# GUYANA'S COUNTER PROLIFERATION FINANCING GUIDANCE

**August 2023**

# Table of Contents

# EXECUTIVE SUMMARY

This Guidance and Strategy provides updated information to competent authorities and reporting entities with regard to, specifically, the countering of the financing of proliferation of weapons of mass destruction.

Supported by the 2021 National Risk Assessment (NRA) and the Updated Terrorist Financing and Proliferation Financing Risk Assessment 2023, this document has the following objectives-

(1) provide updated guidance for authorities and reporting entities on international best practices related to countering proliferation financing;

(2) provide a synopsis of Guyana's improved legislative and policy framework in relation to combatting proliferation financing; and

(3) provide a strategic framework with targeted actions for competent authorities and reporting entities to implement based on the recommendations of the NRA, the draft counter terrorism strategy and the updated risk assessments.

This therefore enables strategic cooperation, whilst ensuring that it follows best practices and the legislation as updated in Guyana, towards keeping Guyana safe from proliferation financing.

The Guidance and Strategy may be read together, or separately, depending on the audience using this document; however, the Guidance provides the necessary considerations to take into account when reading the Strategy, in consideration of the 2023 Updated TF/PF Risk Assessment.

**AML/CFT/PF National Coordination Committee**

# INTRODUCTION

Although Guyana is not an international financial centre but a small emerging economy, the country, in keeping with international best practices and standards, has provided updated guidance on proliferation financing, and a strategy on dealing with related issues.

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 distributed ledger technology (DLT) and the abuse of the financial system by threat actors.

Proliferation of weapons of mass destruction (WMDs), nuclear, biological, and chemical weapons, represents the most serious threat to global security and challenges the entire international community. To circumvent international restrictions and sanctions, states and non-state actors are able to procure components and technology through proliferators, that can then be used to build a weapon. Proliferators use a number of evasive techniques and tactics to circumvent the financial sanctions restrictions applied against them, providing them access to the financial system. Proliferation risks expand further than just those emanating from specific countries, such as North Korea (DPRK) or Iran. There are also non-state actors that can attempt to obtain proliferation-sensitive goods.

There is currently no evidence to suggest that reporting entities in Guyana facilitate proliferation financing (PF) activities. However, whilst there may be no direct PF links, the exposure of financial system when conducting business in the international market can possibly pose PF risks.

As a result, this document provides indicators of possible proliferation financing risks and suggests tools that relevant institutions and businesses or professions should implement and incorporate to counter proliferation financing.

This is in keeping with the recommendations of the 2021 NRA and the 2023 updated TF/PF risk Assessments.

Further, Guyana has revamped its legislative framework to ensure that proliferation financing is adequately criminalized, and listed as a predicate offence for money laundering in its anti-money laundering/countering terrorism financing/countering proliferation financing (AML/CFT/CPF) legislative framework.

This document will also be shared with reporting entities and the private sector so that this guidance and the implementation of the strategic recommendations can be taken on board in a cooperative and collaborative manner; only with synergized efforts, would we as Guyanese be able to prevent detect and mitigate against such a crime occurring in our country.

# WHAT IS PROLIFERATION OF WEAPONS OF MASS DESTRUCTION?

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.

## What is Proliferation Financing?

There is no international definition of proliferation financing. However, the Financial Action Task Force (FATF) produced a working definition of proliferation financing based on United Nations Security Council Resolution (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."

As the FATF definition suggests, proliferation financing is very broad and refers to more than simply the payment for goods and includes any financial service provided in support of any part of the procurement process (even if it is not directly connected to the physical flow of goods). Financing can include financial transfers, mortgages, credit lines, insurance services, middlemen services, trust and corporate services and company formation. Proliferation financing can therefore be described as both a financial crime risk and a sanctions risk.[1]

A report by the Center for a New American Security (CNAS) divided the financial elements of a Weapons of Mass Destruction (WMD) into three stages:

1) Stage 1 – Fund Raising – during this stage, the proliferator raises funds for the program through its domestic budget, perhaps supplemented with funds raised by networks overseas or by criminal activity (conducted by or on behalf of state actors

2) Stage 2 - Disguising the funds – in this phase, the proliferator transfers these funds into the international financial system. If the country is not sanctioned, this is straightforward. For states subject to comprehensive sanctions like North Korea and Iran (prior to implementation of the Joint Comprehensive Plan of Action (JCPOA), it is a major challenge. In addition, in this stage,

[1] Joshi, Dall, Dolzikova, Guide to Conducting a National Proliferation Financing Risk Assessment, RUSI Occasional Papers, May 2019

proliferators rely on extensive networks of businesses (including front companies) and middlemen to obscure any connection on paper to sanctioned countries.

Countries use opaque ownership structures for evading sanctions lists. Often proliferation financing involves companies in or near a sanctioned country and accounts under the control of a foreign national with sympathies to the sanctioned country. This, combined with the use of false documentation, allows proliferators to avoid detection.

3) Stage 3 - Procurement of materials and technology – at this stage, the proliferator uses these funds in the international financial system to pay for goods, materials, technology, and logistics needed for its WMD program. Throughout this third stage, international financial institutions (FIs) will be involved in processing the related transactions. It is important to note that proliferation involves not only the purchase of weapons but also of individual goods and component parts that can be used to develop weapons or missiles. This makes proliferation activities more difficult to detect.

In complex structures PF may not necessarily be directly connected to the physical flow of goods. For example, PF can include, although not be limited to, the following:

› Financial transfers

› Provision of loans

› Ship mortgages and registration fees

› Insurance and re-insurance services

› Credit lines for shipment of illicit sensitive goods

› Trust and corporate services

› Acting as an agent for, to, or on behalf of someone else

› Facilitation of any of the above.

In many cases PF activity has the sole aim of generating access to foreign currency and the international financial system. It may look like a legitimate trading transaction. For this reason, it is important to understand the full payment chain and consider how any trade may be used to enable illicit activity.

**TABLE – DIFFERENCE BETWEEN PF, ML AND TF**

| | **Money Laundering (ML)** | **Terrorism Financing (TF)** | **Proliferation Financing (PF)** |
|---|---|---|---|
| *Purpose* | Use of illicit funds in the regulated system | Supports terrorist activities | Acquisition of WMD |

| | | | |
|---|---|---|---|
| *Source of funds* | Internally from within criminal organisations | Internally from self-funding cells (centred on criminal activity) and externally from benefactors and fundraisers | State-sponsored programs |
| *Conduits* | Favours formal financial systems | Favours cash couriers or informal financial systems such as hawala and currency exchange firms | Favours formal financial system |
| *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 threshold | Moderate amounts |
| *Financial Activity* | Complex web of transactions often involving shell or front companies, bearer shares, and 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 origin of funding |
| 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 |

While some risk indicators may overlap for ML and PF, for example PF transactions may trigger ML risk indicators; sometimes the amounts are small and not all dual-use goods cost large sums of money and fall below ML triggers. In addition, proliferation finance networks are aware of ML triggers and sometimes deliberately structure payments, transactions and corporate architecture to avoid ML triggers.

## Dual Use Goods and Export Controls

Dual-use goods are items or technology that can have civilian and military or proliferation applications. For example, hydrogen peroxide can be used for paper bleach and missile

propellant, while nickel aluminides can be used to manufacture household glass containers and aircraft engine blade coating. Even if some goods do not appear on export control lists, they are still subject to restrictions if their end use is for illicit proliferation purposes.

Dual-use goods can be identified from lists produced by the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies. Other export control regimes include the Nuclear Suppliers Group (nuclear technology), Missile Technology Control Regime (category 1 - missile systems and production capabilities and category 2 include dual-use items), and the Australia Group (chemical and biological agents).

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.

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.

## 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.

*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 transshipment of items that would contribute to weapons of mass destruction proliferation.

*DPRK and Iran*

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(2016);

- 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.

Targeted financial sanctions (TFS) are one component of a range of UNSCR measures to counter the flow of funds to proliferation actors. The full range of UN sanctions measures go

beyond TFS to also include activity-based financial prohibitions, economic or sectoral sanctions and related financial prohibitions, and vigilance measures.

## Domestic Obligations

In addition to the international obligations, there are offences in Guyana's law relevant to the development, production, acquisition, retention and transfer of nuclear, biological and chemical weapons, pursuant **sections 25 and 29** of the Anti-Terrorism and Terrorist Activities Act 2015.

**Section 58 (2)** of this Act also gives Article 11 of the International Convention for the Suppression of the Financing of Terrorism the force of law in Guyana.

The AML/CFT Act (as amended) provides for the criminalization of proliferation financing and inchoate offences by **sections 75A and 75B**, whilst **section 75C** provides procedures for targeted financial sanctions and designations involving any person involved in proliferation financing or any State actor.

According to **section 75B (2)** of the AML/CFT Act, a person who commits proliferation financing is liable to a fine of no less than one hundred million dollars or no more than five hundred million dollars or to imprisonment for life or to both.

*UNSCRs on DPRK and Iran – Example of restrictive measures*

For examples of information concerning restrictive measures against DPRK, please see Annex VIII of Council Regulation EU 2017/150911, on luxury goods referred to in Article 10:

1. It shall be prohibited:

(a) to sell, supply, transfer or export, directly or indirectly, luxury goods as listed in Annex VIII, to the DPRK;

(b) to import, purchase or transfer from the DPRK, directly or indirectly, luxury goods, as listed in Annex VIII, whether or not originating in the DPRK.

2. The prohibition referred to in point (b) of paragraph 1 shall not apply to travellers' personal effects or to goods of a non-commercial nature for travellers' personal use contained in their luggage.

# WHY SHOULD YOU BE CONCERNED WITH THE PREVENTION AND DETECTION OF PROLIFERATION FINANCING?

1) Proliferation financing facilitates the movement and development of proliferation-sensitive goods. The movement and development of such items pose serious threats to human life, the environment, infrastructure and, more broadly, to international peace and security. Thus, countering the flow of funds to proliferation actors (both state and non-state actors, such as terrorists groups) play a vital role in combating the proliferation of WMDs.

2) A sample of publicised cases gives an indication of reputational damage which may cause investors to shy away from a jurisdiction perceived as accessible to proliferators. Caribbean case studies of proximate risk include: Actual and attempted violations of the UN arms embargo on DPRK which involved entities registered in Caribbean jurisdictions.

*Lessons learned*

- Jurisdiction-hopping is an observable trend within DPRK proliferation finance networks
- Commonalities provide for a number of typologies and risk reduction strategies

## DIFFICULTIES FACED IN IDENTIFYING PROLIFERATION FINANCING

- A growing trend in the purchase and sale of elementary components, as opposed to whole manufactured systems. The individual elementary components may also have legitimate uses (dual-use goods), making their identification for illegitimate purposes even more problematic.

- Dual-use goods are difficult to identify, requiring specialist knowledge and can be described in common terms with many uses such as ‘pumps’.

- Networks through which proliferation-sensitive goods may be obtained tend to be complex. This, combined with the use of false documentation, allows for the proliferation of sensitive goods, the entities involved, the associated financial transactions and the ultimate end-user to avoid detection. Front companies, agents and other false end-users are often used to cover up the ultimate end-user.

- Risk of proliferation financing is more likely to be present in cases where the source of funds is legal and the end-user of a type of goods involved is obscured, making identification of such activities difficult.

In addition, identifying PF is not limited to individuals and entities designated on sanctions lists and may involve other actors with no immediately obvious connection to designated entities and individuals, and can be disconnected from the physical flow of proliferation-sensitive goods. Also, detection is difficult because most transactions occur within normal business transaction pathways, and can be masked with all legitimate transactions.

## RED FLAGS

*PROLIFERATION FINANCING INDICATORS*

- When customer is involved in the supply, sale, delivery or purchase of dual-use, proliferation sensitive or military goods, particularly to higher risk jurisdictions.
- When customer or counter-party, or its address, is the same or similar to that of an individual or entity found on publicly available sanctions lists.
- The customer is a research body connected with a higher risk jurisdiction of proliferation concern.
- When customer's activities do not match with the business profile provided to the reporting entity.
- When customer is vague about the ultimate beneficiaries and provides incomplete information or is resistant when requested to provide additional information.
- When customer uses complicated structures to conceal connection of goods imported / exported, for example, uses layered letters of credit, front companies, intermediaries and brokers.
- When a freight forwarding / customs clearing firm being listed as the product's final destination in the trade documents.
- When final destination of goods to be imported/exported is unclear from the trade related documents provided to the reporting entity.
- Project financing and complex loans, where there is a presence of other objective factors such as an unidentified end-user.
- The transaction(s) involve an individual or entity in any country of proliferation concern.
- The transaction(s) related to dual-use, proliferation-sensitive or military goods, whether licensed or not.
- The transaction(s) involve the shipment of goods inconsistent with normal geographical trade patterns i.e. where the country involved does not normally export or import or usually consumed the types of goods concerned.
- Over / under invoice of dual-use, proliferation-sensitive or military goods, trade transactions.
- When goods destination/shipment country is different from the country, where proceeds are sent/ received without any plausible reason.

- Individual or entity targeted by sanctions or connected to a targeted person.
- Customer is involved in the supply, sale, delivery or purchase of dual-use, proliferation sensitive or military goods, particularly to higher risk jurisdictions.
- Customer or counterparty, or its address, is the same or similar to one of the parties found on public available lists or has a history of export control contraventions.
- The customer is a military or research body connected with a higher risk jurisdiction of proliferation concern.
- Customer is vague, particularly about end-user, provides incomplete information or is resistant to providing additional information when sought.
- New customer requests a letter of credit from a bank, whilst still awaiting approval of its account.
- Complex structure to conceal involvement – use of layered letter of credit, front companies, intermediaries and brokers.
- Transaction concerns dual use, proliferation sensitive or military goods whether licensable or not.
- Transaction demonstrates a link between representatives of companies exchanging goods e.g. same owners or management, in order to evade scrutiny of the goods exchanged.
- Transaction involves the shipment of goods inconsistent with normal geographic trade patterns i.e. where the country involved does not normally export or import the types of goods concerned.
- Order for goods is placed by firms or individuals from foreign countries, other than the country of the stated end-use
- Transaction involves financial institutions with known deficiencies in AML/CFT controls and/or domiciled in countries with weak export control laws or weak enforcement of export control laws.
- Unexplained time differences with obviously connected transactions.
- Inconsistencies in information contained in trade documents and financial flows e.g. names, addresses, final destination etc.
- Use of fraudulent documents and identities e.g. false end-use certificates and forged export or reexport certificates.
- Declared value of shipment under-valued in relation to shipping cost.
- Trivial description on customs declaration/export licence e.g. agriculture, electronics and pump (without further explanation of purpose/use).

- Technical descriptions altered.
- Transaction involves shipment of goods incompatible with the technical level of the country to which it is being shipped, (e.g. semiconductor manufacturing equipment being shipped to a country that has no electronics industry).
- Secondary data connected to targeted person (address, phone number).
- A freight forwarding firm being listed as the product's final destination.
- Circuitous route of shipment (if available) and/or circuitous route of financial transaction.
- Final destination or end-use unclear.
- Trade finance transaction involves shipment route (if available) through country with weak export control laws or weak enforcement of export control law.
- Wire instructions or payment from or due to entities not identified on the original letter of credit or other documentation.
- Pattern of wire transfer activity that shows unusual patterns or has no apparent purpose.
- Quantities below reporting thresholds in the context of multiple transactions.

The presence of a single red flag may not automatically make a transaction suspicious. However, combination of red flags with other indicators might warrant you to conduct a deeper investigation. You have an obligation to submit a Suspicious Activity Report or Suspicious Transaction Report to the FIU to report any suspicious or potentially suspicious transactions.

You need to properly understand your PF risk in order to be able to decide what measures to take to mitigate them, and the trade-related indicators above can be used to identify and classify potential threats and vulnerabilities. You should have your own policy regarding risk assessments.

In addition, PF should be included as a specific financial crime risk when providing training or conducting exercises to enhance staff awareness.

You can also use the table to strengthen due diligence procedures aimed at combating PF. As stated above, identifying PF is difficult because most transactions occur within normal business transaction pathways, and can be masked with all legitimate transactions.

Depending on your business model you could incorporate the trade related indicators into Know Your Customer (KYC) procedures, transaction screening procedures, transaction monitoring systems and suspicious activity investigations, regulatory reporting procedures, and due diligence connected to trade finance operations.

## ACTIONS TO MITIGATE PROLIFERATION FINANCING

In recognition that there is the possibility of PF occurring, as a result, reporting entities should develop robust AML standards and enforcement routines to reduce systemic exposure, include counter-proliferation financing considerations in:

- Employee training programmes
- Client and business risk assessments
- Compliance programmes with senior management oversight
- Know Your Customer procedures
- Transaction monitoring programmes
- Reporting procedures
- Develop situational awareness around various sanctions regimes by reading Panel of Experts reports.

This is very important as screening the consolidated list is not enough to detect proliferation and its financing. Even if you carry out appropriate CDD on clients, which includes screening names of clients and clients' counterparties, including shipping companies, beneficiaries of letters of credit and freight companies, against the consolidated list this is still not enough because the names of entities or individuals on sanctions lists rarely appear in financial transactions. This will also help with broadening your understanding of traditional North Korean names.

In addition, on paper, a transaction is rarely directly connected to a sanctioned country.

- Conduct risk assessment of customers and products and geographic location.
- Know Your Customer

For new and existing customers:

- Check customer identity
- Obtain proof of declaration
- Determine ultimate beneficial owner
- Include proliferation financing-specific questions in due diligence evaluations.
- Note any involvement in WMD technology supply chains o Identify if any export control regulations apply
- Be alert to the possibility that your customers may be engaging in, or facilitating, proliferation activities
- Assess due diligence practices of clients working with sensitive goods. o Assess client geographic activity and relations.

• Identify proliferation financing sensitive goods and activities

- Ensure trade finance is integrated into compliance procedures.
- Identify final destinations of goods and finances.
- Draw on export-control regime lists, and any other industry/component lists.
- Engage in partnerships with other relevant industries (insurance/shipping).

• Understand your geographic and activity exposure to proliferation financing risks

- Consider the importance of local market to international financial services.
- Evaluate relation/proximity to proliferator threat.
- Understand and assess own business exposure.
- Assess exposure to key trading hubs (strength of export/customs controls) and trade finance.

• Enhanced due diligence on: high-risk jurisdiction areas, client highlights concern, entity of concern involved is on watch list, usually currency or routes of payments and dual-use goods. Enhanced due diligence checks include:

- The origin of funds and the identity of the ultimate beneficial owner.
- That the wire is consistent with expected behaviour.
- Online open source image research of the address to determine whether the business premises matches the nature of the business.
- Open source research of the address, telephone number, names and emails to identify companies using the same details and news articles and other information on the entity.
- Examine entity on company registries, World Check etc., Panama Papers and other online resources to understand the nature of the entities business.

• Asset freezing is important to counter proliferation finance as it is not only act as deterrence to non-designated individuals and entities to assist but promotes international cooperation and forces proliferators to engage in riskier costly alternatives.

A significant obligation under our domestic legislations is for you to freeze without delay and without prior notice, the funds or economic resources owned, held or controlled by a designated person. You are also prohibited under domestic legislation from:

- dealing with the funds or economic resources belonging to or owned, held or controlled by a designated person,
- making funds or economic resources available, directly or indirectly, to, or for the benefit of, a designated person, or
- Engaging in actions that directly or indirectly circumvent the financial sanctions.

• You must submit a SAR or STR to the FIU to report any suspicious or potentially suspicious transactions.

• As soon as practicable, if you know or have a reasonable cause to suspect that a person is a designated person or has committed an offence under any sanctions legislation, complete and submit a SAR to the FIU.

Please see the link below to additional typologies –

study-of-typologies-of-financing-of-wmd-proliferation-2017.pdf (kcl.ac.uk)

Any further questions may be directed to-

*Your Supervisory Authority*

*The Financial Intelligence Unit*

*The AML/CFT/PF National Coordination Committee Secretariat in the Attorney General's Chambers*.