK on student visas and the fact that opportunities may exist for them to generate revenue.[5]

- Unless a specific exception applies, North Korea is prohibited by UN sanctions from importing or exporting luxury goods, and Member States are prohibited from importing or exporting luxury goods to or from North Korea. **Luxury goods can be purchased for use by the North Korean regime and resold to affluent members of the North Korean population to generate revenue for the regime which can be used for proliferation purposes**. Luxury goods also serve as important sources of patronage and ensuring the maintenance of elite network structures through the provision of such items. The UK could potentially act as a source of luxury goods for North Korea.

- North Korea also accesses proliferation financing through other means. The UN Panel of Experts have highlighted **multiple cases of illicit ship-to-ship transfers in Chinese jurisdiction**. The March 2021 Panel of Experts report notes that there were 'at least 400 shipments' of coal to Chinese jurisdiction, most of which went to the Ningbo-Zhoushan area, where DPRK vessels continue to offload coal[6]. Additionally, a report by the Centre for Advanced Defense Studies, for example, **highlighted a series of large-scale sand extraction activities carried out by vessels in North Korea's Haeju Bay before transporting it to China**. This activity breached UNSCR 2397 (2017), which – among other provisions – prohibited the supply, sale or transfer of sand from North Korean territory or by its nationals, or using North Korean-flagged aircraft or vessels.[7] Moreover, as noted by a specific report within RUSI's Project SANDSTONE[8], satellite imagery has captured networks of ships – usually foreign-flagged but which are owned by UK-registered companies or previously had links to UK entities – taking on cargo at coal facilities in North Korean ports, before transporting them to foreign jurisdictions. Even though the export of North Korean coal has been prohibited in numerous UNSCRs, North Korea's exports of coal remain one the regime's most

[4] James Byrne and Gary Somerville, "Project Sandstone Report 8: Our Man in Malaysia: The Ri Jong Chol Files", Royal United Services Institute, 14 December 2020, https://rusi.org/publication/other-publications/projectsandstone-report-8-our-man-malaysia-ri-jong-chol-files.

[5] United Nations Security Council Resolution 1718 Committee, S/2020/840, 28 August 2020, p. 42, https://undocs.org/S/2020/840.

[6] United Nations Panel of Experts pursuant to Security Council Resolution 1874 (2009), S/2021/211, 2 March 2021, p.28, https://undocs.org/S/2021/211.

[7] Centre for Advanced Defense Studies, "Against the Grain: Sand Dredging in North Korea", https://c4ads.org/blogposts/against-the-grain.

[8] James Byrne, Joe Byrne and Hamish Macdonald, "Project Sandstone Report 4: Down and Out in Pyongyang and London", Royal United Services Institute, 26 September [continues on next page] 2019,https://rusi.org/sites/default/files/project_sandstone_coal_smuggling_using_uk_companies_final_for_web.pdf

effective means of raising financing for its nuclear and ballistic missile programmes.

3.12 UNSCRs impose significant and meaningful restrictions on the DPRK's ability to procure prohibited materials and technology, and its ability to fund its prohibited programmes. But these restrictions are only effective if they are correctly implemented and enforced. Weak implementation by both public and private sector bodies, such as implementing weak import and export rules or lacking understanding of what can be considered as dual-use items, can be exploited by North Korean actors, leading to further revenue raising to support North Korean proliferation.

Iran

3.13 Although it is not illegal in the UK to trade with Iran, some FIs may feel reluctant in facilitating payments for UK exporters to export goods to Iran, or any financial transaction which involves an Iranian entity. While there are existing UK sanctions targeting Iranian actors, these are targeted so have limited impact on business confidence involving Iranian entities. However, existing US sanctions on Iran are considerably more widespread. Many UK entities have a significant US exposure which can make them reluctant to potentially fall foul of US primary or extraterritorial sanctions. Even in the absence of US exposure, some firms – both in banking and other industries – are still reluctant to take on Iranian business even if it is permitted in the UK. Nonetheless, the UK's Protection of Trading Interests legislation aims to prevent UK firms from ceasing their operations with Iranian entities based on the presence of extraterritorial US sanctions, encouraging legitimate trade with Iran.

3.14 The opaqueness of the Iranian economy and the illicit finance risks posed by it – specifically money laundering and terrorist financing, demonstrated by the FATF following the inclusion of Iran on its list of high risk jurisdictions – also create considerable risks and financial costs for UK companies looking to operate in Iran. Iranian proliferators therefore have less opportunities to support CBRN proliferation financially via licit means, causing them to focus on illicit means to obtain this financing. Although on a smaller scale compared to activities undertaken by the DPRK, Iran therefore operates using many of the same activities to obtain financing for its nuclear weapons programme.

- As with North Korean actors, some case studies and other evidence gathering suggests that Iranian individuals with UK bank accounts receive 3rd party payments from unrelated individuals outside the UK, and payments are then made to a UK company from the UK account.

- Selling oil and other petrochemicals to foreign states, particularly China and Syria, creates significant proliferation financing income for the Iranian regime, despite US sanctions targeting these transactions.

Chapter 4

Vulnerabilities to proliferation financing in the United Kingdom

4.1 The UK economy's size and openness, as well as being one of the largest financial services exporters and a major centre for professional services, has great benefits for UK competitiveness and makes London particularly attractive for foreign investors. These factors make the UK attractive for legitimate business, but also do leave it vulnerable to proliferating actors looking to exploit the UK's key role in the global financial system. The UK's global economic role is also more significant to the UK compared to more traditional threats posed by proliferating states or actors, such as geographic proximity.

4.2 Using evidence obtained for this assessment, this chapter highlights those sectors in the UK economy which are most likely to be targeted by proliferating actors. This will indicate where the UK's economy is likely to be more exposed to PF risks. However, there are sectors which have not been covered and every part of the UK economy could be exploited to contribute to the financing of CBRN proliferation.

The UK's role as a global financial centre

4.3 Given the UK's role as a global financial centre, the UK's financial system presents unique opportunities for proliferating actors to access wide ranging financial services and technologies to support their proliferating activity. Understanding this exposure is key to further improve mitigation strategies to protect the UK economy from proliferating actors.

Vulnerabilities posed by the UK's global role in finance

4.4 The UK is particularly vulnerable to several threats which arise primarily due to the UK's position in the global economy. These include:

- **Payments linked to proliferation-related activities or actors** may interact with the UK financial system or overseas branches/subsidiaries of UK-headquartered financial institutions.

- Many UK-headquartered financial institutions have **wide-reaching operations around the world. This includes countries that are particularly exposed to PF activities**, for example those in Asia, due to the presence of active PF networks in those countries or the trade between those countries and proliferating states.

- Local branches and subsidiaries of UK headquartered banks **may facilitate access to financial services for proliferation actors operating in these countries** either directly or through links to local national banks with insufficient compliance controls.

- Even if proliferation-sensitive items and technology are not shipped from or through the UK, the **financial transactions for this trade may be facilitated by or cleared through the UK and auxiliary services**, such as insurance, or could be purchased in the UK.

The insurance and maritime sector

4.5 The London insurance market is key for global maritime insurance products, including Hull & Machinery insurance, Cargo insurance and Liability insurance through Protection and Indemnity[1] insurance clubs. The most significant PF exposure within the UK maritime insurance market comes from reinsurance into London, particularly when the primary insurer is located in Asia. This risk is somewhat similar to the risk posed by correspondent banking as the UK insurance provider is removed from the original underwriting process and will have limited awareness of the due diligence and sanctions screening that was undertaken by the primary insurer. Although UK insurers are aware of their sanctions obligations, primary insurers in other jurisdictions sometimes have limited compliance processes. Insurers in London often rely on so-called sanctions clauses which retroactively halt insurance services if a vessel is found to have been involved in sanctioned activities. However, the insurance sector is largely reliant on the information the customer has provided and it may not always be practically possible for the sector to proactively investigate shipments, for example, to ensure that proliferation-sensitive items are not being masked by false documentation.

4.6 Insurance relating to the maritime sector and the maritime sector more broadly are frequently targeted by proliferating actors, as seen in the case study provided in the 'Direct threats' section. 95% of all UK imports and exports are moved by sea and the maritime sector contributes over £14bn to the UK economy each year, supporting an estimated 186,000 jobs[2]. The UK government is aware of arrangements for marine insurance for oil and gas carriers used by sanctioned destinations, as well as carriers shipping prohibited items in quantity or through clandestine means by sea freight, be they legitimately defence-related or sanctions noncompliant. Vessels can be used by proliferators to either transport proliferation-sensitive items or, more frequently, engage in other forms of prohibited trade. These vessels may seek insurance from, or be reinsured by, UK-based providers. Additionally, insurance for illicit business conducted in third countries obtained by British

[1] Protection and indemnity (P&I) insurance covers risks not usually covered by more traditional maritime insurance. These risks include war risks and environmental damage.

[2] Department for Transport, "UK Port Freight Statistics 2019", 12 August 2020, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/908558/port-freight-statistics-2019.pdf

"Brass Plate" companies, usually for illicit procurement of defence materials, is also an issue we have seen during our evidence gathering.

The ease of establishing companies in the UK

4.7 Corporate registration here can serve as a green flag for companies wishing to access the UK financial system and may allow proliferation-linked companies to access financial services in proliferation and PF-exposed countries. Key actors in this area can create front companies to carry out procurement business. If the use of one entity for illicit activity has been uncovered during a business transaction, it can be quickly withdrawn and replaced by a new entity to carry out the same activities for future transactions. It is also possible to use a Trust or Company Service Provider (TCSP) to buy 'shelf' companies with established banking and credit histories, in order to create the impression of a reputable company, or use a nominee shareholder or directors, in order to increase the anonymity of the beneficial owners of a company.

4.8 The UK register of companies, held at Companies House, has played an important role in underpinning a strong, transparent and attractive business environment in the UK. Valued at up to £3bn per year, the register is accessed over 9.4 billion times a year, helping business people obtain assurance over potential suppliers and partners. However, the same factors that make our framework successful make it attractive to exploitation. UK Companies House has been linked to a number of PF cases and may be exploited similarly in the future. For example, in December 2020, the US Treasury sanctioned a number of UK-based entities that had been used to own vessels trading North Korean coal in violation of United Nations Security Council (UNSC) resolutions.[3] In some cases, shell companies have been set up and used in the UK by one of China's largest North Korean cross-border traders who had acted on behalf of sanctioned North Korean proliferators and had helped them procure items for their weapons programme while laundering tens of millions of dollars on their behalf.[4]

4.9 The Government has set out its plans to reform Companies House, boosting its potential as an enabler of business transactions and economic growth, but also giving it a bigger role in combatting economic crime. The reforms will, amongst other things, deliver more reliably accurate information on the companies register, reinforced by verification of the identity of people who manage or control companies, and anyone else submitting filings; and

[3] James Byrne, Joe Byrne and Hamish Macdonald, "Project Sandstone Report 4: Down and Out in Pyongyang and London", Royal United Services Institute, 26 September 2019, https://rusi.org/sites/default/files/project_sandstone_coal_smuggling_using_uk_companies_final_for_web.pdf.

[4] US Department of Justice, "Four Chinese Nationals and Chinese Company Indicted for Conspiracy to Defraud the United States and Evade Sanctions", 23 July 2019, https://www.justice.gov/opa/pr/four-chinese-nationalsand-chinese-company-indicted-conspiracy-defraud-united-states-and.

greater powers for Companies House to query and challenge the information submitted to it.

Designated Non-Financial Businesses and Professions (DNFBPs)

4.10 Awareness of PF risk in the DNFBP sector is, in general, low in most countries, and globally the PF focus continues to be on financial institutions. Given the important role UK DNFBPs play in facilitating global finance, this could represent a particular risk to the UK, notably in relation to trust and company service providers given the ease of establishing companies in the UK.

UK Crown Dependencies and Overseas Territories

4.11 The close economic ties between the UK, the CDs and OTs generate significant economic benefits. However, criminals seek to exploit this close relationship and try to disguise illicit assets by taking advantage of existing channels and strong business connections. CDs and OTs continue to feature prominently in UK illicit finance investigations and reporting, and financial centres in the CDs and OTs may be used by proliferators for PF purposes, particularly for the establishment of corporate entities or for accessing the formal financial system.

The role of cryptocurrencies in facilitating proliferation financing

4.12 There has been an increasing global trend in recent years of sanctioned actors utilizing cryptocurrencies and other new technologies to evade international sanctions regimes, given the reduced oversight of international trade facilitated by cryptocurrencies[5]. Particularly where this activity involves actors connected to North Korea and Iran, there is a considerable PF risk where sanctions evasion takes place. The use of cryptocurrencies as both a tool for fund raising – such as via hacking exchanges or receipt of payments – as well as fund movement, has allowed North Korea to evade the traditional financial system in a new way that does not require a physical presence in the target countries. The DPRK's PF-related cybercrime activities span the globe and have included theft and laundering from and through international FIs, central banks and cryptocurrency businesses, such as exchanges.[6] The most recent UN Panel of Experts report on DPRK highlighted global cyberactivity on behalf of the North Korean regime, where an estimated $316.4 million worth of virtual assets were stolen by North Korea between 2019-2020.[7] Additionally, Iran is

[5] Shannon Vavra, "How cryptocurrencies are being used to evade sanctions", Axios, 2 February 2018 https://www.axios.com/how-cryptocurrencies-used-to-evade-sanctions-b752de25-0c2e-42f1-a04c-33aad930c6ed.html

[6] For more on North Korean use of cryptocurrencies for sanctions evasion, please see David Carlisle and Kayla Izenman, "Closing the Crypto Gap: Guidance for Countering North Korean Cryptocurrency Activity in Southeast Asia", Royal United Services Institute, 14 April 2019, https://rusi.org/publication/occasional-papers/closingcrypto-gap-guidance-countering-north-korean-cryptocurrency.

[7] United Nations Security Council Resolution Committee 1718, S/2021/211, 4 March 2021, p. 56, https://undocs.org/S/2021/211

considering the launch of a Central Bank Digital Currency to operate as part of an alternative financial system. It also raises money through the mining of cryptocurrencies.

4.13 The UK has a robust cryptocurrency industry, with over 2 million people estimated to own cryptocurrencies in the country.[8] UK consumers have also been found to rely heavily on non-UK based exchanges. In January 2020, the Government brought certain cryptoasset businesses into scope of the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer). The FCA was appointed as the AML/CTF supervisor for these businesses and their AML regime began on the same day with a registration regime for these firms. The AML regime also includes a toolkit to assess applications, and to take appropriate action where failings were identified that went beyond those powers available for other businesses the FCA supervises purely under the MLRs. The FCA has noted that a significantly high number of businesses are not meeting the required standards under the MLRs, resulting in an unprecedented number of businesses withdrawing their applications. The FCA will continue robust assessments of other applications up until 31 March 2022. There is still more to be done by these businesses to develop comprehensive AML programmes and for the UK to meet the FATF standards for these businesses, including implementation of the so called FATF travel rule[9].

The UK's role in global defence (including dual-use items) manufacturing

4.14 As the world's second largest defence exporter and third largest security exporter[10], the UK's industrial sectors in these areas provide widespread opportunities for proliferating actors to obtain proliferation-sensitive items. While the procurement of such items for illicit purposes is not a risk that is specifically focused on proliferation financing, the financial means to obtain the items clearly fall within its scope. Therefore, the UK's leading defence sector attracts proliferating actors and the financial means they employ to obtain these items.

4.15 All UK sectors connected to production of military and dual-use items can be exploited by proliferating actors. This includes sectors such as chemical production and the life sciences. However, the specific entities that a proliferating actor approaches depends on whether they are a state or non-state entity. Major defence suppliers tend not to supply to private entities unless supported by a verified government contract, and eventual supply

[8] Financial Conduct Authority, "Research Note: Cryptoasset consumer research 2020", 30 June 2020, p. 5, https://www.fca.org.uk/publication/research/research-note-cryptoasset-consumer-research-2020.pdf.

[9] Under the FATF's Recommendation 16, the originators and beneficiaries of all transfers of digital funds must exchange identifying information. This intends to mitigate the AML/CTF challenges associated with the increasing global use of cryptocurrency.

[10] Department for International Trade and UK Defence and Security Exports, "UK defence and security exports statistics for 2019", 6 October 2020, https://www.gov.uk/government/statistics/uk-defence-and-security-export-statistics-for-2019/uk-defence-and-security-export-statistics-for-2019

depends on securing a UK export licence. Most at risk are medium-sized defence sub-contractors and the dual-use items sector, where there may be less awareness of proliferation risks and suppliers' export control and other obligations, for example under the Chemical Weapons Act. Small arms and light weapons; small arms ammunitions and tank/artillery munitions; individual ballistic protection; vehicle armour and vehicles; communications (also dual-use); chemical and biological materials and related equipment, are types of items that attract procurement attempts from overseas actors.

4.16 Nonetheless, the UK's stringent export controls limit opportunities for proliferating actors to procure CBRN-related materials. The UK operates its own export control regimes and complies with international regimes, such as the Australia Group and the Wassenaar Agreement to ensure that the trade in dual-use and sensitive items does not pose a threat to international security. Such items are most likely to be transhipped through other jurisdictions, such as China. For example, North Korean front companies and those acting on their behalf often route shipments through Liaoning province in China, meaning that the relevant payment architecture and correspondent banking relationships are maintained with Chinese financial institutions.[11]

The UK's role as a global education hub

4.17 Research taking place at British universities in specific technologies – particularly those that could have a role in a CBRN programme – is particularly vulnerable to influence from proliferating actors. Increasing levels of funding from overseas to British academic institutions makes the sector vulnerable to potential pressure from states with proliferating ambitions, especially where there are links to CBRN-linked research. Influence of other states over UK academic institutions can lead to both a financial dependence on these governments and an increase in research and other academic transfer to those states[12]. Government policy on foreign interference in universities is country agnostic and is designed to protect against all actors who seek to misuse our world-leading higher education sector. We continue to work with the sector to mitigate specific risks and, within the context of this document, consideration should be given to the presence of expert researchers with links to proliferating states who may pose a proliferation vulnerability, as these individuals could obtain proliferation-sensitive material during research and development at UK academic institutions.

4.18 To counter these risks, the government is working with universities, funding bodies and industry to protect our higher education and research sector from hostile interference. For example, the government is running the

[11] James Byrne, Joe Byrne, Gary Somerville and Hamish Macdonald, "Project Sandstone Report 7: The Billion Dollar Border Town: North Korea's Trade Networks in Dandong", Royal United Services Institute, 4 September 2020, https://rusi.org/publication/other-publications/project-sandstone-report-7-billion-dollar-border-town.

[12] House of Commons Foreign Affairs Committee, "A cautious embrace: defending democracy in an age of autocracies", 4 November 2019, https://publications.parliament.uk/pa/cm201919/cmselect/cmfaff/109/109.pdf

Trusted Research campaign[13] and supporting Universities UK to implement guidelines[14] which are designed to help universities make informed decisions on risk in international collaborations. Also, BEIS recently announced a new Research Collaboration Advice Team to promote government advice on security-related topics, such as export controls, cyber security and protection of intellectual property. It will ensure researchers' work is protected, and that the UK research sector remains open and secure.

4.19 In addition, the Academic Technology Approval Scheme (ATAS) requires foreign individuals to apply for an ATAS certificate to study certain subjects in the UK. The Scheme applies to all international students and researchers – apart from exempt nationalities – which are subject to UK immigration controls and intend to be involved in postgraduate level study or research in specific sensitive subjects. These subjects include those where knowledge gained from the work could be used to develop conventional military technology, CBRN-related material or their means of delivery. These measures are supported by one of the most robust export control regimes in the world. The UK rigorously assesses all export licences against strict criteria and has worked with academia to provide updated guidance on export controls that is more specific to their needs.

Limited awareness in elements of the UK economy of proliferation financing

4.20 From our evidence gathering and engagement with government and private sector partners during this assessment, we judge there to be limited awareness in elements of the industrial sector of proliferation procurement methodologies. For example, case study 4 demonstrates insufficient checks to minimise the risk of proliferating actors purchasing high risk goods or items. A lack of awareness of PF in parts of the UK economy can lead to a lack of understanding of how certain industrial products may be manipulated for hostile use or for use in a CBRN programme. An added vulnerability is the fact that some businesses may operate on very low margins. The need for the business to remain financially viable can therefore at times be a factor in limiting the appetite to turn away orders that may contain red flags from a compliance perspective, and these are the companies most at risk from approaches from proliferating actors. Moreover, limited understanding of PF across the UK economy more broadly can at times reduce compliance checks simply because there is a lack of awareness of the role played by PF actors, as noted in case studies 3 and 6.

[13] Centre for the Protection of National Infrastructure, "Trusted Research Guidance for Academia", 29 May 2020, https://www.cpni.gov.uk/trusted-research-guidance-academia

[14] Universities UK, "Managing Risks in Internationalisation: Security Related Issues", https://www.universitiesuk.ac.uk/policy-and-analysis/reports/Documents/2020/managing-risks-in-internationalisation.pdf

Chapter 5
Conclusion

The UK's counter-proliferation regime

5.1 The evidence gathering stage of this assessment highlighted the robust CP legal framework in place in the UK to protect the country from PF. The UK's autonomous financial sanctions regimes targeting CBRN proliferation – as well as UN sanctions regimes implemented in the UK, export control regimes and other tools available to the UK government – limit opportunities for proliferating actors to exploit the UK to obtain financing for CBRN capabilities. Additionally, this assessment will be updated periodically to reflect new threats and risks in the PF space. As with the ML/TF NRA, updating this document to reflect these new challenges will inform more effective UK policy in countering PF.

The UK's role in the global economy

5.2 As we have seen, the size and characteristics of the UK economy mean that it is highly likely that proliferating actors will target the UK to gain financing for CBRN proliferation despite the robust controls in place to prevent this. The UK's financial services industry, particularly the banking and insurance sectors and the ease of establishing companies in the UK, is especially at risk. We have seen case studies of individuals and entities evading financial sanctions regimes to obtain financial services products, for example, which highlight the attractiveness of the UK to these actors. Nonetheless, as noted above, the strength of the UK's legal framework in combatting these efforts to exploit the UK economy for PF purposes greatly inhibits proliferating actors' activities in the UK.

Proliferation financing as an independent risk

5.3 When gathering evidence on PF activity with government, private sector and academic partners, it became clear that PF is often considered alongside other illicit finance risks, particularly terrorist financing and money laundering, rather than as an independent risk which should be considered separately from other illicit activity. The UK has long supported a greater focus on PF risks and has advocated for changes to the FATF's standards to strengthen requirements in this area. The new FATF standards recommend countries undertake national risk assessments on PF and impose new requirements for relevant persons to undertake their own risk assessments.

HM Treasury therefore plans to introduce new provisions to the UK's Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations to require both the UK government and private sector to carry out PF risk assessments in the same way that they do currently for ML and TF. HM Treasury is currently carrying out a consultation on these proposed regulatory amendments which is due to end in October 2021. It is hoped that the increased understanding and awareness of PF risk resulting from these new requirements would help to inform future iterations of this National Risk Assessment.

Glossary

5MLD	EU Fifth Money Laundering Directive
AML/CTF	Anti-money laundering and counter-terrorist financing
ATAS	Academic Technology Approval Scheme
BEIS	Department for Business, Energy and Industrial Strategy
CBRN	Chemical, Biological, Radiological and Nuclear material and weapons
CDs and OTs	Crown Dependencies and Overseas Territories
CP	Counter-proliferation
DIT	Department for International Trade
DNFBPs	Designated Non-Financial Businesses and Professions
DPRK	Democratic People's Republic of Korea
FATF	Financial Action Task Force
FCA	Financial Conduct Authority
FCDO	Foreign, Commonwealth and Development Office
FI	Financial institution
HMRC	Her Majesty's Revenue and Customs
MOD	Ministry of Defence
NRA	National risk assessment
OFSI	Office of Financial Sanctions Implementation
PF	Proliferation financing
POCA	Proceeds of Crime Act 2020
RUSI	Royal United Services Institute
SAMLA	Sanctions and Anti-Money Laundering Act
UN	United Nations
UNSCR	United Nations Security Council Resolution

HM Treasury contacts

This document can be downloaded from www.gov.uk

If you require this information in an alternative format or have general enquiries about HM Treasury and its work, contact:

Correspondence Team
HM Treasury
1 Horse Guards Road
London
SW1A 2HQ

Tel: 020 7270 5000

Email: public.enquiries@hmtreasury.gov.uk