Gibraltar Financial Intelligence Unit
HM Government of Gibraltar

GIBRALTAR FINANCIAL SERVICES COMMISSION

Counter Proliferation Financing

Guidance Notes

Jun 2020

Table of Contents

Scope

This guidance is produced by the Gibraltar Financial Intelligence Unit (GFIU) in collaboration with the Gibraltar Financial Services Commission (GFSC). While it refers mainly to banks, Distributed Ledger Technology (DLT) service providers, trust & company service providers (TCSPs) and insurance sectors, the sound practices described, with the appropriate modifications, would similarly be relevant and applicable to other reporting entities. A number of sources have been used to compile these guidance notes and we are grateful for the support provided by the Royal United Services Institute and Dr Jonathan Brewer. However, the GFIU advises that you should always also refer to the relevant, up-to-date legislation. Please note that the relevant competent authority in Gibraltar would consider each matter on the facts, and the specific legal requirements that apply. Neither the GFIU nor the Gibraltar competent authorities can issue definitive guidance on how the law might be applied in a particular case or how an EU or Gibraltar court might interpret the law. These guidance notes must be read with the Sanctions Guidance Notes issued by the GFIU which can be found here.

Finally, this guidance does not represent legal advice. If you are unsure about your obligations in a given case, you should take independent legal advice.

Introduction

One of the main functions of the GFIU is gathering, storing, analysing and disseminating intelligence related to the proliferation of weapons of mass destruction. As a financial centre, Gibraltar specialises in providing banking, TCSP, DLT and general insurance services. Gibraltar has international obligations to ensure that it has measures in place to adopt the United Nations Security Council Resolutions (UNSCRs) to combat proliferation financing. However, it is neither a weapons manufacturing jurisdiction nor an international trade centre or a market of proliferation goods. Gibraltar's port mainly serves as a transit point and are very limited to provisions and ship spares. Whilst there is no data or evidence to suggest that proliferation or proliferation financing has been experienced, it is important that reporting entities are aware of their international and domestic obligations. The threat is negligible but instances of proliferation financing within Gibraltar's finance centre cannot be discarded.

The proliferation of weapons of mass destruction (WMD) including their means of delivery is a significant threat to global security. Proliferation and the financing of it is quickly evolving as threat actors find innovative ways in disguising the funds using complex web structures. In the latest United Nations (UN) Panel of Experts Report, it highlights that the main vulnerability points for financial institutions are cyber activity which opens new opportunities in areas such as DLT and the abuse of the financial system by threat actors.

Any enhancements to strengthen Gibraltar's measures in countering proliferation financing will also strengthen the protective framework and contribute to global security.

1 Overview of Proliferation Financing

1.1 What is proliferation?

Proliferation is the manufacture, acquisition, possession, development, export, transhipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials (including both technologies and dual-use goods used for non-legitimate purposes), in contravention of national laws or, where applicable, international obligations. It includes technology, goods, software, services or expertise.

1.2 What is proliferation financing?

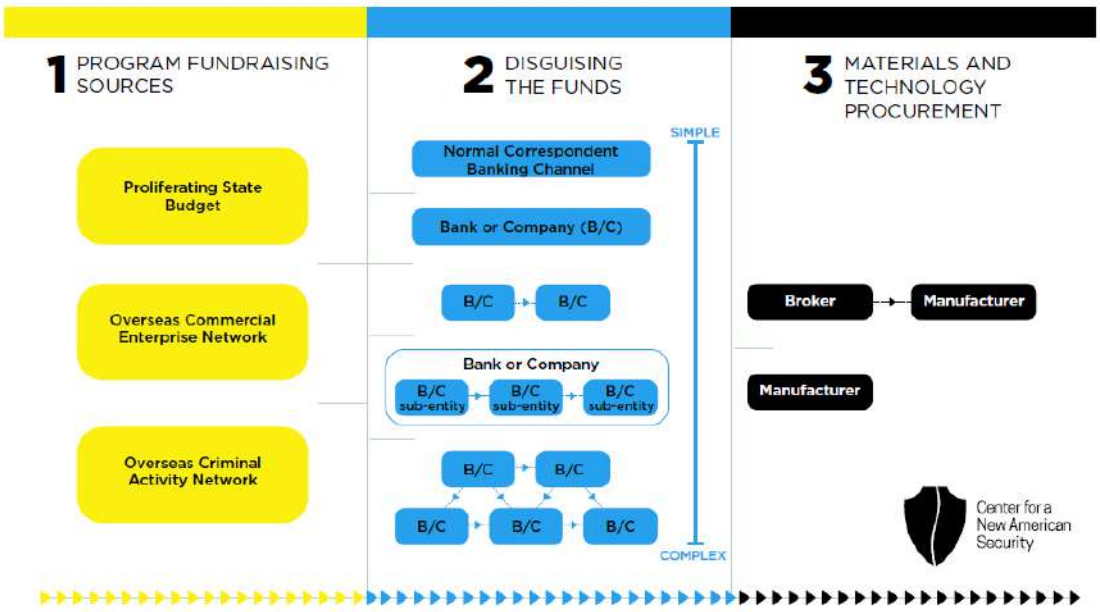
There is no international definition of proliferation financing. However, the FATF produced a working definition of proliferation financing based on UNSCR 1540, which reads as follows:

"Proliferation financing" refers to: the act of providing funds or financial services which are used, in whole or in part, for the manufacture, acquisition, possession, 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.

1.3 Three stages of proliferation financing

A report by the Centre for a New American Security (CNAS) described the financial elements of a WMD program which is broken down into three stages (as depicted in Figure 1 (courtesy of the Centre for a New American Security):

Figure 1. Three stages of FoP



Program fundraising sources: A proliferating country raises financial resources for in-country costs.

Disguising the funds: The proliferating state moves assets into the international financial system, often involving a foreign exchange transaction, for trade purposes.

Materials and technology procurement: The proliferating state or its agents uses these resources for procurement of materials and technology within the international financial system.

1.4 Comparison between Money laundering, Terrorist Financing and Proliferation Financing

	Money Laundering	Terrorist Financing	Proliferation Financing
Source of Funds	Internally from within criminal organisations	Internally from self-funding cells (centred on criminal activity)	Often state-sponsored programs but also through fundraising activities by non-state actors
Conduits	Favours formal financial system	Favours cash couriers or informal financial systems such as Hawala and currency exchange firms	Formal financial system preferred up until the point of entry into DPRK, where the money is then taken out in cash in a neighbouring country and carried in to DPRK. Additionally, the use of DLT has become a widely used mechanism to settle transactions for DPRK
Detection Focus	Suspicious transactions such as deposits uncharacteristic of customer's wealth or the expected activity	Suspicious relationships, such as wire transfers between seemingly unrelated parties	Individuals, entities, states, goods and materials, activities
Transaction Amounts	Large amounts often structured to avoid reporting requirements	Small amounts usually below reporting thresholds	Moderate amounts

Financial Activity	Complex web of transactions often involving shell or front companies, bearer shares, offshore secrecy havens	Varied methods including formal banking system, informal value-transfer systems, smuggling of cash and valuables	Transactions look like normal commercial activity, structured to hide connection to proliferator or proliferation activities
Money Trail	Circular – money eventually ends up with the person who generated it	Linear – money generated is used to propagate terrorist groups and activities	Linear – money is used to purchase goods and materials from brokers or manufacturers. The money can also move in the opposite direction (i.e. from the broker/ manufacturer to the proliferator).

This chart is based on a presentation by James R Richards, Wells Fargo, 2005, quoted in the CAMS Examination Study Guide 5th Edition.

1.5 Why is the prevention and detection of proliferation financing important?

Proliferation financing facilitates the movement and development of proliferation-sensitive goods. The movement and development of such items can contribute to global instability and if proliferation-sensitive items are deployed, this may ultimately result in the loss of life.

1.6 What are the difficulties faced with identifying proliferation financing?

There are a number of challenges associated with identifying proliferation financing:

- The identification and assessment of proliferation financing can be very complex. It may take extensive training and practice for the authorities to better their understanding in detecting and reviewing the source of these funds.
- There is a growing trend in the purchase and sale of elementary components, as opposed to whole manufactured systems, for proliferation purposes. These are described as dual-use goods which are difficult to identify, requiring specialist knowledge of the item. These may also have perfectly legitimate uses making it challenging, at times, to ascertain the intention behind the use of those goods and whether they will be used for illicit purposes.
- The networks through which proliferation-sensitive goods may be obtained tend to be complex. Front companies, agents and other intermediaries are often used to cover up the ultimate end-user. The lack of transparency and opaque processes allow for proliferation sensitive goods, the entities involved, the linked transactions and the ultimate end-user to avoid detection, significantly increasing the risk of proliferation financing.

- This subject has not yet been very elaborated on or researched by other jurisdictions making it challenging to assess and identify through relevant experience, the risks and typologies associated with proliferation financing.

2 Counter Proliferation Financing Obligations

Frameworks to combat proliferation financing rely on three interlinked layers of obligation: international legal obligations put into place by the United Nations Security Council, the Financial Action Task Force recommendations and domestic legislation. All three of these layers impose requirements which impact the risk management practices of the reporting entities in the finance sector.

2.1 International Obligations

In order to address the risk of proliferation financing, all states should take steps to comply with international obligations by establishing a legislative and institutional framework.

United Nations
Member states are required to implement the mandatory key UN Security Council Resolutions (UNSCR) which address proliferation financing under Chapter VII of the UN Charter. The UN Security Council has adopted a two-tier approach, which includes both the implementation of broad provisions covering all non-state actors, as well as targeting jurisdictions who have been specifically identified for their proliferation of WMD. The broad-based provisions for combatting and prohibiting the financing of proliferation related activities for non-state actors falls under:

- **UN Security Council Resolution 1540** (2004), requires countries to prohibit any non-state actor from financing the manufacture, acquisition, possession, development, transfer, or use of weapons of mass destruction. In addition, states must establish, develop, review and maintain appropriate controls on providing funds and services, such as financing, related to the export and trans-shipment of items that would contribute to weapons of mass destruction proliferation.

The UN Security Council has passed a series of resolutions imposing sanctions on the Democratic People's Republic of Korea (DPRK) and the Islamic Republic of Iran. The country specific approach adopted with regard to targeted financial sanctions related to the financing of proliferation of WMD fall under:

- **UN Security Council Resolution 1718** (2006) and all successor resolutions concerning the DPRK; and
- **UN Security Council Resolution 2231** (2015) endorsing the Joint Comprehensive Plan of Action on Iran, and replacing previous resolutions related to Iran.

The UNSC resolutions establishes a series of obligations on member states relating to the DPRK and Iran. This includes the use of targeted Financial Sanctions against designated individuals and entities listed on both Resolutions 1718 and 2231, as well as those acting on, behalf, or at the direction of designated persons or entities, or those owned/controlled by designated persons and entities.

The Resolutions also contain measures specific to the DPRK and Islamic Republic of Iran. In the case of Iran, this includes measures in relation to specific commercial activities, such as ballistic missiles. In the case of the DPRK, the following specific financial measures apply:

- Freezing of any funds, other financial assets or economic resources that are owned or controlled, directly or indirectly, by entities of the Government of the DPRK or the Worker's Party of Korea, or by persons or entities acting on their behalf or at their direction, or by entities owned or controlled by them. This extends to any funds that the state determines are associated with the DPRKs nuclear or ballistic missile programme or any other relevant activities prohibited by the UNSCR;
- The definition of economic resources extends to vessels under UNSCR 2270;
- Prohibition on financing related to the export and import of controlled items with North Korea; and
- Other financial measures often referred to as activity-based restrictions. This includes relationships with DPRK financial institutions, joint ventures with North Korea businesses, etc.

Financial Action Task Force

A reporting entity's implementation procedures should also be in line with the Financial Action Task Force (FATF) criteria for the implementation of targeted financial sanctions. These are prescribed in the FATF's recommendations, interpretative notes and methodology. In 2012, the FATF incorporated two new recommendations on combating proliferation financing within its standards:

- **Recommendation 2** calls on countries to 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.

- **Recommendation 7** directs countries to implement targeted financial sanctions to comply with UNSCRs relating to the prevention, suppression and disruption of proliferation of weapons of mass destruction and it's financing. These resolutions require countries to freeze without delay the funds or other assets of, and to ensure that no funds and other assets are made available, directly or indirectly, to or for the benefit of, 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

2.2 Domestic Obligations

In addition to the international obligations, there are offences in Gibraltar law relevant to the development, production, acquisition, retention and transfer of nuclear, biological and chemical weapons, pursuant to the **Weapons of Mass Destruction Act 2004**. As a British Overseas Territory, Gibraltar is also required to adhere to the legislative requirements set out under the Chemical Weapons (Sanctions) (Overseas Territories) Order 2018.

Domestic legislation also applies certain measures to give effect to decisions under Council Regulations (EU) which relates to the Democratic People's Republic of Korea (DPRK) Sanction Order 2018. This order repeals the DPRK Sanction Order 2016 and creates offences which include; making funds or economic resources available to a designated person (except where an exemption applies or under licence), dealing with funds or economic resources that must be frozen (except where an exemption applies or under licence); and failing to comply with reporting obligations, activities that circumvent an asset freeze, and breaches of licensing conditions.

2.3 Reporting Obligations

The FATF considers the threats related to proliferation financing to be interconnected with terrorism and terrorism financing based on the fact that proliferation might be a means for supporting the undertaking of terrorist activities. Gibraltar's comprehensive legal framework governing targeted financial sanctions and proliferation financing is covered by a number of pieces of legislation. These relate to the obligations to report suspicious activity or report the assets of a designated person or entity.

Under the Proceeds of Crimes Act 2015, a person commits an offence if he enters into or becomes concerned in an arrangement which he knows or suspects facilitates (by whatever means) the acquisition, retention, use or control of criminal property by or on behalf of another person.

Where a person believes or suspects that another person has committed an offence under any of sections 35 to 39 of the Terrorism Act 2018, or when there is a suspicion or belief that any money or other property is terrorist property or is derived from terrorist property may disclose that information as soon as reasonably practicable.

Reports of frozen funds and economic resources, information regarding a designated person, and notifications of credits to frozen accounts should be reported to the Gibraltar competent authority (for further information on reporting process refer to the Financial Sanctions Guidance Notes). For non-targeted financial sanctions reports see section 6 below.

2.4 Getting updates

The United Nations Security Council Resolutions pertaining to non-proliferation can be accessed directly via the following links:

http://unscr.com/en/resolutions/1540

http://unscr.com/en/resolutions/1718

http://unscr.com/en/resolutions/2231

Additionally, the consolidated UN Security Council sanctions list can be accessed here:

https://www.un.org/securitycouncil/content/un-sc-consolidated-list

2.5 What are the penalties related to weapons of mass destruction?

There are a wide range of penalties that can be applied against proliferators and other individuals in Gibraltar law relevant to the development, production, acquisition, and possession of WMD. Some examples are outlined in the table below:

Legislation	Offence	Maximum Penalty	Type
Weapons of Mass Destruction Act 2004	Section 43 - Use of Nuclear Weapons	A person guilty of an offence under this section is liable on conviction on indictment to imprisonment for life.	Nuclear
Weapons of Mass Destruction Act 2004	Section 3 - Restriction on development etc. of certain biological agents and toxins and of biological weapons.	Any person contravening this section shall be guilty of an offence and shall, on conviction on indictment, be liable to imprisonment for life.	Biological
The Chemical Weapons (Sanctions) (Overseas Territories) Order 2018	Section 4 – Dealing with funds and economic resources; Section 13 - Circumvention and contravention of prohibitions	A person guilty of an offence under this section is liable on conviction on indictment, to a fine or to imprisonment for a term not exceeding seven years, or to both.	Chemical

2.6 What are the penalties for failing to report?

There are a number of penalties that exist in Gibraltar's legal framework for failing to report breaches of targeted financial sanctions and non-targeted financial sanctions.

The following table shows some of the relevant legislation.

Legislation	Offence	Maximum Penalty
Democratic People's Republic of Korea (DPRK) Sanction Order 2018	Section 27(1) Penalties	A person guilty of an offence under paragraphs 24 or 25 is liable, on summary conviction, to imprisonment for a term not exceeding three months or to a fine or to both; or on indictment, to imprisonment for a term not exceeding two years or to a fine or to both.
Proceeds of Crimes Act 2015	Section 6B(3) Failure to disclose	A person guilty of an offence under this section is liable on summary conviction, to imprisonment for a term not exceeding six months or to a fine not exceeding level 5 on the standard scale or to both; or on conviction on indictment, to imprisonment for a term not exceeding fourteen years or to a fine or to both.
Terrorism Act 2018	Section 46(14) Failure to disclose	A person guilty of an offence under this section is liable on conviction on indictment, to imprisonment for a term not exceeding 5 years or to a fine or to both; on summary conviction, to imprisonment for a term not exceeding 6 months or to a fine not exceeding the statutory maximum or to both.
Sanctions Act 2019	Section 51(1) General Penalty	A person who commits an offence for which no separate penalty is provided for is liable on summary conviction to a fine not exceeding level 5 on the standard scale or to imprisonment for a term not exceeding 12 months, or to both; on conviction on indictment to a fine or to a term of imprisonment not exceeding 10 years, or to both.

3 Risk Assessment

The FATF emphasises the importance of appropriate risk mitigation and assessment programmes in establishing a sound framework with robust controls. Reporting entities must employ a risk-based approach when considering how to introduce the risk of proliferation financing within their overall risk assessment process. Firms with exposure to a greater variety of risks, such as, those with international client bases, would be expected to include an assessment of proliferation financing risk within their risk management framework. This approach adopted by the firm could be the same as that to money laundering and terrorist financing risks but with an additional focus on proliferation financing.

The Stockholm International Peace Research Institute (SIPRI) guidance published in September 2016 recommends that this assessment include consideration of the following factors:

- Client base;
- Details on the modality of the transaction, including the importer, exporter, collection and delivery addresses;
- Other entities involved in the supply chain, such as subcontractors;
- Associates and business partners; and
- Employees.

Any risk assessment practises related to proliferation financing should be proportionate with the overall proliferation risk that is associated with the activities and services provided by reporting entities. Established mechanisms that are applied to conduct risk assessments for identifying suspicious activity of criminal conduct may be applicable to proliferation financing

The table below (used for national risk assessments but equally applicable to reporting entities) provides a comparison of factors which may impact a firm's assessment of the money laundering, terrorist financing and proliferation financing risks:

Money Laundering	Terrorist Financing	Proliferation Financing
May have comparatively more data and statistics	May have comparatively more data and statistics although case numbers and volume of funds may be low	Limited data, limited cases
Clear international definition	International definition, with some differences in interpretation	No international definition of proliferation financing
International financial channels, correspondent banking relationships, offshore financial products and services are relevant considerations	National risk exposure may have regional or global links to actors, networks, and activities, including recruitment & fundraising methods	National risk exposure difficult to detect without regional and global analysis of proliferation pathways and revenue raising activities
Threats generally defined in terms of predicate crimes	Threats generally defined in terms of terrorist actors	Threats cannot be defined strictly in terms of predicate crimes or proliferation actors
Consequences easier to quantify in terms of monetary value	Consequences include non-quantifiable impacts on human life, infrastructure and the environment	Consequences include non-quantifiable impacts on human life, infrastructure and the environment

This table forms part of a presentation by RUSI on Proliferation Financing delivered in Gibraltar in October 2019.

Particular jurisdictions may have an increased exposure to proliferation or proliferation financing risks. Factors that may contribute to the level of exposure include:

- Whether the jurisdiction hosts a major financial centre, and is thus more likely to be exploited in order to facilitate illicit financial flows;
- Whether it is a major transhipment centre;
- Whether the jurisdiction is home to a manufacturing sector that produces goods controlled by international supplier regimes related to WMD and/or their delivery vehicles;
- The geographical proximity to a proliferating country;
- Whether a proliferating state has diplomatic presence in the country
- Whether a proliferating state has significant corporate and trade networks in the country; and
- Whether the country offers shipping flags of convenience or passports of convenience, which proliferators have been known to exploit.

These indicators are covered further in Section 4 below.

A firm's exposure to proliferation financing risks should be assessed by considering the above factors in line with a further analysis of:

- The jurisdictions involved in the provision of services;
- The types of customers and the customer's business;
- The nature of products and services offered; and
- The channels through which those products and services are delivered.

4 Red Flag Indicators

The following red flags and indicators aim to assist in raising awareness of situations commonly encountered where there may be potential proliferation financing. The purpose is also to strengthen a firm's understanding of the proliferation financing risks which may be associated with customers, transactions, methods or jurisdictions. These are not, however, definitive indicators that proliferation or proliferation financing are occurring but serve as a basis for what measures a firm may implement to detect it. It is crucial and good practice that adequate measures are implemented to mitigate the risks of proliferation and proliferation financing, as well as to deter it. This requires the application of standard operating procedures and risk profiles in order to identify suspicious transactions relative to this topic.

The red flag indicators below have been split into a number of sections for ease of reference.

4.1 Customer

Firms should establish controls to determine their client's exposure to the manufacture, trade or provision of services relating to dual use goods or technology. This could be done via due diligence and ongoing monitoring measures. Where doing so through transaction monitoring, firms should pay particular attention to payments or transfers being made to manufacturing companies, importers, exporters, shipping agents, brokers and freight entities, especially where controlled and dual use goods are involved.

Triggers to watch out for relative to the customer may include:

- Parties are, directly or indirectly, involved in the supply, sale, delivery or purchase of dual-use, proliferation-sensitive or military goods, particularly to higher risk jurisdictions;
- Parties are physically located in proliferating countries/diversion concern;
- Parties maintain connections with a country of proliferation concern
- Customers who have previously had dealings with individuals or entities now designated for proliferation by the UNSC;
- Customers who have entered into a joint venture or cooperation agreements with designated entities or individuals;
- Details of the parties involved or linked are similar to those listed under sanctions lists or trade controls, for example, addresses, directors, owners, telephone numbers, email addresses, etc;
- Parties conducting business inconsistent with their risk profile or expected activities;
- The customer is a military or research body connected with a high risk jurisdiction;
- Customer provides incomplete information or is resistant to providing additional information when this is sought;
- Customer provides the total required funds in advance of a transaction in one large sum (if this is not typically characteristic of the industry in question; and
- Customer purchases or sells goods with a disproportionately expensive delivery cost without a justified reason.

4.2 Product

Potential indicators of proliferation or proliferation financing with regards to the products or methods used to do so may comprise:

- Transaction concerning dual-use goods or military goods;
- An opaque or complex structure where the end-user or end use are not identified, promoting a lack of transparency;
- The use of cash or personal accounts are used in transactions for industrial items which is unusual and making it much more difficult to trace the source of funds or maintain an appropriate audit trail;
- Highly technical goods shipped to countries with low levels of technology;
- Complicated structures to conceal a party's involvement, for example, the use of layered letters of credit, intermediaries and brokers;
- Transactions which involve shell or front companies;
- Wire transfers or payments with parties not originally identified or payment to be made to a beneficiary in a country other than the beneficiary's stated location;
- Pattern of wire transfers or payment activity which are unusual, illogical or have no apparent purpose;
- The transaction structure (whether shipping route, financing arrangement or documentation) appears unnecessarily complex or irrational;
- Switching off the vessel's signal entirely or changing the physical appearance of the ship;
- The description of the goods on the trade/financial documentation that is non-specific or misleading;
- Based on the documentation obtained in the transaction, the declared value of the shipment was obviously under-valued in line with the shipping cost;
- Evidence that documentation or other representation are fraudulent/fake
- Transactions linked to institutions with known AML/CFT deficiencies; and
- Where a new customer requests a letter of credit from a bank, whilst still awaiting approval of its account.
- Transactions involving correspondent banks who have a documented history for facilitating payments for proliferating regimes or within high risk jurisdictions.

4.3 Geographical Location

Although an immediate indicator may be links to a country that is subject to sanctions imposing restrictions on the movement of military goods, firms should determine its exposure to business (including customers and beneficial owners) with countries that are known to have ties with sanctioned countries (e.g. China, Hong Kong, Singapore and Malaysia) and which may pose a higher risk of proliferation financing. For example, shipments and freight forwarding destined to Iran could be labelled as being shipped to bordering countries such as Turkey, Afghanistan, Pakistan, United Arab Emirates, Oman, Qatar, Bahrain, Saudi Arabia, Kuwait, Iraq and Syria.

It is, therefore, imperative that firms assess and understand their customers and the nature of the business relationship. This would aim to ensure that any transactions to these countries are put into context and the potential risks of proliferation financing can be appropriately identified and managed.

Potential indicators of proliferation or proliferation financing within a country or jurisdiction may be:

- The use of jurisdictions where its laws make it difficult to determine the beneficial ownership behind a corporate structure;
- A route of shipment of goods or transactions inconsistent with normal geographical patterns or the customer's expected business activity;
- The use of jurisdictions where there is no public register for company's details, such as the company name, directors, secretaries, etc, promoting a lack of transparency;
- The use of diplomats in countries of proliferation concern to access banking systems;
- The use of nationals who are not linked to a sanctioned country as directors, nominee shareholders or signatories as a front for a designated individual or entity;
- The use of correspondent banking relationships with partners or providers located in high risk jurisdictions for proliferation purposes;
- Transactions which involve individuals, companies or a shipment route located in a country with weak export control laws or weak enforcement of these laws;
- Jurisdictions which may present ongoing and/or substantial money laundering, terrorist financing or proliferation financing risks or have strategic deficiencies in the fight against these, for example those identified by the FATF as Non-Cooperative Countries or Territories;
- Countries which have strong links (such as funding or other support) with terrorist activities or organised crime; and
  Payments or transfers made to importers, exporters, agents or brokers that export to countries and ports near the border of sanctioned countries. For example, shipments of prohibited goods to the DPRK are often marked as destined to Dangdong, China and other nearby ports.

5 Sectoral Guidance

Reporting entities often play a front line role in detecting and managing proliferation financing and their ability to disrupt it, has received greater attention in recent years. It is, therefore, vital that firms understand the threats related to proliferation financing and implement adequate internal processes to counter it. In devising their response to proliferation financing risks, firms should take into account the red flags and indicators provided above, as well as, any emerging practices or modus operandi which may be exploited for proliferation financing purposes. Practices related to the identification of red flags should extend to accountants and auditors.

The UN Panel of Experts Report published in 2019, confirmed that DPRK continues to evade UN sanctions. The report highlights that the implementation and enforcement of financial sanctions remains a major challenge for jurisdictions and firms around the world. It provides valuable data on different methods and tactics that have been identified and which may help firms adjust their preventive measures programs.

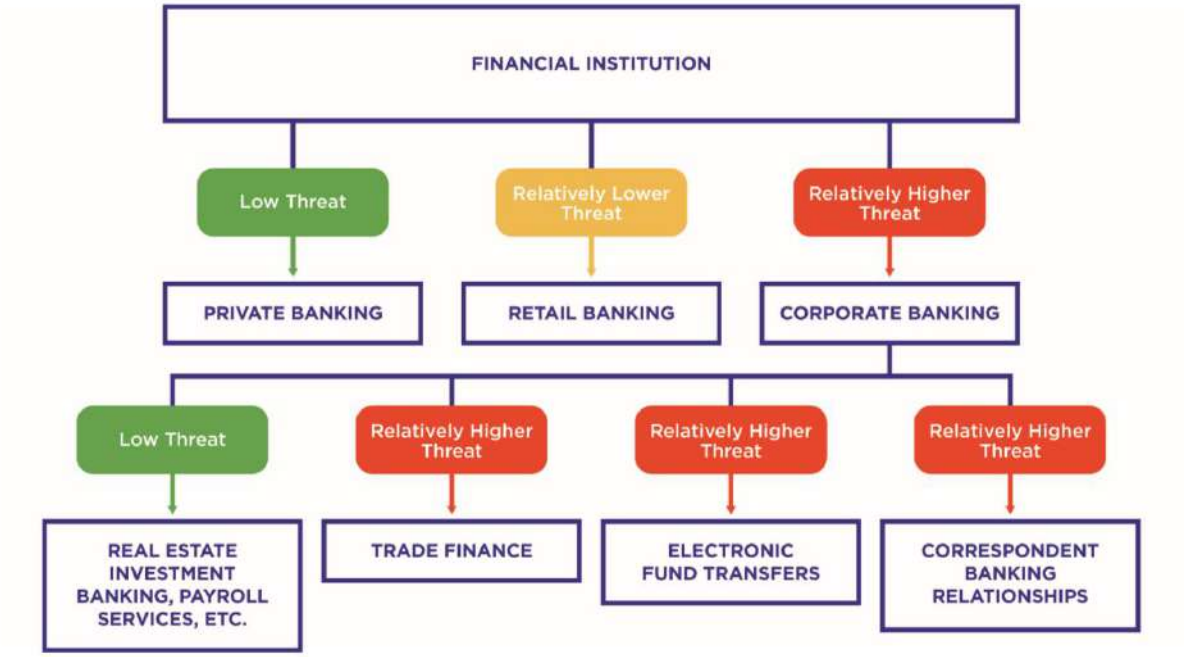
In recent years, there has been a high use of sanctions evasions techniques, therefore, list-based screening is no longer sufficient as a standalone tool. It is important to remember that proliferators and its financers are as aware of the sanctions lists as we all are and can use them to avoid being detected. This is highlighted by the case study under Appendix 1 of this document.

The sectors considered higher risk for proliferation financing purposes are Banking, Insurance, DLT providers and TCSPs. These have been covered in further detail below.

5.1 Banking

The banking sector plays a significant role in mitigating proliferation financing risks as it is at the forefront of the movement of funds and the majority of transactions carried out for companies and/or individuals. Due to this, a bank's risk mitigation programmes and controls are instrumental in effectively managing any potential risks.

The diagram below illustrates the threat profile posed by different types of banks for proliferation financing purposes according to a report published by the Center for a New American Security:



Schematic representation of relative levels of financing-of-proliferation threats to different areas of banking activity, products, and services. The banking categories are indicative and not exhaustive.

This diagram was published by Dr Jonathan Brewer in his report for the Center for a New American Security, on Conducting Risk Assessments dated November 2018.

The UN Panel of Experts Report found that firms often fall prey to DPRK diplomats. A typical scenario would include a DPRK diplomat accredited in a European country, who opens a number of accounts in European banks, both in the country they are accredited and in countries where there is no DPRK diplomatic mission, using either their own information for account opening or employing evasion techniques. This includes accounts in the names of family members and front companies and using different registered or business addresses. They would then use those accounts to engage in the illicit procurement of goods on behalf of DPRK. The UN Panel of Experts has issued a report stating that Member States are required to limit the number of bank accounts in their jurisdiction to one per DPRK diplomatic mission/consular post, and one per accredited DPRK diplomat/consular officer.

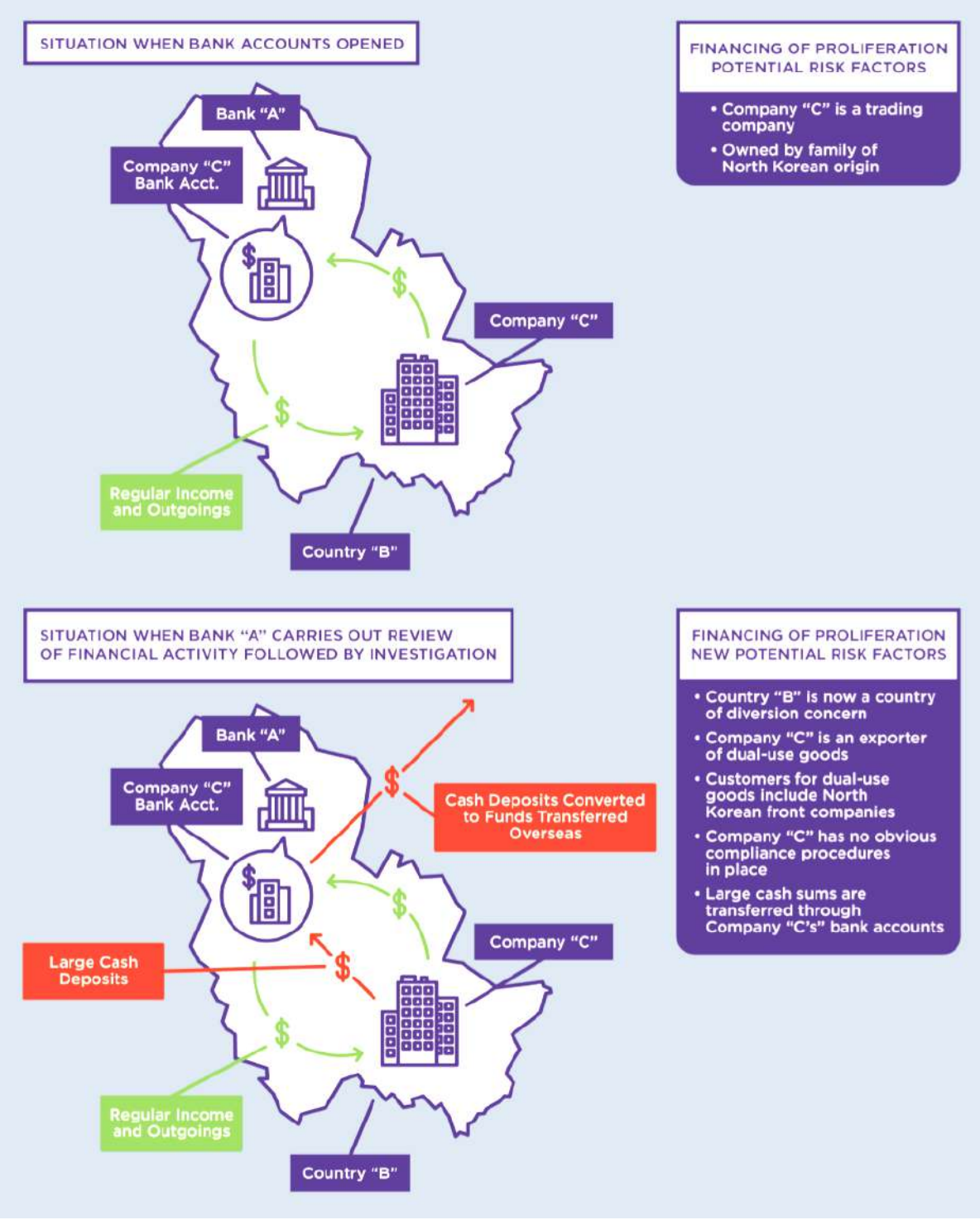
It was also found that correspondent banks carry out financial transactions on behalf of their North Korean counterpart and therefore, give DPRK an access point to the wider global financial system. DPRK financial institutions are not allowed to maintain correspondent banks or any other financial relationships with foreign financial institutions. According to the report it is, however, believed that DPRK has particularly used correspondent accounts held with banks established in China to facilitate its international financial transfers and in this way, infiltrate the international financial system.

The image below provides a simplified illustration of the factors which may contribute to a bank's assessment of the proliferation financing risk posed by a client:

Bank A, an international bank, is headquartered in a Western country. Bank A has a local branch in an Asian country, Country B.

Country B is a regional trade centre with commercial and financial links to North Korea and a substantial North Korean diaspora.

Company C, is a small local trading company, which recently established itself in Country B. It then opened several bank accounts at Bank A's branch in Country B.



This diagram was published by Dr Jonathan Brewer in his report for the Center for a New American Security, on Conducting Risk Assessments dated November 2018.

5.2 Trust and Corporate Service Providers

Gibraltar has a long standing TCSP industry which has been regulated for many years. Nonetheless, it is evident that in carrying out proliferation financing, perpetrators often use this sector to set up front companies and for nominee shareholding services to increase the lack of transparency within a complex, corporate structure. Additionally, there are various local TCSPs which provide its services to shipping companies escalating the proliferation financing risk further and emphasising the need for adequate systems and controls including ongoing transaction monitoring.

According to the UN Panel of Experts Report, one of the most efficient ways DPRK circumvents sanctions is by engaging in illegal shipping transfers of petroleum, coal and other goods. The vessels operating on DPRK's behalf effectively steal another vessel's identity to remain undetected. This highlights the importance of ensuring firms are aware of a vessel's movement and of the individuals behind these vessels. Consequently, firms may end up unwittingly facilitating financial transactions associated with these illegal inter-shipping transfers, as well as, indirectly being associated with the financing of proliferation activities. A relative case study can be found under Appendix 2 of this document.

5.3 Distributed Ledger Technology Providers

Recent evidence has shown an increased risk in the use of cryptocurrencies and cybercrime to evade sanctions and subsequent funding of WMD programs. Perpetrators could seek to use cryptocurrencies as to facilitate proliferation financing efforts through:

- **Fundraising**: To sustain ongoing needs for financial resources by through the acquisition and conversion of cryptocurrencies to fiat currencies in the short term.
- **Stockpiling**: To accumulate reserves of cryptocurrencies with the objective of conversion into fiat currency at one point in the future.
- **Circumvention**: To pay directly for goods and resources that are explicitly prohibited by international sanctions using cryptocurrencies.

In order to convert cryptocurrency funds to fiat currency, or other more favourable forms of cryptocurrency, perpetrators would seek to exploit cryptocurrency exchanges and other related platforms. The Distributed Ledger Technology Regulatory Framework established in Gibraltar includes such platforms under the licensing and supervisory remit of the GFSC. DLT providers are caught within the scope of the Proceeds of Crime Act 2015 and are, therefore, required to comply with all relevant legislative requirements.

Key to the avoidance of exploitation for proliferation financing purposes are the customer due diligence and ongoing monitoring requirements that providers are required to uphold. All clients must be appropriately screened in order to verify their identity, as well as for confirmation that they do not appear on any of the relevant sanctions lists. When scrutinising transactions, DLT providers must ensure that they are made aware of any interaction with known actors linked to WMD programs or dark-web marketplaces; which are known to be used by such perpetrators for the exchange of goods and services in return for financial resources.

The use of cybercrime attacks on cryptocurrency exchanges has also been linked to proliferation financing regimes. It is, therefore, a responsibility of the DLT provider to ensure that all systems and security access protocols are maintained to appropriately high standards to limit the risk of such occurrences.

5.4 Insurance

The Insurance sector in Gibraltar is one of the largest contributors to economic activity. Despite being considered relatively inherently low risk for the facilitation of other forms of financial crime (such as money laundering and terrorist financing), experts globally have identified potential exposure to the exploitation for the proliferation of WMD. The primary risk lies within the shipping insurance industry. Note that while the majority of locally-based insurers underwrite against general classes of risk, there are currently no firms that offer or distribute shipping insurance; reducing the proliferation financing risk posed in Gibraltar.

UNSCR 2397 states the requirement for jurisdictions to prohibit the "provision of insurance or re-insurance services" to any vessels involved in North Korea's proliferation programs. Perpetrators have been found to exploit the provision of insurance in order to facilitate the transfer of dual-use goods. This plays a key role in the acquisition and transfer of sanctioned goods and materials used in the development of WMD, as vessels are typically denied the ability to leave and enter ports without showing evidence of valid insurance.

Where increased proliferation risk is identified, as mentioned above, relevant insurers should not rely solely on list-based screening of targeted financial sanctions. In such cases, due diligence measures should be incorporated into the firm's underwriting processes prior to proceeding with providing insurance coverage to the vessel or transport company in question.

6 Reporting Process

All reporting entities should check whether they maintain any account, or otherwise hold or control funds or economic resources, for individuals or entities included in the relevant sanctions lists. If you know or have 'reasonable cause to suspect' that you are in possession or control of, or are otherwise dealing with, the funds or economic resources of a designated person, the process is as follows:

- freeze them;
- not deal with them or make them available to, or for the benefit of, the designated person, unless there is an exemption in the legislation that you can rely on; and
- immediately report them to the GFIU.

Any information provided will only be used for the purposes for which it was provided or received.

Proliferation financing reports are made using the online reporting system Themis. Please select the Proliferation Financing drop down option when submitting your report.

If you do not yet have access to Themis, you can either register via https://www.gfiu.gov.gi/reporting or by submitting a form as detailed on the GFIU website.

If you are unsure of your reporting obligations, it is strongly recommended that you seek independent legal advice.

7 Guidance & Further Reading

7.1 Sources

The following table provides a list of relevant sources for proliferation financing that may be useful.

Publication	Description
FATF 2008 Typologies Report	Describes PF case studies and indicators
FATF Guidance on Counter Proliferation Financing (2018)	Provides non-binding guidance to facilitate public/private sector stakeholders in understating and implementing FATF Recommendations and IOs.
FATF Guidance on the Risk-Based Approach to Combating ML & TF	Guidance that outlines the risk-based approach and good practice
Jersey Financial Services Commission Guidance on PF (2011)	Describes PF indicators
Royal United Services Institute (RUSI) Reports	Offer guidance for governments and FIs on combating PF
King's College London Project Alpha Typologies Report (2017)	Describes PF case studies and indicators
UN Panel of Experts Reports	Provide valuable data on DPRK's methods and tactics that can help financial institutions adjust their preventive measures programs.
2019 UN North Korea Panel of Experts Report Takeaways for FIs	Article published by the Carnegie Endowment for International Peace summarising the UN Panel of Experts Report for Financial Institutions, dated 27 March 2019.
CNAS Report on The Financing of WMD Proliferation	Report published by the Center for a New American Security offering guidance for financial institutions on the proliferation-related factors that should be considered within risk assessments.
MAS Guidance on Proliferation Financing	PF Guidance issued by the Monetary Authority of Singapore
Sanctions List Materials UNSCR 1718	Lists under Resolution 1718 on Democratic People's Republic of Korea
Sanctions List Materials UNSCR 2231	Lists under Resolution 2231 on Iran nuclear issue
List of designated vessels	UNSCR 1718 list of designated vessels provides information on vessels subject to measures obligated under the relevant resolutions

Glossary

Disclaimer – The following is a general description of terms used throughout this guide or which are relevant to proliferation financing. For exact terms used in context, please see the up-to-date version of the relevant legislation. If you are in doubt about any of the below, please seek independent legal advice.

Biological Agent

Biological weapons are any weapon, equipment or means of delivery designed to use biological agents or toxins for hostile purposes or in armed conflict. Biological agent means any microbial or other biological agent.

Chemical Weapons

Chemical weapons are toxic chemicals and their precursors; munitions and other devices designed to cause death or harm through the toxic properties of toxic chemicals released by them; equipment designed for use in connection with munitions and devices falling within paragraph (b) of the WMD Act 2004.

Competent authority

The GFIU is the designated central authority for the receipt of suspicious activity reports or other reports related to proliferation financing. For most purposes, the Chief Minister is Gibraltar's competent authority for financial sanctions.

Cryptocurrency

A digital currency in which cryptography encryption techniques are used to regulate the generation of units of currency and verify the transfer of funds, operating on a decentralised network. Also commonly referred to as Virtual Assets (VAs).

Counter proliferation

A type of financial sanction. Under an asset freeze it is generally prohibited to:

- deal with the frozen funds or economic resources, belonging to or owned, held or controlled by a designated person
- make funds or economic resources available, directly or indirectly, to, or for the benefit of, a designated person
- engage in actions that, directly or indirectly, circumvent the financial sanctions prohibitions

Distributed Ledger Technology (DLT)

A database system in which information is recorded and consensually shared and synchronised across a network of multiple nodes, where all copies of the database are regarded as equally authentic.

Distributed Ledger Technology (DLT) Provider

Any firm carrying out by way of business, in or from Gibraltar, the use of DLT for storing or transmitting value belonging to others.

Dual-Use Goods

Goods, software and technology intended for civilian uses that can also serve in a military application. The Wassenaar Arrangement on export controls for conventional arms and dual-use goods and technologies lists and provides guidelines for which items may fall under the term.

End user certificate

A certificate with which importing/buying states declare themselves to be the ultimate user of the consignment of arms. No globally binding standards regulate format, content or nomenclature for the transferred arms. Indirect provisions that are part of the UN Arms Trade Treaty may engender globally binding norms.

Designated person (DP)

A person subject to financial sanctions.

Economic resources

Generally means assets of every kind – tangible or intangible, movable or immovable – which are not funds but may be used to obtain funds, goods or services.

Exemption

Generally found in financial sanctions legislation. An exemption to a prohibition applies automatically in certain defined circumstances and does not require you to obtain a licence.

Funds

Generally means financial assets and benefits of every kind, including but not limited to:

- cash, cheques, claims on money, drafts, money orders and other payment instruments
- deposits with financial institutions or other entities, balances on accounts, debts and debt obligations
- publicly- and privately-traded securities and debt instruments, including stocks and shares, certificates representing securities, bonds, notes, warrants, debentures and derivatives contracts
- interest, dividends or other income on or value accruing from or generated by assets
- credit, right of set-off, guarantees, performance bonds or other financial commitments;
- letters of credit, bills of lading, bills of sale and
- documents showing evidence of an interest in funds or financial resources

GFIU

Gibraltar Financial Intelligence Unit.

Gibraltar competent authority

The Chief Minister (or depending on the legislation, this could also be the Minister responsible for financial services). The point of contact in the first instance, however, is the GFIU.

Goods

Generally means items, materials and equipment.

Licence

A written authorisation from the Gibraltar competent authority permitting an otherwise prohibited act.

Name match

The situation where a person you are dealing with partially matches the details of a designated person on the consolidated list. Unlikely to be a target match.

Nuclear Weapons

An explosive device that derives its mass destructive force from atomic fission or fusion reactions.

Office of Financial Sanctions Implementation

Part of HM Treasury and the UK's competent authority for implementing financial sanctions.

Ownership

The possession of more than 50% of the proprietary rights of an entity or having a majority interest in it. Includes both direct and indirect ownership.

Person

Can be a natural person (an individual), or a legal person, body or entity.

Proscription

The power to proscribe (ban) an organisation under the Terrorism Act 2018.

Radiological Weapons

Weapons that disperse radioactive agents to inflict injury or cause contamination or damage.

Reporting Entities

These are also referred to as firms within the guidance document. It includes any entities caught within the scope and definition of a "relevant financial business" under Section 9 of the Proceeds of Crime Act 2015 and Schedule 4 of the Sanctions Act 2019.

Reasonable cause to suspect

Refers to an objective test that asks whether there were factual circumstances from which an honest and reasonable person should have inferred knowledge or formed the suspicion.

Sensitive Defence Technology

Items with significant potential military applications that are not presently subject to controls and could give rise to national security concerns. These encompass both items specially designed for military use that are not subject to current controls, as well as a sub-set of the dual-use items of proliferation concern, for example, high-quality, high-tech components that may be useful for the development of advanced weapons systems.

Space-related Items

Items that are a subset of both dual-use items of proliferation concern and sensitive defence items given their economic and military potential. For example, the items required to build civilian or military communications or imaging satellites are virtually identical, and would be included in this category.

Target Match

The situation where the person you are dealing with matches the details of a designated person on the consolidated list. Likely to be a confirmed match for that person.

Trust and Corporate Service Provider (TCSP)

Any firm carrying out by way of business, in or from within Gibraltar, the creation, operation or management of trusts, companies, foundations or other similar structures.

Weapons of Mass Destruction (WMD)

Weapons of mass destruction are atomic explosive weapons, radioactive material weapons, lethal chemical and biological weapons, and any weapons developed in the future which have characteristics comparable in destructive effect to those of the atomic bomb or other weapons mentioned above.

Appendix 1

Case Study – Proliferation Financing Network

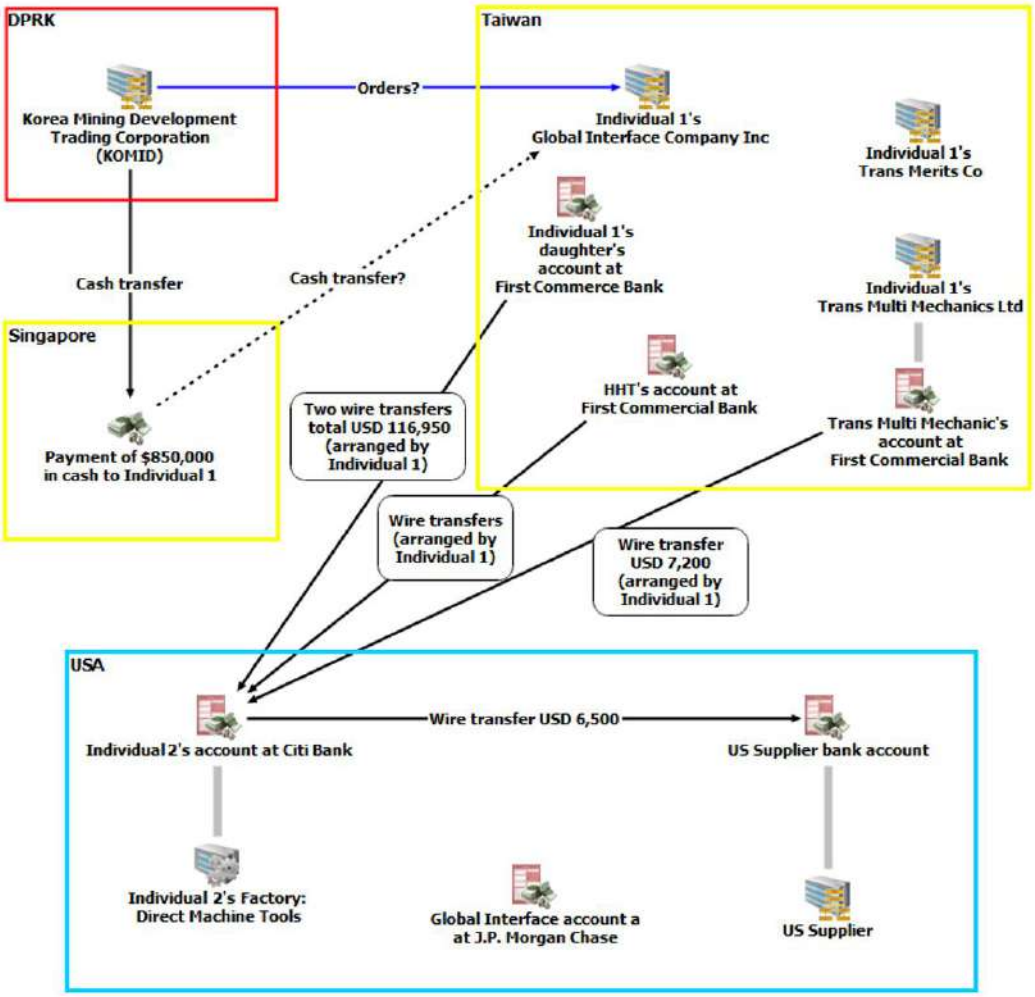
This case study highlights how a procurement network was successfully established adapting to designated entities and individuals.

A network of individuals including a father, based in Taiwan and his son, based in the US, were under investigation from 2009 for the export of US origin goods and machinery that could be used to produce WMD. The father and one of the companies were convicted by Taiwanese authorities in 2008 in connection with shipping restricted materials to DPRK. The network consisted of at least three Taiwan-based companies set up and managed by the father. His wife was also an officer in two of these companies.

In January 2009, the US Treasury Department designated the father, his wife and two of the companies involved, for supporting the Korea Mining Development Trading Corporation (KOMID). The KOMID is an entity closely linked with DPRK's WMD programs. As a result, US persons could only do business with the father and his designated companies with a license from the US Treasury Office of Foreign Assets Control (OFAC). Despite his designation, the father imported a precision machine tool from the US through his third, non-designated, Taiwanese company, with the assistance of his son.

In mid-2009, the US authorities learned that the father was due meet a KOMID representative in Singapore to receive a payment, probably for the shipment of equipment worth over USD 850,000, and possibly in cash. The involvement of a designated entity in the transaction and payment for the machinery was hidden because the wire transfer was to his son's US bank account, from a corporate bank account in Taiwan. Similarly, subsequent financial transfers from father to son took the form of two further wire transfers from a bank account in Taiwan controlled by his daughter, in effect hiding the involvement of a designated individual from the US banking system. To do so, the daughter also managed to set up a US-based company, relating to Factory Machine Tools, to help develop business with her father's companies.

The diagram below illustrates the case study further:



This diagram was issued by Dr Jonathan Brewer in his final report on Project Alpha dated 13 October 2017.

It is key to note that the network was resilient. Despite the designation of the main person involved and two of his companies, the network was adapted by creating additional companies, and expanding its proliferation and non-proliferation trading activities, hence, increasing the lack of transparency. In silo, each wire transfer or company does not appear problematic. However, when looking at the big picture there was a complex network set up to carry out proliferation financing and proliferation programmes.

Appendix 2

Case Study – Chinpo Shipping

This case study highlights how proliferation financing may be carried out through shipping companies and where illicit activities are concealed through a legitimate business.

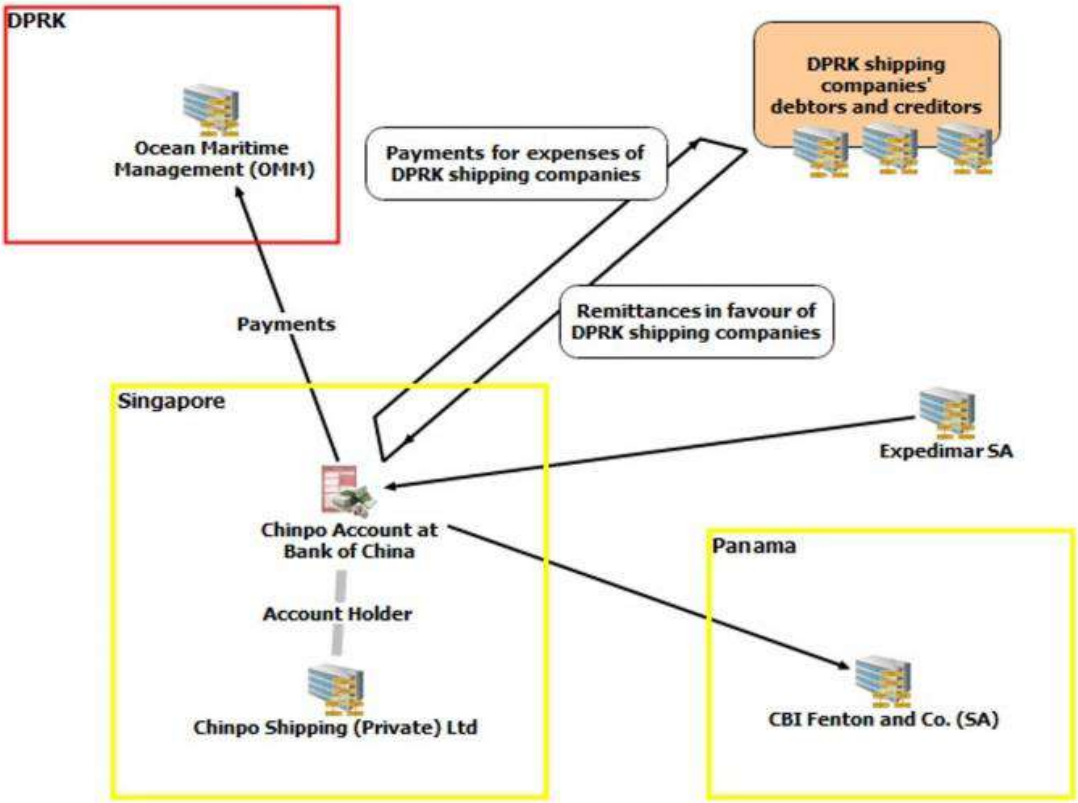
In July 2013, Panama Canal authorities detained a North Korean vessel, the Chong Chon Gang (CCG), while it was transiting the Panama Canal from Cuba to DPRK. Canal authorities found a shipment of arms and related materials concealed under other cargo. Costs in connection with the voyage of the CCG were paid by Chinpo Shipping (Private) Ltd (Chinpo), which was based in Singapore. Chinpo had business relationships with North Korean shipping companies since the 1980s as it was an existing shipping company.

According to court documents, Chinpo was a shipping agent and general wholesale importer/exporter. It was one of three companies run by a family that shared the same business address, employees and an email account for communications with North Korean entities. The three companies also shared an account at the Bank of China, in Chinpo's name. The North Korean Embassy in Singapore used the business as a postal address.

Over three years, approximately 605 remittances took place totaling more than USD 40 million, all related to North Korean vessels. Chinpo was also found to be effectively operating a remittance business although the company had no licence to do so from the Singapore authorities. Chinpo tried to hide its involvement with North Korean companies by removing the names of its vessels and other identifying details from remittance forms and email correspondence. Payments from Chinpo's account took place in the absence of invoices or other details.

Following subsequent investigations, Singaporean authorities filed criminal charges. Chinpo was convicted of proliferation financing in connection with a sum of USD 72,016.76 that Chinpo had remitted by wire transfer from a Bank of China account to a Panama Canal shipping agent, CBI Fenton & Co. (SA). However, Chinpo's conviction on charges of proliferation financing were subsequently overturned on appeal.

The diagram below illustrates the case study further:



This diagram was published by Dr Jonathan Brewer in his final report on Project Alpha dated 13 October 2017.