JULY 2025

GUIDANCE ON THE RISK OF ABUSE OF NON-PROFIT ORGANIZATIONS FOR TERRORIST PURPOSES

1. Introduction

Non-Profit Organizations[1] ("NPOs") are critical stakeholders in the national and international community, performing much needed charitable, social and cultural work that enriches the lives of individuals, communities and countries as a whole. As with other organizations, NPOs are diverse in their structure, purpose and reach with some operating internationally and others securing support from foreign donors. Their efforts complement the activity of the government and business sectors in providing essential, sometimes life-saving, support, comfort and hope to those in need. Well-functioning NPOs may also help to prevent terrorism by preventing radicalization and extremism through targeted support to vulnerable persons and communities. While some NPOs operate within highly vulnerable local communities, others may directly or indirectly provide relief to high-risk communities abroad including in conflict zones.

Over the past two decades however, the potential for misuse of non-profit NPOs by terrorists and terrorist organizations has been widely recognized. Terrorism can be motivated by political, religious or ideological objectives and uses violence or other inimical acts to advance such a cause. It can be domestic or international and on occasion both can be linked, with terrorists or their supporters or agents exploiting advances in global travel.

The noble efforts and willingness of NPOs to engage in their selfless works also makes them targets for misuse by terrorists and terrorist organizations in several ways including:

- By terrorist organizations posing as legitimate entities;
- By providing logistical and other types of support for example, encouraging terrorist recruitment;
- To exploit legitimate NPOs as conduits for terrorist financing, including for the purpose of escaping asset freezing measures; and
- To conceal or obscure the clandestine diversion of funds, which were intended for legitimate purposes, to terrorists or terrorist organizations.

To counter these risks, appropriate risk-based mitigation measures can however be taken by NPOs and thus give the local and international donor community greater confidence in the NPO and the NPO sector as a whole. This also helps to address some of the concerns of financial institutions ("FIs")

[1] An NPO is a legal person, arrangement or organization that primarily raises or disburses funds for charitable, religious, cultural, educational, social, or fraternal purposes or carries out other "good works".

and listed businesses ("LBs") that have the potential to result in the termination of or refusal to enter into business relationships with an NPO. FIs and LBs are themselves subject to strict anti-money laundering, combatting the financing of terrorism and countering the proliferation of weapons of mass destruction ("AML/CFT/CPF") laws and obligations. Transparency of NPOs when dealing with FIs and LBs can help those businesses and professionals to meet these AML/CFT/CPF requirements. It also enhances FIs and LBs understanding of the risks related to the NPOs and what is considered "normal" for the sector, thus helping to ensure that only reasonable safeguards are taken. This can ultimately increase the ease of individual NPOs and NPOs in general accessing the services of FIs and LBs.

It should be noted that NPOs are not subject to the same requirements to protect themselves against the risk of abuse for terrorist purposes as FIs and LBs[2]. Trinidad and Tobago has however adopted focused, proportionate and risk-based measures to address the TF risks identified through the National NPO Risk Assessment and the mechanisms by which the National Anti-Money Laundering and Combatting the Financing of Terrorism Committee maintains an ongoing understanding of the risk of NPO abuse.

2. NPO Abuse

NPO's can be exploited in various ways by individuals both inside and outside the organization, such as:

Funding Abuse

Funds related to an NPO can be abused in several ways:

- Funds may be solicited from donors in the name of an NPO for a charitable purpose but may instead be used for terrorist purposes with or without the knowledge of the NPO;
- Funds which were legitimately raised for charitable purposes and being transferred may be diverted before reaching their intended beneficiary; and
- An NPO might be used by a donor to launder money (including terrorist funds) or be used as a legitimate front for transporting cash or other financial support from one place to another in support of terrorist activity.
- Stronger monitoring, financial controls and due diligence measures help to reduce these risks of abuse by officers of the NPO, donors or recipients of support.

NPO property

Various categories of property, including vehicles and real-estate, can be abused for terrorist purposes. Vehicles may be used to transport terrorist personnel, funds, weapons and supplies. NPO

[2] The Miscellaneous Provisions (Proceeds of Crime, Anti-Terrorism, Financial Intelligence Unit of Trinidad and Tobago, Securities, Insurance, Non-Profit Organisations, Civil Asset Recovery and Management and Unexplained Wealth and Miscellaneous Provisions [FATF Compliance]) Act, No. 17 of 2024, s. 3(e)(iv) amended the Proceeds of Crime Act, Chap 11:27 (POCA) and removed NPOs from the Second Schedule which identifies businesses which are subject to the provisions of POCA.

premises may be used for storage, housing, training or recruitment. The communications infrastructure of an NPO, including its information technology systems, could also be misused by terrorists for internal communication, operational coordination, recruitment, and even fundraising. Such vulnerabilities may also lead to ransomware incidents or other forms of cyberattacks targeting essential services like utilities, hospitals, and financial institution.

Abuse of the NPO's name

Terrorists may use the name or reputation of a legitimate NPO in order to gain access to a region or community. In some cases, such cover is used for travel to conflict zones or other difficult to reach areas to attend terrorist training or provide other support for terrorism.

A recipient of support from an NPO may also use such funds to directly or indirectly further terrorism. Examples include but are not limited to:

- Funding a hospital controlled by a terrorist organization which gives priority to the treatment of its fighters or their families; and
- Funding a school that teaches terrorist ideology, even if alongside other mainstream classes.

Abuse by Officers of an NPO

Officers of an NPO may abuse it in different ways. For example, NPO funds may be diverted for terrorist purposes. NPO property may be used for transport, housing, training, promoting or recruitment. In other cases, the NPO may have been established solely for the purpose of tricking donors into providing funding which will in reality be used for terrorist purposes.

Purpose of due diligence regarding the potential financier[3]

The purpose of due diligence regarding a prospective financier is to help identify and manage risks associated with the business relationship. This process ensures that the relationship does not exceed acceptable limits and aligns with risk characteristics. By conducting due diligence, organizations can gather necessary information and documents to mitigate and prevent involvement in money laundering, terrorism financing, and proliferation from the start of the business relationship. This includes documenting identifying information, true beneficiaries, sources of funding, and analysing any negative information about the financiers, as well as monitoring transactions.

Further guidance can be found on due diligence on the FIUTT website: CUSTOMER DUE DILIGENCE GUIDANCE TO SUPERVISED ENTITIES

3. Assessing Risks Related to Donors/Know Your Donor

As with all other aspects of NPO administration, not every donor poses the same level of risk to the NPO. The same approach to assessing such risk would therefore not be appropriate for each donor.

3 **NVO document**- ***ETHICAL FUNDING GUIDELINES (Approved on October 26, 2020)***

Depending on the circumstances, some of the following factors may be important in assessing such risk:

- Who are the donors?
- What is known about them?
- Does the NPO have a well-established relationship with them?
- Do any additional identity checks need to be made for individual donors or donor organizations? (Publicly available information such as via the internet or the Companies Registry of the Ministry of Legal Affairs may be useful sources of information. Such information may be similarly available in the home country of a foreign donor.)
- How is the money being received? (Cash, cheque, bank transfer or some other means?
- Have any public concerns been raised about the donors or their activities? If so, what was the nature of the concerns and how long ago were they raised? Did any law enforcement or regulatory body investigate the concerns? What was the outcome?
- How large is the donation?
- Is the donation in the form of a loan? If so, can the source of the funds be identified or checked by the NPO? Is there a condition that funds are only to be retained by the NPO for a period and then returned to the donor, with the NPO retaining the interest?
- Are there unusual or substantial one-off donations?
- Does the donation come with any conditions attached? What are they? Are they reasonable?
- Is the donation conditional on particular organizations or individuals being used to apply the funds?
- Is the donation conditional on being applied to benefit particular individuals either directly or indirectly?
- Is there a suspicion that the NPO is being used as a conduit for funds to a third party?
- Is the donation in one currency with a requirement that the donation be returned in a different currency?
- Is the donation received from a known donor but through an unknown party or an unusual payment mechanism where this would not be a typical method of payment?
- Are any of the donors based, or does the money originate, outside the Trinidad and Tobago? If so, from which country? Does this country/area pose any specific risks?
- Are donations received from unknown bodies or international sources in countries where financial regulation or the legal framework is not rigorous? (Risks related to geography is discussed further below).
- Is anything else unusual or strange about the donation?

While not all of these questions need to be answered in respect of each donor in assessing risk, it should be noted that in some cases, having this information would also help the NPOs satisfy the AML/CFT/CPF requirements of FIs or LBs whose services the NPO wishes to access. Developing a good working relationship with the FI or LB will help the NPO understand how improvements to the NPOs governance and due diligence can maintain and improve access to these services.

4. Assessing Risks Related to Geography

Some geographical regions, which may range from a part of a country to multiple countries, may pose higher risk of abuse to NPOs. While there are no universally recognized criteria for assessing and determining risk in particular countries or geographic regions, areas with higher risk may include but are not limited to:

- Regions where terrorists or terrorist organizations are known to operate;
- Countries subject to sanctions by the United Nations or other international organizations;
- Countries or regions vulnerable due to internal conflict or criminal activity; and
- Countries identified by the Financial Intelligence Unit, the Financial Action Task Force (FATF) or FATF-styled regional bodies (e.g., the Caribbean Financial Action Task Force) as having weak anti-money laundering, terrorism financing and proliferation financing laws and enforcement of these laws. These organizations publish lists of such countries which can be easily accessed via the internet.

Other factors which could be taken into account in assessing risk related to geography include:

- The types of services provided by the NPO;
- Strength of local laws and law enforcement;
- The political environment and the ability of the State to govern the region;
- The extent and types of criminal activity in the region;
- The size and reliability of FIs; and
- The main channels available for financial transactions.

5. Sending and Receiving Money

Law enforcement agencies have identified sending and receiving of money, particularly to and from abroad, as posing an increased risk of abuse of NPOs in Trinidad and Tobago. The informal money transfer sector and underground activities provide an extremely high risk of abuse for terrorist financing. FIs in Trinidad and Tobago and in other countries are heavily regulated to guard against such abuse regarding funds being sent out of or received into the country. **NPOs are therefore strongly advised to use the formal mechanisms through established FIs wherever possible.**

It should also be noted that cash presents increased risks both in terms of receiving and disbursing funds, limiting the ability of the NPO to identify the source of funds from donors and to track the use of funds when disbursed by the NPO. The NPO, after recording, should promptly deposit all received funds into an account maintained by the NPO at a financial institution. In particular, all cash donated should be promptly deposited into the NPO's financial institution account.

The NPO should also make disbursements by cheque or electronic means rather than in cash whenever such financial arrangements are reasonably available. Where these financial services do not exist or other exigencies require making disbursements in cash, the NPO should disburse the cash in the smallest increments sufficient to meet immediate and short-term needs or specific projects rather than in large sums intended to cover needs over an extended time frame. The NPO should exercise oversight regarding the use of the cash for the intended charitable purposes, including keeping detailed internal records of such cash disbursements.

Trinidad and Tobago has completed its 2nd National Money Laundering and Terrorism Financing Risk Assessment (NRA) consistent with FATF Recommendation 1, which requires countries to identify, assess and understand their money laundering and terrorist financing (ML/TF) risks and take mitigating actions. The NRA exercise was conducted using the National Money Laundering and

Terrorism Financing Risk Assessment Tool developed and provided by the World Bank.

The NRA ensures that all stakeholders have a contemporary understanding of ML/TF risks and provides a foundation for applying a risk-based approach to their AML/CFT activities. It therefore is a critical resource for Competent Authorities, Financial Institutions (FIs), Listed Businesses (LBs) and other stakeholders in developing and implementing policies, procedures and actions. FIs and LBs in particular are required to review the NRA and update their institutional ML/TF risk assessment accordingly. The wider Public is also encouraged to access and utilize the NRA report as appropriate. The NRA can be found on the following link : https://www.agla.gov.tt/anti-terrorism-unit/atu-namlc/trinidad-and-tobagos-national-risk-assessment/

Further guidance on the benefits of the use of regulated financial institutions and payment channels and the risks of using cash can be seen in the FATF Best Practices Paper on Combatting the Terrorist Financing Abuse of Non- Profit Organizations which can be found at https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/BPP-Combating-TF-Abuse-NPO-R8.pdf.coredownload.inline.pdf

6. Legislation

The Non-Profit Organisation Act, No. 7 of 2019 sets out a registration and regulatory framework designed to protect the NPO sector in Trinidad and Tobago. While some key provisions are set out below, NPOs should become familiar with the entire Act.

Key provisions of the Act include:

- **Section 5** – All NPOs must register at the Registrar General's Department (RGD) and upon registration all NPOs must complete an AML/CFT Questionnaire. Please note that this registration process does not change their status/capacity on whether they are legal entities or not. NPOs are not required to be incorporated under the Companies Act, Chap. 81:01 or to otherwise be structured as a legal person;
- **Section 13** – NPOs must keep proper financial accounts and records which can be disclosed at any time;
- **Section 14** – NPOs with gross annual income exceeding $10,000,000.00 shall have their financial accounts and records audited and reported on annually by a qualified auditor. The audit must be submitted to the RG whenever requested;
- **Section 18** – NPOs must keep records of its purposes and activities, controllers, senior officers, directors, trustees and source of its gross annual income; and
- **Section 19 –** This sets out the criteria disqualifying a person from serving as a controller of an NPO.

Many of the areas discussed in the paragraphs above are subject to criminal offences under the Anti-Terrorism Act, Chap. 12:07 such as:

- Section 5 – Collection of provision of property for the commission of a terrorist act;
- Section 6 – Use of property for the commission of a terrorist act;

- Section 7 – Arrangement for the retention of control of terrorist property;
- Section 8 – Dealing with terrorist property;
- Section 9 – Soliciting or giving support for the commission of a terrorist act;
- Section 15 – Providing facilities in support of a terrorist act; and
- Section 22A – Financing of terrorism.

It should be noted that Section 2A provides that these and other offences under the Act apply whether or not the offence took place within or outside of Trinidad and Tobago. NPOs should thus equally exercise due diligence in respect of their international activities including sending and receiving funds, supplies and personnel.

The Financial Intelligence Unit of Trinidad and Tobago Act, Chap. 72:01 (FIUTT Act), s. 18J provides for the FIUTT as the **oversight** body for NPOs. It mandates that the FIUTT take measures to promote focused, proportionate and risk-based oversight of NPOs in its role as the Oversight Authority. The FIUTT is specifically empowered to issue guidelines about the vulnerabilities of NPOs in respect of terrorist financing abuse and risks and the measures NPOs can take to protect themselves against such abuse and risks. This is aimed at preventing the abuse of civil-society spaces as "fronts" for illicit conduct.

The provisions in the FIUTT Act above compliment Non-Profit Organisation Act, No. 7 of 2019[4] (NPO Act) which further outlines the responsibilities of FIUTT as the oversight authority, including providing AML/CFT/CPF oversight and guidance to NPOs who:

- meet the FATF functional definition of NPOs; and
- have been identified as at risk by an AML/CFT/CPF sector risk assessment carried out by the supervisory authority or NRA.

Trustees and officers of NPOs should however familiarize themselves with the NPO Act and the Anti-Terrorism Act. The Economic Sanctions Act, Chap. 81:05 and The Economic Sanctions (Implementation of United Nations Resolutions on the Democratic People's Republic of Korea) Order, 2018 contain AML/CFT/CPF provisions that apply to the public generally, including NPOs and their officers.

There can sometimes be a link between terrorism and money laundering or proliferation of weapons of mass destruction. Money laundering is a process aimed at concealing the illegal origin of profits of crime. Terrorist financing is the collection or provision of funds for terrorist purposes. Unlike money laundering where the funds are always the proceeds of a crime, terrorism can be financed through both legal and illegal sources. Money laundering techniques can be used to funnel the proceeds of crime to terrorists or terrorist organizations. These techniques can also be used to mask the movement of funds for terrorist purposes regardless of the legitimacy of their source. Terrorists and other non-state actors may also seek to acquire nuclear, chemical, biological or radiological weapons (WMDs) to carry out terrorist attacks. In other cases, proliferating states may either fund terrorists or terrorist

[4] The Miscellaneous Provisions (Proceeds of Crime, Anti-Terrorism, Financial Intelligence Unit of Trinidad and Tobago, Securities, Insurance, Non-Profit Organisations, Civil Asset Recovery and Management and Unexplained Wealth and Miscellaneous Provisions [FATF Compliance]) Act, No. 17 of 2024, s. 8 amended the NPO Act in this regard.

organizations or provide them with material support, including through providing weapons platforms which may be used to deliver WMDs. Such states may also rely on terrorist funds to advance their proliferation goals.

Both the Anti-Terrorism regime and the counter-proliferation financing regime established under Trinidad and Tobago's legislative framework incorporate lists of persons and entities, either designated by Trinidad and Tobago or by the United Nations Security Council or its committees, against whom sanctions apply. Such persons or entities are referred to as "listed entities". Persons and organizations within Trinidad and Tobago, including NPOs, are prohibited from providing property, financial or other support to such listed entities. It should be notes that breaches of these prohibitions can result in the imposition of criminal sanctions in accordance with the Anti-Terrorism Act and the proliferation financing legislation discussed above.

7. Reporting of Suspected Terrorist Financing Abuse

Section 32 and 33 of the Anti-Terrorism Act, Chap. 12:07 provides:

33. (1) Every person shall forthwith disclose to the FIU—

> (a) the existence of any property in his possession or control, which to his knowledge is terrorist property, or which there are reasonable grounds to believe is terrorist property;
> (b) any information regarding a transaction or proposed transaction in respect of terrorist property; or
> (c) any information regarding a transaction or proposed transaction which there are reasonable grounds to believe may involve terrorist property.

(5) No civil or criminal proceedings shall lie against any person for making a disclosure or report, in good faith, under subsection (1), (2) or (3).

(6) Every person who fails to comply with subsection (1) or (3) commits an offence and shall, on conviction on indictment, be liable to imprisonment for five years.

32. (1) Every person or regulatory authority who has any information which will assist in—

> (a) preventing the commission by another person, of a terrorist act; or
> (b) securing the arrest or prosecution of another person for an offence under this Act, or an offence under any other law and which also constitutes a terrorist act, shall forthwith disclose the information to a police officer or the Central Authority as defined under the Mutual Assistance in Criminal Matters Act.

(2) Notwithstanding subsection (1) a person referred to in subsection (1), shall not be required to disclose any information which is protected by privilege.

(3) Civil or criminal proceedings shall not lie against any person for disclosing any information in good

faith pursuant to subsection (1).

(4) Any person who fails to comply with subsection (1) commits an offence and is liable on conviction on indictment to a fine of ten thousand dollars and to imprisonment for two years.

Officers of an NPO who in good faith believe that they have information which will assist in preventing a terrorist act, including terrorist financing or any other offence under Parts II, III or IIIA of the Anti-Terrorism Act, must therefore disclose this information to the police. When acting in good faith the officer of the NPO is protected from civil or criminal proceedings resulting from making such report.

Such reports can be made to:

- The Special Brach of the Trinidad and Tobago Police Service by contacting them at 1-868-628-8925 ext 12052 or sb.anti-terrorism@ttps.gov.tt;
- The Financial Investigations Branch at Riverside Plaza, Besson St, Port of Spain, via telephone at 1-868-627-4281 or email at fibchiefclerk@ttps.gov.tt;
- In addition, reports can be made to any police station in Trinidad and Tobago which would then be directed to the relevant authorities.

Further guidance can be accessed on FIUTT website on the reporting : TFS Guidance Notes – Financial Intelligence Unit

8. Donor Support for Mitigating the Risk of Abuse of NPOs for Terrorist Purposes

Support from donors to sector organizations or umbrella NPOs, by means of training or shared resources, can be beneficial to strengthen due diligence and risk management mechanisms of NPOs that lack the necessary resources and capacity. Practical guidance, tailored to specific contexts, operational or organizational characteristics can support better alignment of risk management mechanisms and broader implementation. For donors, it is good practice to undertake reasonable steps to research reliable publicly available materials in order to ascertain how an NPO operates, how it is managed, the nature of its programmes and where they operate. This is especially true for NPOs that operate in areas where there is known risk of terrorist activity.

9. Further Information

For further information, please contact:
The Anti-Terrorism Unit,
Office of the Attorney General,
AGLA Tower,
Cor. London & Richmond Streets, Port of Spain
Tel: (868) 223-AGLA (2452) ext. 3815
E-mail: antiterrorismunit@ag.gov.tt

NOTICE

This document has been prepared for information purposes only and does not relieve you of any obligation under the laws of Trinidad and Tobago. Members of the public should familiarize themselves with the Anti-Terrorism Act, Chap. 12:07, the Non-Profit Organization Act, No. 7 of 2019 and all other relevant laws. This document is not intended as and does not constitute legal advice. Each case is unique and members of the public, including officers of NPOs should seek the advice of a qualified attorney-at-law with respect to their particular case.

AGLA Tower, Government Plaza,
Corner of London and Richmond Streets, Port of Spain
Tel: 223-AGLA (2452) EXT: 3772/3794 Email: antiterrorismunit@ag.gov.tt