Australian Government
AUSTRAC

FIGHTING FINANCIAL CRIME TOGETHER

PROLIFERATION FINANCING IN AUSTRALIA

NATIONAL RISK ASSESSMENT

COPYRIGHT

This risk assessment is intended to provide a summary and general overview. It does not set out the comprehensive obligations under the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (AML/CTF Act), the Anti Money Laundering and Counter Terrorism Financing (Prescribed Foreign Countries) Regulations 2018 (AML/CTF Regulations) or the Anti Money Laundering and Counter Terrorism Financing Rules Instrument 2007 (No. 1) (AML/CTF Rules). It does not constitute nor should it be treated as legal advice or opinion. The Commonwealth accepts no liability for any loss suffered as a result of reliance on this publication. AUSTRAC recommends that independent professional advice be sought.

CONTACT US

If you have questions about your AUSTRAC compliance obligations, or enquiries regarding the licence and any use of this report please email contact@austrac.gov.au or phone 1300 021 037 (within Australia).

AUSTRAC is committed to continual improvement and values your feedback on its products. We would appreciate notification of any outcomes associated with this report by contacting AUSTRAC at austrac.gov.au/contact-us/form.

CONTENTS

EXECUTIVE SUMMARY

Australia is committed to ensuring the country and its financial system are resilient in preventing the proliferation of **weapons of mass destruction** (WMD) and the financing or support of these activities.

Australia combats **proliferation financing** through comprehensive sanctions regimes and a complementary anti-money laundering and counter-terrorism financing (AML/CTF) framework. Australia also maintains robust legal and operational counter-proliferation and **counter-proliferation financing** frameworks. Australia's National Intelligence Community (NIC) and other agencies work together to provide wide-ranging intelligence collection capabilities and a significant toolkit for disrupting threat actors and networks.

In October 2020, the Financial Action Task Force (FATF) – the international body that sets AML/CTF standards – revised Recommendation 1 (R.1) and Interpretive Note to R.1 of their global standards on countering financial crime. Under the amended recommendation countries should identify, assess, understand and mitigate risks associated with proliferation financing, specifically the *potential breach, non-implementation or evasion of targeted financial sanctions (TFS) obligations relating to the DPRK and Iran*.

This national risk assessment adopts a broad approach to proliferation financing risk. It goes beyond FATF R.1 requirements and assesses Australia's exposure to a wide range of direct and indirect proliferation financing threats.

This assessment brings together expertise from across government and a wide range of private sector stakeholders, to provide a contemporary, consolidated picture of proliferation financing risk, how it is combatted and where efforts can be improved. Completion of this assessment is an important step in strengthening Australia's efforts in combatting proliferation financing, as well as ensuring Australia meets its international obligations. This assessment will also raise awareness among the private sector and encourage businesses to continue improving their investigations of proliferation financing activity.

THREAT ENVIRONMENT

State-based or state-linked procurement networks that target Australia operate on behalf of the Democratic People's Republic of Korea (DPRK) and Iran, as well as other countries of proliferation concern. There has also been activity by non-state actors that may pose an increasing threat as new technologies become more available to the general public.

Procurement networks aim to export restricted, sensitive or dual-use goods and the associated intellectual capital or knowledge with countries of proliferation concern or with entities sanctioned for proliferation activity.

The most significant proliferation financing **threats** facing Australia include the:

- use of Australian financial services and infrastructure to procure dual-use goods and evade sanctions
- use of Australia-based corporate structures to facilitate proliferation financing and evade sanctions
- use of Australian or third-country nationals to facilitate proliferation financing and evade sanctions
- exploitation of Australian citizens to source and export sensitive technologies and knowledge for **actors of proliferation concern**
- use of designated non-financial businesses and professions (DNFBPs) to facilitate proliferation financing and evade sanctions.

Procurement networks use a range of methods to help obscure their illicit activities and evade sanctions. For example:

- using front or shell companies
- mislabelling goods
- sourcing either components or sub-components from a variety of suppliers
- using transhipment hubs to hide the ultimate destination of goods
- exporting goods just under control or reporting thresholds.

NATIONAL VULNERABILITIES

A wide range of national proliferation financing **vulnerabilities** were considered as part of this risk assessment. Key vulnerabilities are listed below.

Economic and trade factors:

- Australia's extensive economic relations and trade with Asian markets, a number of which have historically been a popular destination for transhipment of sanctioned goods.
- High volume of dual-use and proliferation-sensitive exports.
- A large mining industry that exports metals and materials subject to United Nations Security Council (UNSC) and Australian sanctions restrictions, which could be diverted to the DPRK or Iran.

Legislative and regulatory factors:

- Lack of reporting requirements for key types of DNFBPs, such as lawyers, accountants and company service providers.

- Poor transparency of companies and trusts (otherwise known as legal persons and legal arrangements), including ultimate beneficial ownership structures, that can be misused to enable and conceal proliferation financing.

Industry and technology factors:

- Limited awareness of proliferation financing risk exposure and indicators in some financial service sectors.
- A large financial services sector, including digital currency exchanges, that is exposed to cyberattack or misuse by proliferators.

POTENTIAL BREACH, NON-IMPLEMENTATION OR EVASION OF TARGETED FINANCIAL SANCTIONS

RISK[1]	THREAT RATING[2]	VULNERABILITY RATING[3]
Potential breach or non-implementation	●	●
Potential evasion	●	●

AUSTRAC assesses the risk of potential breach or non-implementation of targeted financial sanctions (TFS) obligations relating to the DPRK and Iran to be **low**.

- Australia implements robust sanctions regimes. The Australian Sanctions Office conducts private sector outreach and has resources in place to help industry understand and meet their sanctions obligations, including TFS.
- Findings from an industry survey (see page 13 for more information) indicate a very high understanding of and compliance with TFS obligations relating to the DPRK and Iran – particularly among those reporting entities most at risk, such as entities processing high volumes of international transactions or offering trade finance products.

AUSTRAC assesses the risk of potential evasion of TFS relating to the DPRK and Iran to be **medium**.

- The extent of suspected and known cases of TFS evasion is relatively low. However, the nature of all proliferation financing threat typologies noted in this report are used to evade TFS. These typologies do not require extensive knowledge or expertise to establish and use.
- All national vulnerabilities noted in this report can be exploited to either facilitate TFS evasion or complicate detection efforts by financial institutions and authorities.

[1] While AUSTRAC recognises that overall risk is a function of threats, vulnerabilities and consequences, this assessment focusses on analysing threats and vulnerabilities.

[2] Refer to the '**Methodology'** section of this report for an explanation of the risk rating system.

[3] Ibid.

CONSEQUENCES

The potential **consequences** of proliferation financing activities involving Australia are diverse. Australia's position in the broader geostrategic arena with the DPRK, as well as its close economic and diplomatic ties with the United States and the Indo-Pacific region, means that any regional instability caused by the DPRK's nuclear program has important security and economic implications for Australia. Breaches of proliferation financing sanctions would likely raise concerns over the integrity and effectiveness of Australia's counter-proliferation financing framework.

Proliferation financing activities that involve other forms of financial or serious and organised crime divert funds from Australia's legitimate economy. This could negatively impact the reputation of the Australian economy and financial system.

INTRODUCTION

This is Australia's first national risk assessment of proliferation financing. AUSTRAC has completed this assessment as Australia's financial intelligence unit. The Australian Sanctions Office in the Department of Foreign Affairs and Trade (DFAT) is the Australian government sanctions regulator.

AUSTRAC wishes to acknowledge and thank the Royal United Services Institute (RUSI) in London, a global leader in proliferation financing risk assessment, for their important contributions to this project. In preparation for this assessment, RUSI completed a comprehensive report based on open-source information outlining Australia's proliferation financing risk environment. This report was a key resource in completing this assessment.

BACKGROUND

In October 2020, FATF revised R.1 and Interpretive Note to R.1 of their global standards on countering financial crime. Under the amended recommendation countries should identify, assess, understand and mitigate the risks of potential breach, non-implementation or evasion of TFS obligations relating to the DPRK and Iran. FATF provides explanations for these terms, which are detailed on the next page. The revised recommendation applies to government agencies and financial institutions, as well as businesses and professions that may enable financial activity (such as lawyers, accountants, real estate agents and company and trust services providers), and digital currency service providers.[4]

[4] Businesses may assess proliferation financing risk as part of their pre-existing sanctions or financial crimes compliance programs. They are not obliged to complete a separate risk assessment. Businesses may wish to refer to FATF's website for guidance on conducting enterprise risk assessments, including detecting and reducing exposure to proliferation financing and sanctions evasion risk. For the latter, please see FATF's recently updated Guidance on Proliferation Financing Risk Assessment and Mitigation.

BREACH OR NON-IMPLEMENTATION OF TFS[5]

This risk may materialise when designated entities and individuals access financial services, and/or funds or other assets, as a result, for example, of delay in communication of designations at the national level, lack of clear obligations on private sector entities, failure on the part of private sector entities to adopt adequate policies and procedures to address their proliferation financing risks (e.g. weak customer on-boarding procedures and ongoing monitoring processes, lack of staff training, ineffective risk management procedures, an inadequate sanctions screening system having regard to the nature, size and complexity of the relevant business, irregular or inflexible screening procedures, or a general lack of compliance culture).

EVASION OF TFS

This risk may materialise due to concerted efforts of designated persons and entities to circumvent TFS, for example by using shell or front companies, joint ventures, dummy accounts, middlemen and other fraudulent/sham intermediaries.

SCOPE

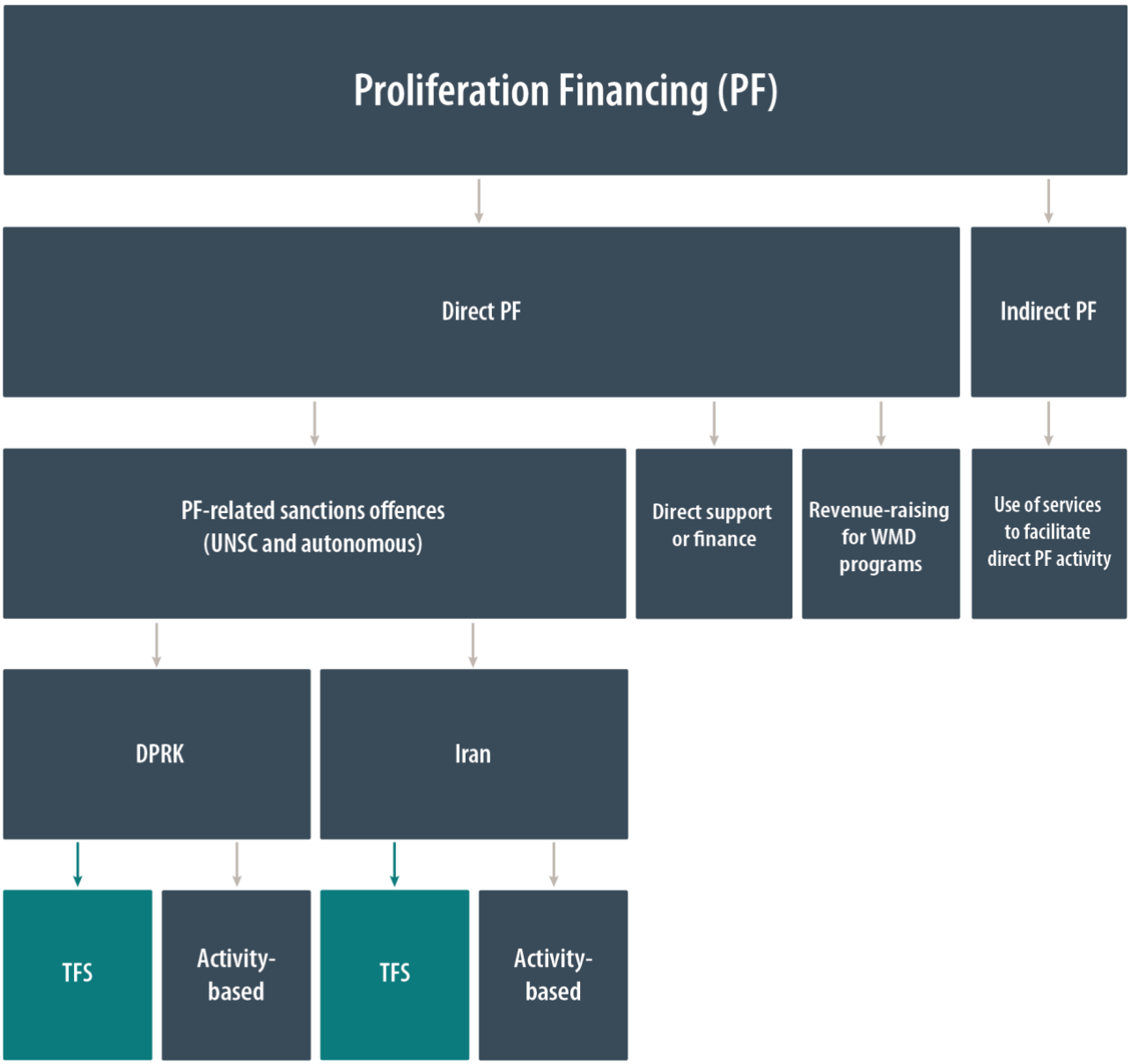
This assessment adopts a broad approach to proliferation financing risk. It goes beyond requirements under FATF R.1 to assess TFS obligations relating to the DPRK and Iran and assesses Australia's exposure to a wide range of direct and indirect proliferation financing threats (see **diagram A**).

To be in scope, threats must have a connection to Australia, or threaten Australia's financial system, key industries and technologies or national security.

While this assessment focuses on threats relating to the DPRK and Iran in line with FATF requirements, other actors of proliferation concern are included where there is evidence of proliferation financing threats to or activity in Australia.

[5] The definitions in this call-out box are provided in FATF's recently updated Guidance on Proliferation Financing Risk Assessment and Mitigation.

DIAGRAM A: RANGE OF ACTIVITIES ASSESSED IN THIS REPORT (FATF R.1 OBLIGATIONS IN GREEN)



DEFINING PROLIFERATION FINANCING

This assessment adopts RUSI's working definition of proliferation financing (provided in the call-out box below). This definition is in line with the broad approach of this assessment. It includes activities that may indirectly finance or support proliferation efforts, such as establishing opaque corporate structures and banking arrangements to facilitate illicit financial transactions.[6]

Proliferation financing is when a person:

a. makes available an asset; or

b. provides a financial service; or

c. conducts a financial transaction; and

the person [knows that, or is reckless as to whether,] the asset, financial service or financial transaction is intended to, in whole or in part, facilitate the proliferation of WMDs, regardless of whether the activity occurs or is attempted.

The specified activities that comprise **WMD proliferation** include:

a. the manufacture, production, possession, acquisition, stockpiling, storage, development, transportation, sale, supply, transfer, export, transhipment or use of:

   i. nuclear weapons; or

   ii. chemical weapons; or

   iii. biological weapons; or

   iv. materials related to nuclear weapons, chemical weapons or biological weapons that are prescribed by Regulations; or

b. the provision of technical training, advice, service, brokering or assistance related to any of the activities in Paragraph (a).[7]

UNDERSTANDING SANCTIONS

Sanctions are measures that do not involve using armed force that are imposed in situations of international concern. Sanctions can impose financial restrictions and/or travel bans on activities that relate to specific countries or in response to egregious acts - such as proliferation of WMD, significant cyber incidents, serious violations or serious abuses of human rights and serious corruption; jurisdictions; goods and services; and persons and entities.

TFS are one type of measure that is used in a sanctions regime. TFS prohibit:

- directly or indirectly making an asset available to (or for the benefit of) a person or entity recorded on a sanctions list (also known as a listed or 'designated' person or entity)

[6] In 2010, FATF offered the following working definition of proliferation financing: *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.* International feedback and guidance suggests this definition may not capture all proliferation financing activities. Most notably it does not include indirect proliferation financing activities such as establishing opaque corporate structures and banking arrangements to facilitate illicit financial transactions.

[7] Royal United Services Institute's (RUSI) Model Law on Proliferation Financing (RUSI, Guide to Conducting a National Proliferation Financing Risk Assessment, 2019).

- an asset-holder using or dealing with an asset that is owned or controlled by a designated person or entity. As these assets cannot be used or dealt with, they are referred to as 'frozen'.

FATF RECOMMENDATION 7[8]

FATF Recommendation 7 requires countries to implement TFS to comply with UNSC resolutions relating to the DPRK and Iran. This includes proliferation financing-related TFS made under UNSC Resolution 1718 (2006) and UNSC Resolution 2231 (2015) and their (future) successor resolutions.

The scope and nature of DPRK-related sanctions have been expanded following the country's repeated violations of UNSC resolutions. On the other hand, UNSCR 2231 (2015), endorsing the Joint Comprehensive Plan of Action (JCPOA), terminated previous provisions of resolutions relating to Iran and WMD proliferation, but retained TFS on a number of designated individuals and entities.

AUTONOMOUS SANCTIONS AND PROHIBITIONS

In addition to TFS and activity-based sanctions mandated by the UNSC, countries may implement their own sanctions, either unilaterally or as a group (as in the case of the European Union). Breach of unilateral sanctions (referred to as 'autonomous sanctions' in Australia), especially US sanctions, may have significant consequences for governments and private entities. Entities that breach certain US sanctions provisions and prohibitions may be subject to legal action by the US government or be denied access to the US financial system and markets, with serious reputational and economic consequences.

This assessment focuses on Australian sanctions law only. Entities that operate or transact with customers outside Australia may wish to assess their exposure to the risk of breach or evasion of US sanctions and of other autonomous sanctions regimes.

METHODOLOGY

This assessment follows guidance and reporting from FATF and other international bodies on risk assessment methodology. Generally, it follows three key stages of risk assessment development: identification, assessment and evaluation of evidence.

RISK MODEL

This assessment differs from AUSTRAC's other money laundering and terrorism financing (ML/TF) risk assessments. AUSTRAC recognises that overall risk is a function of threats, vulnerabilities and consequences. However, this assessment concentrates on analysing proliferation financing threats and vulnerabilities, with consequences touched upon briefly (in the executive summary). This is consistent with updated FATF guidance, which notes countries may wish to focus primarily on achieving a comprehensive understanding of their threats and vulnerabilities given the challenges of determining and estimating proliferation financing consequences.[9]

[8] The FATF Recommendations set out a comprehensive and consistent framework of measures which countries should implement in order to combat money laundering and terrorist financing, as well as the financing of proliferation of WMD. The Recommendations are available at Documents - Financial Action Task Force (FATF) (fatf-gafi.org).

[9] While it is generally recognised that WMD proliferation carries significant consequences – from regional instability to potentially catastrophic loss of life – the consequences of proliferation financing activities are not always readily identifiable or easy to measure. For example, it is generally impossible to measure the harm of a financial activity designed to obscure a procurement, other than a potential estimate of the value of illicit funding.

WEIGHTINGS

This assessment uses weightings of low, medium and high to estimate the risk of potential breach, non-implementation or evasion of TFS obligations relating to the DPRK and Iran. An explanation of each weighting is listed in the below table.

CONDITIONAL RISK STATEMENT	
HIGH	Risk requires immediate attention. Illicit activity is widespread, and there are many barriers to detecting or disrupting criminal actors. Continued exploitation is highly likely.
MEDIUM	Risk is moderate and requires further assessment. There is evidence of some illicit activity, and there are some barriers to detecting or disrupting criminal actors. Continued exploitation is possible.
LOW	Risk is acceptable but requires monitoring. There is little evidence of illicit activity. An increase in exploitation over the next two years is unlikely.

TERMINOLOGY

In the context of this assessment, the following terms are defined as follows:

- **Threats** refer to people, entities, objects or activities that have the potential to cause proliferation financing risk.
- **Vulnerability** refers to matters that the threat may exploit or may be used in support of, or to facilitate, threats.
- **Consequence** is the potential impact or harm caused by the presence of proliferation financing activities on a national economy and society.

KEY INFORMATION SOURCES

Key information sources used to inform this assessment include:

- AUSTRAC and partner agency intelligence holdings
- suspicious matter reports (SMRs) submitted to AUSTRAC between October 2016 and September 2021
- a comprehensive review of Australia's proliferation financing risk environment completed by RUSI in July 2021
- survey responses from 215 reporting entities across 13 financial sectors (the '**industry survey**')
- consultation with partner agencies in the NIC
- international reporting on proliferation financing trends and investigations, including by the UN Panel of Experts.

INDUSTRY SURVEY

Sanitised results of the industry survey are provided throughout this assessment. They demonstrate industry perceptions of proliferation financing risks in Australia and strategies used to mitigate them. This information may help businesses determine whether their compliance program is calibrated to prevent and detect suspicions of proliferation financing and sanctions evasion.

AUSTRALIA'S COUNTER-PROLIFERATION FINANCING REGIME

Australia has implemented comprehensive sanctions regimes and a complementary AML/CTF framework to combat proliferation financing activity. Australia also maintains a robust legal and operational framework to combat proliferation activities.

Australia is a signatory to a number of multilateral non-proliferation, disarmament and export control treaties and regimes. Since 2003, DFAT has housed the Australian Safeguards and Non-Proliferation Office, which (among other responsibilities) ensures Australia's international obligations are met under the Nuclear Non-Proliferation Treaty and the Chemical Weapons Convention.[10]

Australia has implemented the following legislation to combat WMD proliferation:

- *Chemical Weapons (Prohibition) Act 1994* – implements criminal offences for violations of the 1972 United Nation's Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on their Destruction.
- *Comprehensive Nuclear-Test Ban Treaty Act 1998* – prohibits the causing of any nuclear explosion at any place within Australian jurisdiction or control and establishes a penalty of life imprisonment for an offence against this prohibition.
- *Crimes (Biological Weapons) Act 1976* – implements criminal offences for violations of the 1972 United Nation's Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on their Destruction.

[10] Further details of the work and priorities of the Australian Safeguards and Non-proliferation Office are available here.

- *Customs Act 1901* and (Prohibited Exports) Regulations 1958 – prescribes prohibited exports and is administered by the Australian Border Force.
- *Nuclear Non-Proliferation (Safeguards) Act 1987* – regulates nuclear material in Australia and is administered by the Australian Safeguards and Non-Proliferation Office.
- *Weapons of Mass Destruction (Prevention and Proliferation) Act 1995* – covers exports not controlled under the Customs Act which may contribute to WMD programs and is administered by the Department of Defence.

SANCTIONS REGIMES

Australia has comprehensive sanctions regimes relating to the DPRK, Iran and WMD proliferation. They go beyond UNSC and FATF obligations, and the automatic and immediate implementation of UNSC designations was flagged in Australia's 2015 Mutual Evaluation Report as best practice to follow for other countries.

Under the *Charter of the United Nations Act 1945* and related subsequent legislation, Australia integrates UNSC TFS and activity-based sanctions on the DPRK and Iran into Australian law, including prohibitions on the provision of assets as well as financial services and resources for sanctioned activities. Additionally, Australia imposes sanctions on the DPRK and Iran under its autonomous sanctions framework, including TFS.

Australian sanctions law is administered by the Australian Sanctions Office in DFAT. As the sanctions regulator, the Australian Sanctions Office:

- provides guidance to regulated entities, including government agencies, individuals, business and other organisations on Australian sanctions law
- processes applications for, and issues, sanctions permits
- works with individuals, business and other organisations to promote compliance and help prevent breaches of the law
- works in partnership with other government agencies to monitor compliance with sanctions legislation
- supports corrective and enforcement action by law enforcement agencies in cases of suspected non-compliance.

DPRK'S NUCLEAR WEAPONS AND BALLISTIC MISSILE PROGRAMS

The DPRK's pursuit of WMD and missile delivery systems pose a grave threat to international peace and security and a serious challenge to international non-proliferation efforts.

The regime continues to develop nuclear weapons and ballistic missiles in violation of UNSC resolutions, and the International Atomic Energy Agency (IAEA) assesses that various nuclear facilities in the DPRK remain operational. The UN Panel of Experts continues to identify widespread sanctions evasion, particularly of refined petroleum imports and coal exports, which includes ship-to-ship transfers and direct shipments to and from the DPRK.

AUSTRALIA'S RESPONSE

Australia remains committed to strictly enforcing UNSC and autonomous sanctions against the DPRK until it takes clear steps towards complete, verifiable and irreversible denuclearisation. Since 2018 Australia has also contributed to a multinational force to monitor and deter illegal ship-to-ship transfers of sanctioned goods.

Sanctions measures include restrictions on the export and import or supply of a range of goods and services. It is prohibited to supply all goods, except food[11] and medicine, to the DPRK unless a permit has been granted by the Minister for Foreign Affairs. There are also restrictions on commercial activities, vessels and aircraft, and scientific and technical cooperation in addition to TFS and travel bans.

In July 2021, the New South Wales Supreme Court sentenced an individual to three years and six months imprisonment for a series of sanction offences. This was the first time charges were laid in Australia for alleged breaches of sanctions in relation to the DPRK. Details of this matter are discussed on page 25.

IRAN'S NUCLEAR PROGRAM

Iran's existing nuclear program continues to be a cause for concern, for both Australia and the international community. Since the US withdrawal from the JCPOA (or 'nuclear deal') in May 2018, Iran has taken progressive steps away from compliance with restrictions imposed on its nuclear program by the nuclear deal.

Iran continues to grow its stockpile of enriched uranium, with enrichment levels reaching 60 percent purity – well above the 3.67 percent limit mandated by the JCPOA. This was first reported by the IAEA in April 2021 and has been regularly verified since. Moreover, since February last year, Iran has ceased provisional application of its Additional Protocol – a mechanism providing for enhanced IAEA oversight of its nuclear activities.

AUSTRALIA'S RESPONSE

In 2015, the UNSC adopted Resolution 2231 which endorsed the JCPOA, terminating previous sanctions but imposing measures that restrict certain activities. Australia implements UNSC sanctions and imposes autonomous sanctions in relation to Iran. Australia also calls on Iran to reverse all steps away from the JCPOA and return to full compliance with the nuclear deal, including full implementation of the Additional Protocol and other JCPOA transparency commitments.

Sanctions measures in relation to Iran include restrictions on the export or supply of certain goods, including arms or arms or related materiel, as well as restrictions on certain commercial activities, provision of certain services, providing or dealing with assets of designated persons or entities, and travel bans. The Minister for Foreign Affairs may grant a sanctions permit to allow an activity that would otherwise be prohibited under this regime provided the activity meets specific criteria.

INVESTIGATION AND PROSECUTION OF SANCTIONS BREACHES

The Australian Sanctions Office assesses potential sanctions breaches and refers matters to the Australian Federal Police for further investigation and the Commonwealth Director of Public Prosecutions for prosecution. The Australian Border Force (with guidance from the Australian Sanctions Office as needed) investigates border-related sanctions breaches, including TFS restrictions and trade restrictions, and may apply a range of enforcement options.

Australia has a range of criminal offences for sanctions violations and providing false or misleading information to government authorities in connection to the administration of a sanctions law. In certain circumstances, individuals who are not directly party to a violation but support sanctions

[11] Sanctions prohibitions will apply to food that has been designated as a 'luxury good' under the *Charter of the United Nations (Sanctions – Democratic People's Republic of Korea) (Luxury Goods) Instrument 2017* (Cth) <https://www.legislation.gov.au/Details/F2017L00635>.

evasion (for example, handling financial transactions or providing corporate or legal services) can also be subject to criminal prosecution and penalties.

PRIVATE SECTOR OUTREACH

The Australian Sanctions Office provides a range of resources to help industry understand and meet their sanctions obligations, including:

- enabling users to register and receive email updates on changes to Australian sanctions legislation and listings.
- providing users with access to the PAX Portal, where they can submit general inquiries, apply for sanctions permits and request an indicative assessment of how Australian sanctions law applies to their case.
- hosting a searchable consolidated list of sanctioned individuals and entities.
- providing training and guidance material on Australia's sanctions regimes and relevant regulations, including on the DPRK and Iran. The training goes beyond TFS restrictions to include activity-based prohibitions like bans on the trade of goods and services.

AUSTRAC provides a range of online resources and guidelines on AML/CTF expectations and sanctions compliance – a number of which are relevant to establishing processes to mitigate proliferation financing risks. These include guidance on conducting assessments of ML/TF risks, risk management, due diligence and screening procedures, and sector-specific red flags and ML/TF risk assessments.

In 2021, the Australian Banking Association published good practice guidelines on sanctions implementation. AUSTRAC and the Australian Sanctions Office supported this work.

ANTI-MONEY LAUNDERING AND COUNTER-TERRORISM FINANCING FRAMEWORK

Australia's AML/CTF regime establishes a regulatory framework for combatting ML/TF and other serious crimes. Although the AML/CTF regime does not make specific mention of proliferation financing, many of its provisions are relevant to countering instances of proliferation financing or sanctions evasion.[12]

The AML/CTF legislative regime comprises of:

- the *Anti-Money Laundering and Counter-Terrorism Financing Act* 2006 (AML/CTF Act)
- the *Anti Money Laundering and Counter-Terrorism Financing Rules Instrument 2007 (No. 1)* (AML/CTF Rules)
- the *Anti-Money Laundering and Counter-Terrorism Financing (Prescribed Foreign Countries) Regulations 2018*
- the *Financial Transaction Reports Act 1988* (FTR Act).

[12] The AML/CTF regime applies to residents of Australia as well as Australia-based entities or subsidiaries of Australian companies abroad. The AML/CTF Act requires reporting entities to identify customers' identities; mandates the collection of certain information for electronic funds transfers; places restrictions on correspondent banking relationships; places certain reporting requirements for suspicious activity, transactions past a certain threshold and cross-border movement of funds, physical currency and bearer negotiable instruments; and requires the establishment and compliance of an AML and CTF programme that identifies and addresses institutional risk.

The AML/CTF Act focuses on regulating businesses that provide a range of services (known as designated services).[13] Businesses that provide designated services are known as reporting entities. Reporting entities must comply with obligations under the AML/CTF legislative regime. There are currently more than 17,000 reporting entities enrolled with AUSTRAC.

All reporting entities must have risk-based systems and controls in their transaction monitoring programs to identify and report suspicious matters. This obligation includes monitoring for suspicions that individuals or businesses are attempting to avoid Australia's sanctions laws in connection with the provision of a designated service, or a request to provide a service.

Reporting entities play an important role in Australia's counter-proliferation financing regime. Under the AML/CTF Act, reporting entities have an obligation to report suspicious matters to AUSTRAC. A reporting entity must submit an SMR under a number of circumstances, including if they suspect on reasonable grounds that information they have concerning a service they are providing, or will provide, may be relevant to the investigation or prosecution of a crime.

SMRs provide valuable intelligence to AUSTRAC. Working with its partner agencies, AUSTRAC pieces together intelligence from a range of sources to develop a picture of criminal activities and networks. Many of AUSTRAC's partner agencies have access to SMRs to generate investigative leads and conduct further analysis and investigation. High-quality, accurate and timely SMRs give AUSTRAC and our partners the best chance to detect, deter and disrupt proliferation financing activities and sanctions breaches.

INTER-AGENCY COORDINATION AND INFORMATION-SHARING

The following are the main agencies, authorities and bodies responsible for formulating and implementing Australia's counter-proliferation financing regime:

- **AUSTRAC** is Australia's AML/CTF regulator and financial intelligence unit. AUSTRAC provides specialist financial analysis capabilities to help protect Australia from proliferation actors and sanctions evasion activities.
- The **Australian Border Force (ABF)** monitors and detects the illegal movement of people, goods, and illicit cash across the border. It also administers border controls on United Nations-sanctioned goods to prevent activities that may contribute to the proliferation of WMD.
- The **Australian Federal Police (AFP)** is responsible for investigating serious and complex crime against the federal government (including sanctions offences). The AFP leads the multi-agency Criminal Asset Confiscation Taskforce, which would be involved in any asset seizure or forfeiture relating to designated entities.
- The **Commonwealth Director of Public Prosecutions** prosecutes offences against federal law, which includes sanctions and proliferation financing-related offences.
- The Defence Export Controls (DEC) branch within the **Department of Defence** is Australia's military and dual-use goods and technology export regulator. The DEC issues permits to export, supply, publish or broker military and dual-use goods and technology listed on the Defence and

[13] Designated services are defined in section 6 of the AML/CTF Act and include financial services - including remittance and digital currency exchange – gambling and bullion dealing.

Strategic Goods List;[14] and works to ensure exported items are not used in, or assist, a WMD program.

- The **Department of Foreign Affairs and Trade (DFAT)** leads domestic coordination, cases, and international cooperation in relation to proliferation financing. The Australian Sanctions Office in DFAT is responsible for the administration of Australian sanction laws, consistent with Australia's international obligations and foreign policy objectives. The Australian Sanctions Office works with a range of intelligence partner agencies – including AUSTRAC – to analyse proliferation financing risks associated with activities that violate, or may violate, Australian sanctions laws. The Australian Sanctions Office also works closely with the Department of Defence's Defence Export Controls Branch, which includes technical assessments of goods and technology to be exported.
- The **National Intelligence Community (NIC)** is comprised of ten Commonwealth agencies that have intelligence and operational roles for aspects of counter-proliferation and counter-proliferation financing. The NIC and other agencies have formed operational counter-proliferation financing working groups to share intelligence and coordinate their activities. This provides wide-ranging intelligence collection capabilities as well as a significant toolkit for disrupting proliferation financing threat actors and networks.

A number of law enforcement and Commonwealth agencies, including AUSTRAC, also work closely to support a collaborative, cross-agency effort to protect the safety, security and national interests of Australia. A number of these agencies are directly relevant to countering proliferation financing threats, which include:

- maintaining secure borders (includes preventing smuggling and other criminal cross-border activities)
- disrupting organised crime, including cybercrime, money laundering, and the importation of illicit drugs, tobacco, firearms and weapons
- enhancing the integrity of trade and travel systems. This includes the migration system and the movement of goods and people across Australia's borders through air and sea ports.

INTERNATIONAL COOPERATION AND INFORMATION SHARING

Australia has invested significant effort into establishing mechanisms for international information and intelligence sharing, as well as strengthening regional counter-proliferation financing and related TFS regimes. Many of the NIC agencies have information sharing arrangements with foreign counterparts that enable exchange of proliferation financing intelligence and support coordinated efforts to monitor and disrupt proliferation financing networks and activity.

[14] The Defence and Strategic Goods List was updated and came into effect in August 2021. It can be accessed here: https://www.defence.gov.au/business-industry/export/controls/export-controls/defence-strategic-goods-list.

THREAT ENVIRONMENT

A wide range of direct and indirect threat typologies were examined as part of this assessment.

- A **direct threat** refers to:
    1. financial products and services directly related to procurement of proliferation-sensitive goods[15]
    2. legitimate and illicit revenue-raising activities undertaken by actors of proliferation concern to fund WMD programs
    3. evasion of proliferation financing-related sanctions (including TFS)
    4. the provision of technical training, advice, service, brokering or assistance related to proliferation activities.
- An **indirect threat** refers to financial or corporate infrastructure that can help facilitate proliferation financing activity, but is not necessarily established for that sole purpose.

PROLIFERATION PATHWAYS AND RELATED RISK

State-based or state-linked procurement networks target a range of sectors in Australia to export restricted, sensitive or dual-use goods and knowledge. This can include industries such as aerospace, automotive, information technology, research, higher education, extractive and general manufacturing.

[15] This includes financial products and services associated with trade in goods that are directly usable or modifiable for use in the development of WMDs, their means of delivery and related materials.

The key proliferation financing threats facing Australia relate to financial assistance or related services for direct trade in these goods with, and knowledge transfer to, countries of proliferation concern or entities sanctioned for proliferation activity. This could include trade finance products or the remittance of funds linked to illicit procurement activities as well as the exploitation of individuals who can provide access to restricted or sensitive information or technology. Actors who establish companies onshore to conceal a wider network of proliferation financing-related activity also pose a threat to Australia.

Procurement networks operate on behalf of the DPRK and Iran, as well as other countries of proliferation concern. Activity by non-state actors has also been observed[16] and may pose an increasing threat as new technologies become more available to the public.

Procurement networks use a range of methods to help obscure their illicit activities and evade sanctions. For example:

- using front or shell companies
- mislabelling goods
- sourcing either components or sub-components from a variety of suppliers
- using third-country transhipment locations to hide the ultimate destination
- exporting goods just under control or reporting thresholds.

KEY THREATS

FATF R.1: THREAT RATINGS

RISK	THREAT RATING	VULNERABILITY RATING
Potential breach or non-implementation	●	●
Potential evasion	●	●

AUSTRAC assesses the threat of potential breach or non-implementation of TFS is **low**.

- While this threat may exist, no examples were identified for this assessment. Threats could include complicit actors who do not comply with sanctions laws or financial institutions that do not implement a strong compliance program.
- Risks concerning potential breach or non-implementation of TFS primarily stem from vulnerabilities present in the private sector. These factors are discussed in the '**National proliferation financing vulnerabilities'** section of this report.

AUSTRAC assesses the threat of potential evasion of TFS is **medium**.

- Threat typologies identified in this report have been used in efforts to evade TFS. They do not require extensive knowledge or expertise and are often difficult for financial institutions and authorities to detect.

[16] For example, in 2019, an Australian citizen was jailed for knowingly providing technical advice to Islamic State of Iraq and the Levant on how to develop laser-guided weapons. See R v Zahab - NSW Caselaw for more details.

The most significant proliferation financing threats facing Australia include the:

- use of Australian financial services and infrastructure to procure dual-use goods and evade sanctions
- use of Australia-based corporate structures to facilitate proliferation financing and evade sanctions
- use of Australian or third-country nationals to facilitate proliferation financing and evade sanctions
- exploitation of Australian citizens to source and export sensitive technologies and knowledge for use by actors of proliferation concern
- use of DNFBPs to facilitate proliferation financing and evade sanctions.

USE OF AUSTRALIAN FINANCIAL SERVICES AND INFRASTRUCTURE

Proliferation actors use Australian financial services and infrastructure to secure trade financing and remit payments associated with trade activity related to proliferation financing or activities that breach proliferation-related sanctions. In cases to date, this has almost exclusively involved the use of major domestic and foreign banks.

To a lesser extent, remittance and foreign exchange providers have also been misused. In these cases, Australia-based customers maintain close personal and business relationships with individuals in countries of proliferation concern. This can help obscure the illicit purpose of the transfer. Additionally, some businesses are likely to be targeted due to real or perceived gaps in customer due diligence processes, particularly operators who serve a customer base with close personal or cultural ties.

Proliferation financing actors use a range of methods to disguise their activity including:

- The use of front or shell companies (onshore and offshore) and professional intermediaries to mask parties to transactions and end users.
- Procurement through complicit Australian companies using unwitting third-party Australian suppliers.
- Convoluted financial routes to hide the final destination or ultimate beneficiary, such as transfers to third-countries not of proliferation concern. These typologies also exploit trans-shipment hubs.
- Financial services or transactions that are physically distanced from the actual trade of goods. For example, this could involve an Australian-registered company shipping goods from an offshore operational location, but using onshore financial services to receive payment.

Levels of proliferation financing risk exposure between financial institutions vary significantly, and are largely dependent on the scale of the institution's operations, the type of financial products and services offered and the channels used to deliver those services.

- Smaller banks that do not offer trade finance products or fast and efficient international remittance may not be as attractive to proliferators. However, they could be targeted due to the perception they have weaker due diligence processes, are not aware of their proliferation financing risks and do not have processes in place to identify proliferation financing activity.
- Large financial institutions may be more attractive, especially those with international operations, however their greater capacity to understand and counter-proliferation financing risks could make them a more difficult target. At the same time the greater

volume of financial transactions handled by these banks may make it harder for them to identify proliferation financing-related activity, particularly given the complexity of trade financing arrangements that often involves multiple parties and jurisdictions.

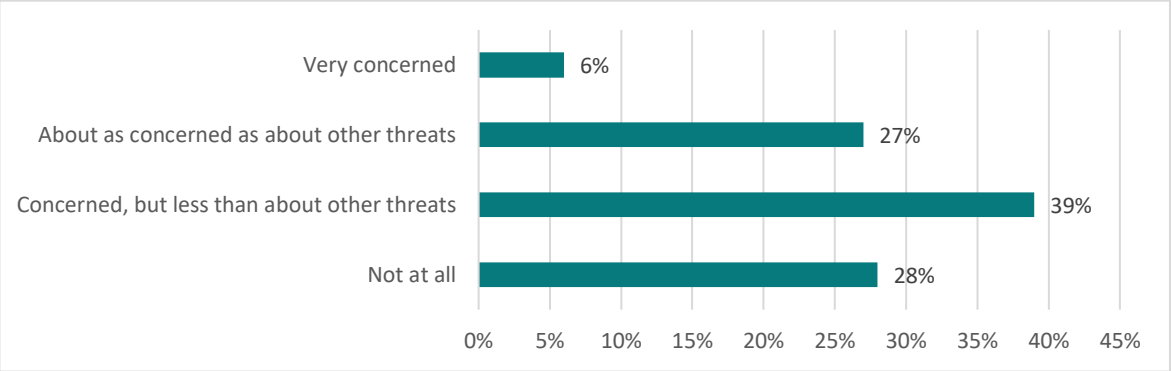
- Other financial service providers such as foreign exchange, remittance services or digital currency exchanges may also be targeted by proliferators to avoid the formal financial system. In addition, some of these providers may be exposed given the ongoing international implementation efforts relating to FATF's Travel Rule[17] for remittance service providers or digital currency exchanges.

Importantly, proliferation financing actors often use methods that mirror money laundering schemes. For this reason, it can be very challenging for reporting entities to distinguish proliferation financing or sanctions evasion from traditional money laundering activity.

Under the AML/CTF Act, reporting entities are not required to implement a separate compliance program specific to proliferation financing. However, all Australian entities are required to comply with Australia's sanctions law. See the '**Sanctions regime**' section for published information and guidance to help businesses mitigate proliferation financing risks and ensure compliance with TFS obligations.

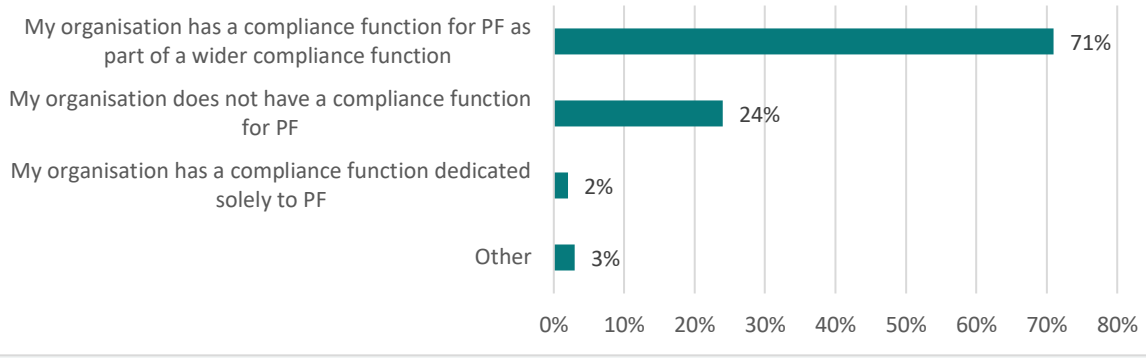
INDUSTRY SURVEY: PERCEPTIONS OF PROLIFERATION FINANCING RISK

How concerned are you about your institution's exposure to and ability to identify counter-proliferation financing and proliferation-related TFS evasion?

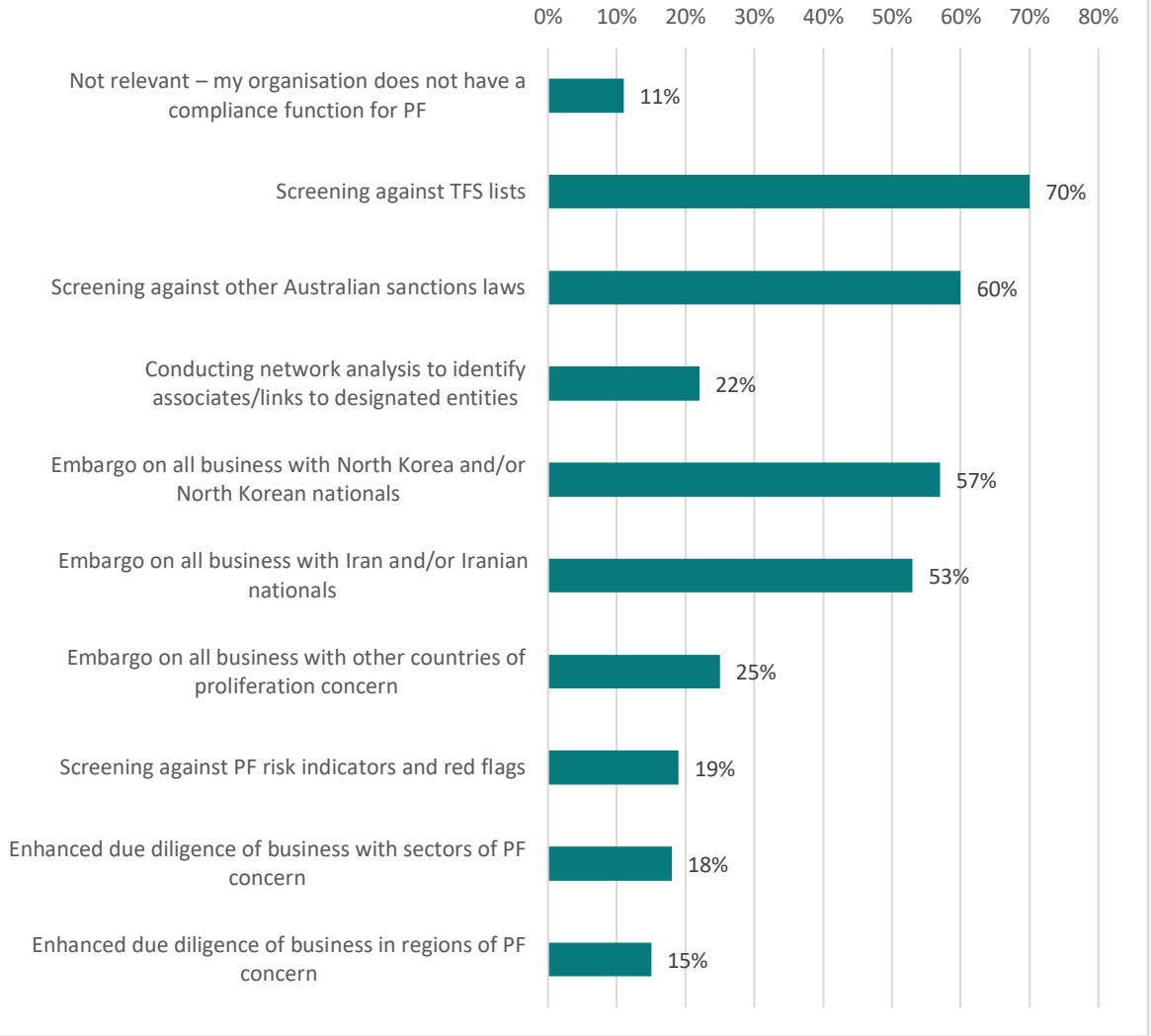


[17] The Travel Rule would require companies to identify all parties involved in transactions (e.g. exchanges between digital currencies), custodial wallet providers and transfers made on behalf of customers.

Does your institution have a proliferation financing compliance function?



What types of activities are undertaken as part of your institution's proliferation financing compliance function?[18]



[18] Please note, respondents could select more than one answer. Responses therefore do not total to 100 percent.

USE OF AUSTRALIA-BASED CORPORATE STRUCTURES

Corporate entities and complex networks are used to directly and indirectly facilitate proliferation financing activity. In some instances they may conduct legitimate business and not solely be used for proliferation financing.

Corporations used for proliferation financing purposes may share directors and management, addresses, emails, phone numbers and financial infrastructure with other entities in their networks. They are often subsidiaries or otherwise affiliated with one of a number of larger corporations in countries of proliferation concern.

These corporate entities may obfuscate their identities and activities by:

- using aliases and transliteration of company names
- using subsidiaries or branches
- using third-country nationals in corporate ownership structures
- registering in jurisdictions with opaque corporate registers where information on ultimate beneficial ownership is not easily accessible.

Australian companies that are not regulated by AUSTRAC have also been suspected of remitting funds for proliferation financing networks, and have engaged in joint ventures with DPRK and Iranian-linked companies to either generate revenue or import goods in contravention of sanctions.

CASE STUDY ONE

On 23 July 2021 the New South Wales Supreme Court sentenced a South Korean-born Australian citizen to a term of three years and six months imprisonment for contravening Australian sanctions law relating to the DPRK. The individual used offshore bank accounts and a series of Australia-based front companies to broker trade with the DPRK in a variety of goods, including coal, graphite, copper ore, gold, crude oil (including purchasing Iranian petrol on behalf of the DPRK), missiles and missile-related technology. This was the first time charges were laid in Australia for breaches of sanctions in relation to the DPRK.

CASE STUDY TWO

In 2019, a New South Wales-based couple was convicted and sentenced for contravening Australian sanctions law relating to Iran. The sanctions breaches occurred in 2009 and 2010 and involved the procurement and supply of approximately 90 tonnes of export-sanctioned nickel alloys to Iran. The couple established and used a joint business venture to procure the production of the nickel alloy from a company based in the United Kingdom (UK). Once produced, the nickel alloy was shipped from the UK to an Iranian-owned Dubai-based company, then forwarded to Bandar Abbas, Iran.

While the evidence suggested the nickel was likely not used for illegitimate purposes in this case, this example demonstrates how joint ventures can help mask sanctions evasion activity by physically distancing the supply and movement of goods from Australian corporate and financial structures.

CASE STUDY THREE

In 2017, an Australian-registered property company and its director, a Chinese national, were reportedly involved in the smuggling of DPRK coal. The coal was carried on-board a Panamanian-flagged vessel and destined for Vietnam. The individual mislabelled the coal as originating from Russia. The company and the director were investigated by the Australian Government.

USE OF THIRD-COUNTRY NATIONALS

Proliferators often rely on nationals of third countries for much the same reason as they rely on front companies and complex corporate structures. This is to obfuscate the connection between designated individuals or entities and sanctioned activities. This is particularly true of the DPRK, which has been known to use nationals of other Asian countries, especially China. Australia's close economic relations with Asian countries may create some vulnerability in this context.

See the '**Extensive economic relations and trade with Asian markets' section** for more detail.

TARGETING AUSTRALIAN CITIZENS TO SOURCE AND EXPORT SENSITIVE TECHNOLOGIES

Australian citizens have been used – both wittingly and unwittingly – to source and export critical and sensitive technologies to actors of proliferation concern. A key method involves targeting individuals with access to sensitive information, business connections or specialist knowledge that could benefit a WMD program. This includes professionals working in a range of desired dual-use goods sectors, Australia's import-export sector, as well as individuals working in higher education and research.

In some instances, Australian individuals have received multiple cash deposits into their bank account. While there is no visible link to proliferation financing activity, these suspicious cash deposits could indicate links to other criminal activity by persons of proliferation financing interest (notably money laundering), or deliberate attempts by proliferation financing networks to avoid remitting funds through banks or remittance channels.

In its latest threat assessment, the Australian Security Intelligence Organisation (ASIO) assessed that espionage and foreign interference have now supplanted terrorism as Australia's principal security concern. Of particular relevance to proliferation financing, foreign spies are targeting Australia's defence industry.[19]

USE OF DESIGNATED NON-FINANCIAL BUSINESSES AND PROFESSIONS

Proliferation actors exploit DNFBPs in much the same way as money launderers. In Australia, this has primarily involved the use of DNFBPs to establish complex corporate structures - including shell and front companies - and related banking arrangements to evade sanctions and generate revenue for proliferation activities. While the extent of criminal exploitation for these purposes is likely low, certain types of DNFBPs will remain particularly exposed, namely lawyers, accountants and trust and company service providers.[20]

CASE STUDY FOUR

A Hong Kong-based accounting firm known for specialising in offshore company registration and providing secretarial services is believed to have helped an Australian resident establish front and shell companies (Company X and Company Y) for the purpose of facilitating high-risk financial transactions to beneficiaries in Russia, including to an entity subject to US financial sanctions.

[19] ASIO, Director-General's Annual Threat Assessment, 9 February 2022, <https://www.asio.gov.au/publications/speeches-and-statements/director-generals-annual-threat-assessment-2022.html>, accessed 7 October 2022.

[20] AUSTRAC acknowledges the establishment of a corporate structure by a DNFBP is a lawful activity and may be established for an intended legitimate purpose. The future misuse of the corporate structure is likely unknown to the DNFBP, unless an ongoing business relationship is maintained.

- In 2018, a foreign bank submitted an SMR to AUSTRAC regarding Company X. The report noted Company X had a declared principal place of business in the Dalian province in China (near the border of the DPRK and considered a high-risk region for sanctions evasion and proliferation financing activity). Company X received a number of incoming transfers from shipping companies located in Hong Kong and China, and then attempted to remit these funds to an unknown beneficiary in Vladivostok, Russia.
- In 2018, another major bank submitted an SMR regarding Company Y, which was an Australian-registered company with limited public details available. The report noted Company Y attempted to remit funds to a US-sanctioned beneficiary in Russia.

NATIONAL PROLIFERATION FINANCING VULNERABILITIES

FATF R.1: VULNERABILITY RATINGS

RISK	THREAT RATING	VULNERABILITY RATING
Potential breach or non-implementation	●	●
Potential evasion	●	●

AUSTRAC assesses that Australia's vulnerability to potential breach or non-implementation of TFS is **low**.

- Findings from the industry survey indicate a high understanding of and compliance with TFS obligations relating to the DPRK and Iran, particularly among the most at-risk reporting entities (e.g. those processing high volumes of international transactions or offering trade finance products).
- Australia implements a robust sanctions regime, which includes private sector outreach and support for industry to understand and meet their TFS obligations by both the Australian Sanctions Office and AUSTRAC.

AUSTRAC assesses that Australia's vulnerability to potential evasion of TFS is **medium**.

- All vulnerabilities identified in this report can be exploited or misused to facilitate or enable TFS evasion. They can also complicate the detection of suspicious activity by financial institutions or investigation efforts by authorities.

Key national vulnerabilities were identified across the following categories:

- Economic and trade factors.
- Legislative and regulatory factors.
- Industry and technology factors.

ECONOMIC AND TRADE FACTORS

EXTENSIVE ECONOMIC RELATIONS AND TRADE WITH ASIAN MARKETS

The prevalence of Asian countries among Australia's key export destinations creates an inherent proliferation financing vulnerability. Established trade and financial networks and relationships may lend themselves – wittingly or otherwise – to sanctions evasion or proliferation financing activity.

Asia has historically been a popular destination for sanctioned trade with DPRK. The DPRK has been known to route sanctioned goods and proliferation financing-related financial transactions through third countries as a way of obfuscating their connection to the country, designated entities and sanctioned activities. The combination of geographic proximity, gaps in sanctions compliance and regimes to fight financial crime, and in some instances political sympathies and cultural ties, makes parts of Asia particularly vulnerable to proliferation financing activity by the DPRK.

Australia's free trade arrangements with the Association of Southeast Asian Nations (ASEAN) and a number of bilateral agreements in the region may add to this vulnerability by streamlining the flow of goods and finances between Australia and the region. Illicit trade and financial flows may be mixed with legitimate activity, making it difficult to identify instances of sanctions evasion through third countries. Some goods – namely petroleum and coal – may also be transferred in illicit ship-to-ship transfers at sea, with parts of the Yellow Sea and East China Sea being particularly popular locations for such transfers.

TRADE VOLUMES WITH ASIA[21]

In 2019, Australia exported USD $237 billion to Asia and imported USD $123 billion from the region. A number of exports are subject to proliferation and proliferation financing-related restrictions under UNSC sanctions. China was Australia's biggest trading partner in 2019, accounting for USD $111 billion in exports and USD $57.2 billion in imports.

HIGH VOLUME OF DUAL-USE AND PROLIFERATION-SENSITIVE EXPORTS

The diversion of dual-use and proliferation-sensitive goods and expertise to countries of proliferation concern or entities sanctioned in relation to proliferation activity – and more specifically financial services in support of these activities – is a key proliferation financing vulnerability for Australia. This includes exports from the extractives sector and automotive, aerospace and technology industries.

In 2019, Australia exported:

- USD $3.53 billion in transportation products and components (including aircraft, spacecraft, ship and automotive components)

[21] Observatory of Economic Complexity, 'Australia', <https://oec.world/en/profile/country/aus>, accessed 20 April 2022. Please note figures for 2019 are used in this report. This is because more recent figures have been impacted by the COVID-19 pandemic and associated shutdown measures globally, and are not likely a true reflection of expected trade volumes moving forward.

- USD $130 million in weapons parts and accessories
- USD $7.79 billion in machines (a broad category that includes items such as gas turbines, liquid pumps and centrifuges[22] – all of which may be employed in a WMD programme if of certain specification).

Asian countries were the primary destination for these exports. Proliferation financing vulnerability associated with these markets is discussed in the previous section.

Australia also has a sophisticated defence sector, including a program of research and development. In 2019, Australia exported USD $130 million in weapons and related parts. When looking only at weapons parts and accessories, Australia made up 4.72 percent of global exports, trailing only the United States, South Korea and Italy.[23] As noted in the '**Threat environment**' section, Australia's defence sector is actively targeted by foreign espionage and interference actors. While the nature of contact may not be explicitly tied to foreign proliferation efforts, this espionage and interference threat increases the sector's vulnerability to possible diversion activities.

MITIGATING PROLIFERATION FINANCING VULNERABILITY

All exports are subject to routine assessment by the Australian Border Force, which must ensure all export requirements have been met prior to releasing the cargo for export. This is to ensure the export will not breach export control legislation. The Australian Border Force works closely with a range of other government agencies, including DEC within the Department of Defence and DFAT to administer a series of controls on the export of dual-use and defence goods and other goods of security concern. Under Australian export control laws it is a serious criminal offence to export goods subject to permit requirements without the necessary authorisations.

Financial institutions play a key role in helping to mitigate the risk of diversion of dual-use and proliferation-sensitive goods and expertise. Institutions involved in the financing of trade in such goods should ensure they screen against a list of dual-use or proliferation-sensitive goods as part of their compliance activities.[24]

A GLOBALLY SIGNIFICANT MINING INDUSTRY

Australia's globally significant mining industry creates a considerable proliferation financing vulnerability. As of January 2022, Australia was operating over 350 mines across the country. Australia is a leading global exporter of zinc ore, iron ore, precious metal ore, aluminium ore, gold, copper ore, raw aluminium, as well as natural uranium, uranium ores and concentrates.[25]

Australia also hosts a number of busy ports, including the world's largest iron ore loading port in Port Hedland, Western Australia. The sheer volume of exports alone makes Australia vulnerable to the diversion of resources by actors of proliferation concern, particularly in metals and other goods that are prohibited for export to the DPRK. The extensive trading and economic activity with Asian markets,

[22] Ibid.

[23] The Observatory of Economic Complexity, 'Weapons parts and accessories', <https://oec.world/en/profile/hs92/weapons-parts-and-accessories>, accessed 28 June 2021. Please note figures for 2019 are used in this report. This is because more recent figures have been impacted by the COVID-19 pandemic and associated shutdown measures globally, and are not likely a true reflection of expected trade volumes moving forward.

[24] Australia's Defence and Strategic Goods List can be accessed at https://www.defence.gov.au/business-industry/export/controls/export-controls/defence-strategic-goods-list.

[25] The Observatory of Economic Complexity, various publications available on their website.

outlined earlier, provides opportunities for proliferation-sensitive exports to be transhipped through third countries to arrive ultimately in the DPRK.

Under UNSC sanctions, export of metals to the DPRK is prohibited, so the financing of such trade with the country would risk violating UNSC proliferation financing sanctions. Iran is banned from entering into any commercial agreements involving the mining of uranium, or the 'production or use of nuclear materials and technology.' Export of proliferation-sensitive materials, technology and expertise to Iran and the DPRK is also prohibited.

Australian mining expertise and technology and some of the materials it produces may also be of interest to other proliferation actors, either for their value (in the case of gold or other precious metals) or for their application in industry, including for military or WMD purposes (in the case of aluminium, iron or uranium). Involvement in prohibited commercial activities or trade within the mining sector may therefore constitute proliferation financing and may involve sanctioned entities, or those acting on their behalf.

The DPRK also has extensive experience in mining and has been known to offer mining services to other countries in the past. Such services may be offered abroad to generate revenue for the DPRK regime. Australian mining companies may seek to enter into joint ventures with DPRK or Iranian mining companies and offer technical expertise and revenue generating opportunities to these countries, which may violate UNSC proliferation-related sanctions.[26]

In addition, China is among the top global importers of a number of metals which are banned for export to the DPRK. Trade with China is not on its own a risk indicator. However, China is a conduit for sanctioned and smuggled goods into and out of the DPRK.

PROLIFERATION FINANCING VULNERABILITY ASSOCIATED WITH AUSTRALIA'S PETROLEUM TRADE

Similar considerations around proliferation financing vulnerability can be applied to Australian exports of petroleum. While not a top global exporter, Australia exports crude and refined petroleum, largely to Asia. Petroleum imports into the DPRK are capped and Pyongyang often relies on illicit imports of petroleum – as well as ship-to-ship transfers – in violation of UNSC sanctions. Providing financial services in support of such activity, or to entities that engage in such activity, would be in violation of UNSC sanctions and may be considered proliferation financing.

MITIGATING PROLIFERATION FINANCING RISK ASSOCIATED WITH AUSTRALIAN EXPORTS

All goods being exported from Australia must be reported to the Australian Border Force using an Export Declaration. An Export Declaration is a statement made by the exporter, owner of the goods, or their agent. The statement provides information about the goods and the export transaction, including transhipment ports and final destination of the goods, which are used by border authorities to conduct a risk assessment of the export. Providing false and misleading information in the declaration is a serious criminal offence.

Since 2018, Australia has worked alongside international partners and deployed military assets to monitor and deter the shipment of illegal goods to and from the DPRK. Australia also makes diplomatic representations to the flag states of vessels observed engaging in

[26] DPRK companies are not permitted under UNSC sanctions from entering into any joint ventures with foreign companies and Iran is expressly prohibited from acquiring a commercial interest in commercial activity related to uranium mining.

suspicious activity, and provides the information to the United Nations Panel of Experts for investigation.

LEGISLATIVE AND REGULATORY FACTORS

GAPS IN AML/CTF REGULATION OF KEY DNFBPs

Certain types of services provided by DNFBPs are not regulated by AUSTRAC – notably those provided by 'gatekeeper' professions such as lawyers, accountants and trust and company service providers, as well as real estate agents and other high-value goods dealers.[27] While all Australian entities are subject to Australian sanction laws, many DNFBPs are not subject to the due diligence, transaction reporting and supervision requirements outlined in the AML/CTF Act. These AML/CTF requirements help reinforce Australia's counter-proliferation financing regime.

Given the role of gatekeeper-type DNFBPs in facilitating proliferation financing and sanctions evasion (either wittingly or unwittingly), this regulatory gap creates a vulnerability for Australia. For example, one of the key threats identified in this report is the use of complex corporate structures to obfuscate proliferation financing activity. Such networks often rely on legal professionals and corporate service providers for their establishment and operation.

Outreach activity and guidance provided by the Australian Sanctions Office partly mitigates this vulnerability. However, the limited direct sanctions compliance supervision and absence of AML/CTF controls on these DNFBP sectors leaves a vulnerability that can be exploited.

In January 2022, RUSI published the report North Korean Proliferation Financing and Designated Non-Financial Businesses and Professions which examined the role of DNFBPs in DPRK proliferation financing and sanctions evasion activity. The report found that the DPRK has become increasingly skilled at evading TFS and has often exploited or used DNFBPs to do so. The report highlights a range of vulnerable sectors including real estate and dealers in high-value goods and precious metals and stones, as well as exploitation by various gatekeeper professions. Importantly, the report notes the full extent to which DNFBPs facilitate proliferation financing is almost certainly understated, and highlights the need for further research and understanding.

POOR TRANSPARENCY OF LEGAL PERSONS AND LEGAL ARRANGEMENTS

There are opportunities for proliferation actors to create opaque business structures in Australia to help conceal their illicit activity. This vulnerability is of particular concern as the use of Australian companies and financial infrastructure to evade sanctions is a key proliferation financing threat.

Factors that make it easier to create opaque business structures in Australia include:

- There is no requirement to provide ultimate beneficial ownership information for corporate registration, with nominees permitted to register as company directors and non-beneficial shareholders.
- The absence of state- or federal-level transparency mechanisms related to trusts.

[27] A notable exception relates to solicitors who must report cash transactions of $10,000 or more – or the foreign currency equivalent – to AUSTRAC under the FTR Act.

The inability to access public and timely information on the ultimate beneficial owners of corporate entities, assets and financial infrastructure creates a significant proliferation financing vulnerability for Australian authorities and industry. It can prevent financial institutions and other businesses from verifying whether they are engaging with sanctioned entities or entities for whom a certain activity or trade in a certain good is prohibited under proliferation financing-related sanctions.

The use of intermediaries to establish or operate corporate and financial infrastructure makes it more difficult to identify ultimate beneficial ownership and connections to sanctioned entities. The use of trusts, powers of attorney or third-party authorities increases the potential for anonymity and increases proliferation financing and broader sanctions evasion risk. The lack of obligations for DNFBPs such as lawyers and accountants to undertake due diligence on their clients or monitor for suspicious activities further exacerbates this risk.

INDUSTRY SURVEY: ACCESSING ULTIMATE BENEFICIAL OWNERSHIP AND OTHER CORPORATE INFORMATION

Nineteen percent of respondents said their institution is not able to access sufficient ultimate beneficial ownership and other corporate information on their customers or the entities they do business with to effectively assess potential exposure to sanctioned entities or other illicit activity.

IMPROVING AUSTRALIA'S CORPORATE REGISTRATION SYSTEM

Australia is currently progressing the Modernising Business Registers program, which will bring together more than 30 ASIC registers and the Australian Business Register, into one place. The program has already established the Australian Business Registry Services (ABRS) and introduced the Director Identification Numbers regime which will verify the identity of company directors and the relationships they have with Australian companies.

INDUSTRY AND TECHNOLOGY FACTORS

AWARENESS LEVELS OF PROLIFERATION FINANCING RISK EXPOSURE AND INDICATORS

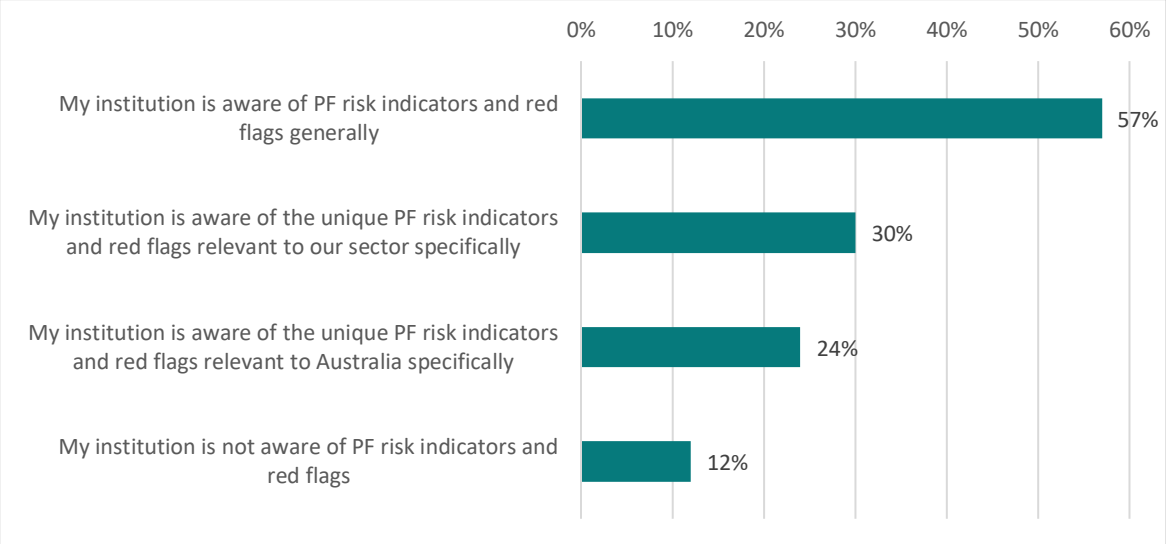
Various government agencies conduct outreach and provide resources to help businesses understand and meet their sanctions obligations. However, responses to the industry survey indicate there is limited awareness of broader proliferation financing risk exposure and the indicators of illicit activity in some industries, primarily among some small to medium-sized businesses.

This vulnerability may be partly mitigated by the fact that some of these entities are less likely to be exposed to broader proliferation financing threats. This could be for several reasons, including the fact they do not offer certain products and services such as trade finance or international remittance. However, these entities may be targeted for real or perceived weaknesses in their AML/CTF or counter-proliferation financing measures.

Current government outreach, resources and training on proliferation financing focuses primarily on sanctions obligations for the DPRK and Iran. This can create the perception that screening against TFS lists or simply foregoing business with the DPRK and Iran are sufficient to mitigate proliferation financing risks. As proliferation actors engage in a wide range of finance activities – many of which may appear legitimate – engagement, resources and training on broader proliferation financing threats will help industry harden itself against misuse.

INDUSTRY SURVEY: UNDERSTANDING PROLIFERATION FINANCING RISK EXPOSURE AND INDICATORS

What is your institution's level of awareness of proliferation financing risk indicators and red flags?[28]



The Australian government provides resources to help businesses mitigate proliferation financing risks and ensure compliance with sanctions obligations. These are noted in the '**Sanctions regime**' section.

[28] Please note, respondents could select more than one answer. Responses therefore do not total to 100 percent.

POTENTIAL CYBERATTACK AND MISUSE OF DIGITAL CURRENCY EXCHANGES

Australia is home to a large financial services sector and a number of digital currency exchanges, which may be vulnerable to attack or misuse by proliferators. Difficulty identifying the source of cyberattacks, the anonymity afforded by some digital currencies, and extensive reliance on technology makes this an attractive method of sanctions evasion and revenue-raising to proliferation actors.

INDUSTRY SURVEY: CYBER SECURITY MEASURES

Most respondents do not consider cybercrime as a key proliferation financing risk. However, responses on the maturity, capacity and resources invested in their institution's cyber security measures varied widely. Organisations with poor cyber security measures are vulnerable to proliferation financing, including potential breach, non-implementation and evasion of TFS.

AUSTRAC encourages all reporting entities to visit the Australian Cyber Security Centre's website for examples of strategies to mitigate cyber security incidents.

Although no known links to Australia were identified in research for this assessment:

- The DPRK is responsible for a range of malicious cyber activities, including against financial institutions and digital currency exchanges in our region.[29] The United Nations Panel of Experts has highlighted these activities as an important source of revenue for the DPRK's WMD program.
- Iranian entities have also carried out cyberattacks against financial institutions, however it is not clear whether these attacks resulted in financial gain for the hackers or facilitated financial sanctions evasion. Recently, the Iranian government has been considering developing a central bank for digital currency, which could potentially be used to evade US sanctions.

Financial institutions and digital currency exchanges can mitigate vulnerability to proliferation financing with adequate cybersecurity measures, being aware of their proliferation financing risk exposure and having measures in place to address their risk.

In Australia, digital currency exchange providers must register with AUSTRAC. This means providers must comply with AML/CTF obligations including identifying their customers, maintaining records and reporting transactions including suspicious matters to AUSTRAC. This obligation applies only to the exchange of digital currency to fiat currency and the reverse.

Australia has not yet implemented FATF's 'Travel Rule' for digital currency exchanges. The Travel Rule would require businesses to identify all parties involved in transactions (for example, exchanges between digital currencies), custodial wallet providers and transfers made on behalf of customers. These obligations would provide greater visibility of ultimate beneficial ownership of digital currency assets, as well as parties to transactions.

AUSTRAC provides guidance to digital currency exchange providers on assessing their risk exposure and complying with their AML/CTF obligations. Regulation and guidance can help mitigate proliferation financing risk exposure, to the extent that AML/CTF measures help protect businesses from a range of criminal misuse, including proliferation financing.

[29] This has included cyberattacks on financial institutions, ransomware attacks, crypto-jacking and hacking of digital currency exchanges.

RESPONDING TO MALICIOUS CYBER ACTIVITY

The Government works hard to protect Australians from a range of cyber threats. This includes collaborating with international partners to monitor and respond to malicious activity, including sharing intelligence and identifying disruption opportunities.

Public attribution is another tool. Since 2017, Australia has worked with international partners to attribute malicious cyber activity on eight occasions. One of these was the 'WannaCry' ransomware campaign which was attributed to the DPRK.

The Australian Government also works with ASEAN and Pacific countries to strengthen cyber resilience, including through DFAT's Cyber Cooperation Program.

APPENDIX A: GLOSSARY

NAME	DESCRIPTION
Actors of proliferation concern	States or entities that should be subject to interdiction activities because they are or are believed to be engaged in: • efforts to develop or acquire WMD (see below) or their delivery systems • trafficking (either selling, receiving, or facilitating) of WMD, their delivery systems, or related materials. The assessment focuses largely on the DPRK and Iran but also considers other countries of diversion risk.
Counter-proliferation financing	Appropriate and effective laws and measures which prohibit and prevent proliferation financing.
Proliferation financing[30]	Proliferation financing is when a person: a. makes available an asset; or

[30] This definition is taken from the Royal United Services Institute's (RUSI) Model Law on Proliferation Financing (RUSI, Guide to Conducting a National Proliferation Financing Risk Assessment, 2019).

	b. provides a financial service; or c. conducts a financial transaction; and the person [knows that, or is reckless as to whether,] the asset, financial service or financial transaction is intended to, in whole or in part, facilitate the proliferation of WMDs, regardless of whether the activity occurs or is attempted. Specified activities that comprise WMD proliferation are defined below.
Weapons of mass destruction	WMD refers to nuclear, biological or chemical weapons or missiles capable of delivering such weapons, and includes delivery systems, components, related technology and expertise.
WMD proliferation[31]	The specified activities that comprise WMD proliferation include: a. the manufacture, production, possession, acquisition, stockpiling, storage, development, transportation, sale, supply, transfer, export, transhipment or use of: i. nuclear weapons; or ii. chemical weapons; or iii. biological weapons; or iv. materials related to nuclear weapons, chemical weapons or biological weapons that are prescribed by Regulations; or b. the provision of technical training, advice, service, brokering or assistance related to any of the activities in Paragraph (a).
RISK TERMINOLOGY	
Threat	Threats refer to people, entities, objects or activities that have the potential to cause proliferation financing risk.
Vulnerability	Vulnerability refers to matters that the threat may exploit or may be used in support of, or to facilitate, threats.
Consequence	Consequence is the potential impact or harm caused by the presence of proliferation financing activities on a national economy and society.

[31] This definition is taken from the Royal United Services Institute's (RUSI) Model Law on Proliferation Financing (RUSI, Guide to Conducting a National Proliferation Financing Risk Assessment, 2019).

AUSTRAC.GOV.AU