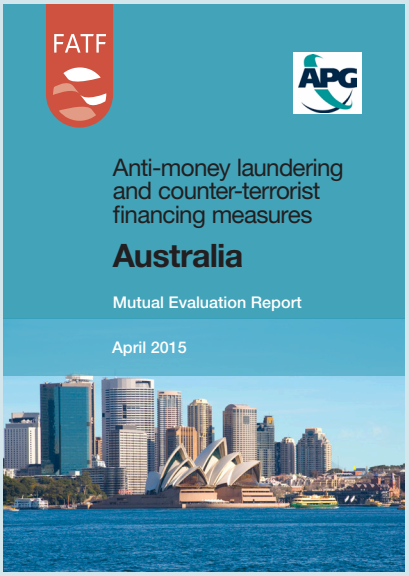
Anti-money laundering and counter-terrorist financing measures - Australia



4. Terrorist financing and financing of proliferation

Effectiveness and technical compliance

Citing reference:

FATF and APG (2015), "Terrorist financing and financing of proliferation" in *Anti-money laundering and counter-terrorist financing measures - Australia,* Fourth Round Mutual Evaluation Report, FATF, Paris and APG, Sydney
www.fatf-gafi.org/topics/mutualevaluations/documents/mer-australia-2015.html

For more information about the FATF, please visit the website: **www.fatf-gafi.org**

4. TERRORIST FINANCING AND FINANCING OF PROLIFERATION

Key Findings

Australia has undertaken several TF investigations and prosecutions and secured three convictions for the TF offence. Australia also successfully uses other criminal justice and administrative measures to disrupt terrorist and TF activities when a prosecution for TF is not practicable. Australia has successfully disrupted two domestic terrorist plots at the time of the on-site visit.[1] Australia also uses these other measures to address the most relevant emerging TF risk – individuals travelling to conflict zones to participate in, or advocate, terrorist activity. Australian authorities identify and investigate different types of TF in each counter-terrorism investigation, and counter-terrorism strategies have successfully enabled Australia to identify and designate terrorists, terrorist organisations, and terrorist support networks. On the other hand, **Australian authorities have not prosecuted all the different types of TF offences, such as the collection of funds for TF, or the financing of terrorist acts or individual terrorists, and the dissuasiveness of sanctions for TF has not been clearly demonstrated**.

Australia demonstrates a number of characteristics of an effective system for targeted financial sanctions (TFS) both for TF and PF. A key area of demonstrative effectiveness is in the direct implementation of TFS against persons and entities designated by the UNSC and under Australia's autonomous sanctions regimes. Australia has also domestically listed individuals and entities pursuant to UNSCR 1373 and received, considered, and given effect to third party requests. Australia's legal system and processes for implementing targeted financial sanction provisions related to UNSCRs represent a best practice for other countries, especially the direct legal obligation regarding UN designations.

However, the effectiveness of the overall framework for targeted financial sanctions both for TF and PF is heavily impacted by the lack of financial supervision of the financial and DNFBP sectors, to ensure compliance with the domestic framework. Due to the lack of financial supervision or monitoring, the lack of practical examples of implementation issues from the financial sector, and the lack of frozen assets, assessors were unable to establish that the framework is effectively implemented by the financial sector and DNFBPs. A related shortcoming is that AUSTRAC and ASIC do not check their own databases for designated entities.

NPOs are an area for improved efforts and additional action. According to the NRA, charities and NPOs are a key channel used to raise funds for TF in or from Australia. However, the lack of a comprehensive sectorial risk assessment (as required by R8), the lack of subsequent outreach in relation to TF to the sector, and the lack of adequate preventive requirements or a supervisory framework that cover all relevant NPOs, leave them vulnerable to misuse by terrorist organisations.

1 Another plot was disrupted soon after the on-site visit.

4.1 Background and Context

Terrorist financing (criminal justice measures)

4.1. Terrorist and terrorist financing offences are contained in sections 103.1 (financing of terrorist acts), 102.6 (financing of a terrorist organisation) and 103.2 (financing of an individual terrorist) (all Criminal Code).

Targeted financial sanctions for terrorist financing and proliferation financing

4.2. Targeted financial sanctions for terrorist financing and proliferation financing are contained in the Charter of the United Nations Act 1945 (CotUNA) and its implementing regulations. The programmes are administered by DFAT, in coordination with other relevant agencies.

Not for profit organisations

4.3. Australia has a general charity regulator, but its focus is on voluntary registration (mainly for tax purposes) and not on TF. About 40 000 of the estimated 140 000 NPOs with legal personality, and 20 000 without legal personality, have registered. No TF-related risk assessment has been conducted, no TF-related monitoring and limited TFS-related outreach has taken place.

4.2 Technical Compliance (R.5-8)

4.4. See for the full narrative the technical compliance annex:

- **Recommendation 5 (terrorist financing offence) is rated largely compliant.**
- **Recommendation 6 (targeted financial sanctions related to terrorism and terrorist financing) is rated compliant.**
- **Recommendation 7 (targeted financial sanctions related to proliferation) is rated compliant.**
- **Recommendation 8 (non-profit organisations) is rated non-compliant.**

4.3 Effectiveness: Immediate Outcome 9 (TF investigation and prosecution)

Prosecution/conviction for TF activity consistent with Australia's risk profile

4.5. Australian authorities demonstrated a generally broad understanding of TF risk (see IO1 above). Risks are largely influenced by international tensions and conflicts, particularly Iraq and Syria. The main domestic risks involve small-scale collection and use of legitimate and illegitimate funds by domestic cells aligned with, or sympathetic to, radicalised Islamic jihadist groups abroad, for the purposes of committing domestic terrorist acts. The most significant emerging risk is the potential for groups as well as other individuals to send money, directly or indirectly, or raise money for, or otherwise support Australians travelling to conflict zones abroad (especially Syria and Iraq) to support foreign terrorist groups and terrorist acts. An on-going risk relates to how these foreign factors continue to pose risks for terrorist activities within Australia.

4.6. Prosecutions are handled by the Commonwealth Director of Public Prosecutions (CDPP), following referral from an investigative agency. The CDPP has designated combat terrorism (CT) prosecutors in each office, and dedicated CT branches in the Sydney, Melbourne, and Canberra Offices to assess briefs of evidence alleging terrorism related offences and to prepare and carry on matters for prosecution. The CDPP designated CT prosecutors in each of its other offices (Brisbane, Perth, Adelaide, Hobart, and Darwin).

4.7. The CDPP also briefs external counsel to provide advice in CT prosecutions, including provision of qualified advice during the investigation stage, and to conduct prosecutions. The CDPP works closely with the AFP to bring the strongest case possible. Cooperation involves the provision of legal advice, the provision of training to AFP CT investigators as required, and joint scenario-based exercises with AFP investigators.

4.8. **Australian authorities have not prosecuted all different types of TF offences**. Australia has prosecuted nine individuals for TF and convicted three. All nine of these prosecutions were for section 102.6(1) CC —making funds available to a terrorist organisation.

4.9. Authorities have prosecuted 41 individuals under Australia's counter-terrorism framework. Twenty-three have been convicted of terrorism offences under the Criminal Code (such as conspiracy to commit or preparation of a terrorist act, or membership of a terrorist organisation); three have been convicted of making an asset available to a proscribed entity under the CotUNA, one has been convicted of an offence under the *Crimes (Internationally Protected Persons) Act 1976*, and one has been convicted under the *Crimes (Foreign Incursions and Recruitment) Act 1978.*

4.10. Most of these terrorism prosecutions have resulted from three counter-terrorism investigations. *Operation Pendennis* (which included TF charges) and *Operation Neath* both involved domestic, "home-grown" cells, sympathetic to radicalised terrorist groups, which aimed to commit terrorist acts on Australian soil in response to Australia's involvement in counter-terrorism efforts abroad. Operation Halophyte involved domestic individuals sending funds to support a foreign terrorist organisation (Liberation Tigers of Tamil Eelam (LTTE)). The cases can be summarised as follows:

- *Operation Pendennis* (2005-2009): involved the prosecution of 13 individuals based in Melbourne, and 9 based in Sydney. The Melbourne cases included charges against six individuals for TF (section 106(1) of the CC—attempting to intentionally make funds available to a terrorist organisation), which resulted in three convictions, as well as convictions for other terrorist offences. The specific terrorist acts the group aimed to commit were not identified. The funding involved was raised from legitimate and illegitimate sources (mainly theft and fraud). Three of the defendants charged with TF were acquitted.

- *Operation Neath* (2009-2010): involved the prosecution of five individuals for terrorism charges, and conviction of three, who plotted to attack the Holsworthy Army barracks. TF charges were not laid in this case.

- *Operation Halophyte* (2007-2009): involved the prosecution of three individuals who were alleged members of, and provided support and/or funds to, LTTE. Charges included section 106(1) of the CC—attempting to intentionally make funds available to a terrorist organisation, i.e. LTTE. These charges were later dropped, given the difficulty to gain evidence relevant to their defence from northern Sri Lanka. However, the individuals were convicted of other terrorist-related offences (i.e., making an asset available to a proscribed entity under Australia's targeted financial sanctions regime).

4.11. As noted above, **the Pendennis case involved convictions for the provision of funds to be used by a terrorist organisation—authorities have not prosecuted other types of TF offences (i.e., collection of funds for TF, the financing of terrorist acts or individual terrorists).**

4.12. Prosecutors have identified potential difficulties in demonstrating a connection with a terrorist act when pursuing an individual, as well as difficulties in proving that an organisation is a terrorist organisation when it is not formally designated under the Criminal Code (which was the case in Operation Halophyte). It is also difficult to pursue TF charges that relate to money supporting terrorists in other countries. The money trail becomes difficult to follow as funds are first transferred to conduit countries -generally countries neighbouring conflict zones making it difficult to prove the final destination of the funds. Prosecutors also face challenges in complex, large-scale investigations involving a large number of people, and indicated that pursuing specific TF charges would add to the burden of prosecutors, without adding much value to the case or sentences (since terrorism offences carry sentences of up to life imprisonment). Australia also focuses on disrupting potential terrorist activity, given the potential high impact of terrorism, before a TF case would have

time to be developed. For these reasons, specific TF charges are not often pursued. The technical deficiencies identified in R.5 have not negatively impacted Australia's investigation and prosecution of TF offences.

TF identification and investigation

4.13. **Australian authorities identify and investigate different types of TF offences in each counter-terrorism investigation**. TF is an avenue of enquiry in all terrorism investigations that are conducted. Where evidence supports other more specific offences, TF will be examined as an adjunct to the broader investigation.

4.14. In 2010, the AFP established a Terrorism Financing Investigations Unit (TFIU) dedicated to addressing the TF aspects of all matters identified for consideration of criminal investigation. The TFIU is a multi-agency, multi-jurisdictional team with representation from the AFP and State police, AUSTRAC, and input from the Australian Intelligence Community (AIC). It is based on similar successful groups operating in the UK (NTFIU) and the United States (TFOS). The TFIU provides expertise, specialised support, and focused engagement on an Australia-wide basis with internal and external stakeholders on all aspects of TF. The TFIU, based in the AFP's Sydney office, consists of six AFP employees as well as seconded staff from other agencies. All CT investigations which TFIU supports, are done through an investigator nominated as a financial coordinator to the investigation. Seconded members included one staff member from AUSTRAC, one staff member from an AIC agency, and, 2 New South Wales Police officers. Non-seconded staff members also contribute on a regular basis by attending TFIU coordination meetings, and by being available as a direct agency contact point for the TFIU. Both seconded and non-seconded membership fluctuates over time and as needed. The TFIU also has contact points in all Australian capitals to help facilitate a national counter-terrorism approach. The broader CT staffing for the AFP includes approximately 129 (full-time-equivalent) AFP employees complemented by staff from State police and other organisations.

4.15. The AFP has investigated 36 matters which were either TF matters or had a substantive TF component as part of the investigation. The cases included the mentioned prosecutions above and focussed, wholly or in part, on TF aspects which could have led or did lead to charges for TF offences. The investigations were preventative, as proactive steps were taken to ensure that a terrorist act did not occur or that a terrorist, terrorist act or terrorist organisation would not be funded. **In the two cases where TF offences were prosecuted, the investigations identified the financiers**.

4.16. The identification of terrorism cases occurs through a variety of means including:

- information provided by human sources;
- community reporting, including anonymously;
- information coming to the attention during the course of an existing investigation; and
- referral by AIC agencies or by foreign law enforcement or intelligence agencies.

4.17. Once a matter is identified, the full range of investigative powers (see Recommendation 31) supports the investigation process. These powers have been used in Australia's successful terrorism investigations. Investigators can also access relevant analytical software tools through AUSTRAC, or through the authorised disclosure of information which can be analysed using AFP analytical software, to support joint operational and task force investigations. More generally, spreadsheet software and analytical software linked to operational databases provide important means to address the TF components of terrorism investigations.

TF investigation integrated with and supporting national counter-terrorism strategies and investigations

4.18. Counter-terrorism strategies have successfully enabled Australia to identify and designate terrorists, terrorist organisations, and terrorist support networks, and TF investigation has contributed to this. **TF investigation is integrated with, and used to support, national counter-terrorism strategies, and investigations.** Financial intelligence, in particular AUSTRAC information, has contributed to broader

investigations by identifying other persons of interest and the existence of networks. There is also an AUSTRAC Senior Liaison Officer embedded in the TFIU. This has assisted in opening new lines of enquiry or options for disruption. The TFIU has assisted in identifying:

- the financial activities of a suspected terrorist or terrorist supporter;
- evidence of the means by which a terrorist may conduct his or her financial activity;
- evidence of financial transactions conducted;
- evidence about the time, date and place where financial activity occurs; and
- financial evidence which can be correlated against evidence from other sources, such as surveillance, travel movements or telephone interception, as a means of corroboration.

Effective, proportionate, and dissuasive sanctions

4.19. The sanctions applied against natural persons convicted of TF offences have been effective and proportionate; however, their dissuasiveness is unclear. Three convictions have taken place—all as part of the Pendennis case. The total effective sentences imposed on the accused in relation to all offences were:

- Ahmed Raad: 8 years with a non-parole period of 6 years' imprisonment (including 5 years for TF)
- Aimen Joud: 8 years with a non-parole period of 6 years' imprisonment (including 5 years for TF), and
- Ezzit Raad: 6 years with a non-parole period of 4.5 years' imprisonment (including 4 years for TF)

4.20. One person convicted of terrorism (not TF) charges in the Pendennis case has returned to a conflict zone in the Middle East to support designated terrorist groups (including the Islamic State of Iraq and the Levant (ISIL)) and advocate terrorist activity (mainly through social media). On the other hand, the ideological nature of these individuals and their associations may explain such recidivism, rather than the sanctions previously imposed on them.

Other criminal justice and other measures to disrupt TF activities

4.21. Australia primarily and successfully uses other criminal justice and administrative measures to disrupt TF activities when a prosecution for TF is not practicable. Australia places a strong focus on disrupting terrorist organisations, and terrorist acts before they occur. Thus, investigations may not advance to the stage where a TF charge is practicable. As noted above, there are also practical difficulties in pursuing TF offences.

4.22. The CDPP examines the briefs of evidence provided by the AFP and decides, in line with the Prosecution Policy of the Commonwealth, on the available and appropriate charges to bring. The assessment of the evidence by the CDPP may result in other terrorism offences in the Criminal Code, (e.g. doing an act in preparation for, or planning, terrorist acts or providing support to a terrorist organisation), offences under the CotUNA (e.g. making an asset available to a designated person or entity), or offences under the *Crimes (Foreign Incursions and Recruitment) Act 1978* (e.g. preparations for incursions into foreign states for purpose of engaging in hostile activities) being brought. Administrative action includes ASIO issuing adverse security assessments to DFAT, which can lead to a revocation of a passport.

4.23. These measures are being used to identify and disrupt domestic terrorist activity and the provision of financial support from Australia to offshore extremist groups. This confronts the risk posed by individuals travelling to conflict areas abroad (in particular Syria and Iraq) to become directly involved in designated terrorist groups, and so called "lone-wolves", who may be sympathetic to but are only indirectly aligned with such groups. The authorities have already convicted one individual under the *Crimes (Foreign Incursions and Recruitment) Act 1978*, and had begun prosecutions of three more at the time of the on-site visit. Since 1 July 2013, the federal government has also cancelled more than 70 passports on national security grounds.

Overall conclusions on Immediate Outcome 9:

4.24. Australia exhibits most characteristics of an effective system for investigating, prosecuting, and sanctioning those involved in terrorist financing. It is positive to note that Australia has undertaken several TF investigations and prosecutions, and also secured three convictions for the TF offence. Australia also successfully uses other criminal justice and administrative measures to disrupt terrorist and TF activities when a prosecution for TF is not practicable. Australia had successfully disrupted two domestic terrorist plots (Pendennis and Neath) at the time of the on-site visit.[2] Australia also uses these other measures to address the most relevant emerging TF risk – individuals travelling to conflict zones to participate in or advocate terrorist activity. Australian authorities identify and investigate different types of TF offences in each counter-terrorism investigation, and counter-terrorism strategies have successfully enabled Australia to identify and designate terrorists, terrorist organisations, and terrorist support networks. Australian authorities have not prosecuted all the different types of TF offences, such as the collection of funds for TF, or the financing of terrorist acts or individual terrorists, and the dissuasiveness of sanctions applied has not been clearly demonstrated.

4.25. **Australia is therefore rated as having a substantial level of effectiveness for IO.9.**

4.4 Effectiveness: Immediate Outcome 10 (TF preventive measures and financial sanctions)

Targeted financial sanctions for TF

4.26. **Australia is actively using the TFS framework and demonstrates some characteristics of an effective system for TFS.** With UNSCR 1267/1989 and UNSCR 1988 designations, the legal obligation to freeze assets is automatic upon designation at the UN; no additional action by Australian authorities is needed to give legal effect to a designation. Nevertheless, when there is a change in the listing at the UN, the next business day DFAT amends its Consolidated List to reflect changes in the UNSCR 1267 designations and the updated Consolidated List is published on the DFAT website and circulated for information to subscribers via email. **The automatic asset freeze obligation is a best practice for other countries on how UN designations can be implemented without delay.**

4.27. Australia had co-sponsored or acted as co-designator for a number of designations at the UN. Australia's decision to co-sponsor proposals or co-designate, includes consideration of whether the proposed designation has links to Australia or is otherwise in Australia's national interest. At the time of the on-site visit, Australia also took into account the necessity of ensuring its impartiality as chair of the UNSCR 1267/1989 and 1988 Committees when considering possible co-sponsorship or co-designation.

4.28. Australia is also using its framework to domestically list individuals and entities pursuant to UNSCR 1373 and has listed 89 persons and entities (at the time of the on-site). At the domestic level, targets for listing can be proposed to DFAT by any agency, including AFP, AGD, ASIO and other intelligence agencies. DFAT then works with intelligence agencies and law enforcement to determine if the proposed designee meets the legal test for designation. Authorities can use both open source and classified information in the creation of a statement of reasons (SOR), but the preference is to rely as little as possible on classified information in composing the SOR. After consideration by the Ambassador for Counterterrorism (a DFAT official), the SOR and a recommendation for listing, is submitted to the Minister for Foreign Affairs, who makes a final determination. After listing, a designee may contact DFAT for a copy of the unclassified SOR.

2 Another plot was disrupted soon after the on-site visit. AUSTRAC also took action in November 2014 to cancel the registration of remittance dealer (Bisotel Rieh Pty Ltd) due to concerns that its continued registration may involve a TF risk. This followed a period of engagement and notification of action by AUSTRAC.

4.29. Third party requests from foreign jurisdictions are considered under the same process. Australia receives requests either directly through DFAT or via its embassies or High Commissions abroad. DFAT begins consideration of such requests within one business day. Australia has received numerous requests from foreign jurisdictions since the establishment of the regime and has given effect to both formal and informal requests. DFAT noted that most of its domestic designations were a result of either formal requests or informal discussions with like-minded countries. Where Australia does not believe that the information provided meets the legal threshold for designation (for example due to differences in designation criteria or because the request is politically motivated), authorities still continue to monitor the individuals and entities for information to substantiate a designation. Australia has never formally rejected a request. From November 2013 to June 2014, Australia received only 3 formal third party requests. At the time of the on-site visit, authorities were advancing one for domestic designation.

4.30. Australia has made no unilateral requests to other countries for consideration of the names it has designated.[3] Australia explained that many of the designees it believes would have warranted a third-party request were subsequently designated at the UN or were subject to a third-party request by a like-minded country with Australia's active or in-principle support, often after informal discussions between Australia and a group of like-minded countries.

4.31. All designations made pursuant to Australia's implementation of UNSCR 1373 must be reviewed every three years. The review process is similar to the process for the initial listing and is to determine that the designee continues to satisfy the criteria for listing. DFAT also invites, via a media release and posting on its website, public submissions for the review regarding listees and anyone can make a submission. The Minister for Foreign Affairs must make a formal determination to renew the listing or the listing expires. As a result of the review process, four listings were permitted to expire in 2013.

4.32. Listees may apply to the Minister for revocation of the designation. Since 2002, DFAT has received three de-listing requests related to TF TFS. Two requests were filed by the same entity and were rejected in 2003 and 2004; the third request, which was filed in January 2014, was still pending at the time of the onsite visit.

4.33. As part of its outreach efforts, DFAT administers an Online Sanctions Administration System (OSAS) through which members of the public can enquire if an activity is subject to prohibitions under the sanctions regime and can apply for a sanctions permit (license). Across the TFS regimes, the average time to consider a request for a sanctions permit is approximately 15 days. DFAT also offers LinkMatchLite software to assist asset holders to consider the probability that a provided name is a match with a name on the Consolidated List. Under section 41 of the *Charter of the United Nations (Dealing with Assets) Regulation 2008,* asset holders may contact the AFP for assistance to determine whether or not an asset is owned or controlled by a listee (the process has been agreed by DFAT, the AFP, the Australian Bankers Association and major banks, and as set out on the website of DFAT). Based on the information available to the AFP, it provides an indication as to whether a name match to the Consolidated List is 'likely', 'unlikely' or 'unknown'. Under its TF sanctions regime Australia has frozen property related to only one entity listed pursuant to 1373; in 2002 AUD 2 000 was frozen in multiple bank accounts for the listed entity. There was also a false positive in 2002, where funds were initially frozen and then released. DFAT also conducts sanctions-related outreach to businesses, universities, and individuals and holds national outreach tours twice a year and speaks at relevant seminars and conferences. The March 2014 DFAT outreach events had over 100 attendees from across ten sectors, including banks, law firms, mining and dual use industries.

4.34. DFAT has primary responsibility for compliance with sanction requirements and it does issue production orders to enforce the sanctions framework. However, this is a reactive process, as DFAT's production orders are usually in response to a suspected violation. DFAT also undertakes outreach to educate society on the requirements. However, DFAT does not monitor or supervise the financial sector for compliance with the requirements of the FATF Recommendations (which would be difficult given that DFAT is not a supervisory

3 After the on-site, Australia made requests to other jurisdictions following designations in Australia under UNSCR 1373.

entity) and as expected of a supervisory authority. In addition, no financial institutions are supervised or monitored for compliance with the TFS requirements (as in financial supervision) by any other competent supervisory authority. This is a major shortcoming in the supervisory regime, as reflected under IO.3, but is relevant for IO.10 to measure effective implementation. The assessment team also confirmed that AUSTRAC does not check its own databases for matches with DFATs lists on an ongoing basis. AUSTRAC staff indicated that the vast number of false positives this would generate, would make this a challenging or impossible task. However, there is an internal SMR analysis rule that allows for checking with possible list hits, and reporting agencies can indicate on an SMR that there is a possible list hit. In addition, when discussing company registration with ASIC, ASIC stated that it does not automatically check the DFAT lists when registering a company, its directors or its shareholders. Not checking government databases against government issued lists effectively limits the same government ability to detect compliance breaches.

4.35. Assessors also sought to establish effective implementation of the requirements during interviews with the private sector, or through the statistics. All financial institutions were aware of their obligations to freeze (often referred to as the "UN, OFAC and DFAT lists") and confirmed that they were not supervised for compliance with their sanctions obligations. A few were aware that they should contact AFP if there was a question about whether they had a match with the Consolidated List, but most were unable to share feedback on the remaining practical issues that inevitably would have to come up during implementation (e.g. how to deal with similar names i.e. false positives issues; what assets needed to be frozen) and that would establish that the private sector effectively implements the requirements. Moreover, as indicated above, despite the large number of domestic designations (89 at the time of the on-site visit), only in one case were assets detected (approximately AUD 2 000 in 2002), and one false positive in 2002. The list of designated entities contains names that are common in Australia. As a result, it could be reasonably expected that similar names would have caused false positives, which would have allowed financial institutions to gather experience with dealing with false positives, demonstrating that the system was being effectively implemented.

4.36. A possible explanation for this lack of evidence of implementation may be that it seems that the sanctions framework to implement UNSCR 1373 is not used to target entities in Australia or against Australian citizens (at the time of the on-site), which indeed limits the likelihood of detecting funds and other assets of designated entities in Australia. This is in line with another related shortcoming, which is that the legal provisions are not applied systematically by the authorities. Specifically, some of the persons that had previously been convicted in Australia for terrorism or terrorist financing completed their sentences and then left Australia to openly take part in terrorist acts abroad. At the time of their travel, the groups that these Australians joined (Jabhat al-Nusra or JN and Islamic State of Iraq and the Levant or ISIL) were already designated by the federal government under UNSCR 1373 (JN) and under UNSCR 1267 (ISIL and JN) in 2013. Nevertheless, at the time of the on-site, these persons (especially those that had previously been convicted) had not been referred to the UN (under UNSCR 1267) for designation, or designated domestically (under UNSCR 1373). It should, however, be noted that two of these individuals were considered by the federal government for designation. Designation of these two persons took place on 13 November 2014, which was only after the on-site. The Australian authorities believe that their regular interaction with financial entities regarding possible designated entities before an institution entered into a customer relationship also limits the number of possible false positives.

4.37. **The Australian legal framework for the implementation of TFS is a good example for other countries, especially the immediate legal obligation to freeze assets as soon as an entity is listed by the UN, and the numerous designations made under the domestic regime are to be commended as best practices for other countries. However, effective implementation of the framework is difficult to confirm in the absence of freezing statistics, financial supervision, supervisory experience, and feedback on practical implementation by the private sector.**

Non-Profit Organisations (NPOs)

4.38. The NRA cites charities and NPOs as one of the key channels that can be used to raise funds for TF in or from Australia. It notes that organisations can be exploited in a number of ways, including disguising international funds transfers to high-risk regions, co-mingling of humanitarian aid and funds raised to finance terrorism, and diversion or siphoning of legitimate funds by or to terrorist groups after the funds arrive in the destination country.

4.39. **Despite the general risks identified by the authorities in the NRA, Australia has not undertaken a risk review of the NPO sector to identify the features and types of NPOs that are particularly at risk of being misused for TF. Subsequently, there is no TF-related outreach to, or TF-related monitoring of, the part of the sector that would be at risk and that account for a significant share of the sector's activities.**

4.40. Australia's general NPO regulator, the Australia Charities and Not-for-profits Commission (ACNC) was established in 2012 to administer the framework for the voluntary registration and regulation of charities. Only charities are permitted to register with the ACNC. About 40 000 of the 140 000 NPOs with legal personality and 20 000 without legal personality have registered, and mainly to take advantage of tax incentives. The ACNC has the ability to conduct reviews of registered charities, which focus on whether the organisation has a charitable purpose and the funds are used solely for that purpose. While the ACNC actively works to improve transparency, it has no specific TF mandate and it has not conducted outreach to the NPO sector regarding TF risks.

4.41. **Outreach efforts to the NPO sector are minimal, and not targeted.** In 2009 the AGD issued a brochure "Safeguarding Your Organisation against Terrorism: A Guidance for Non-profit Organisations". This non-binding guidance sets out best practice principles for NPOs, including on undertaking risk assessments, applying due diligence procedures to beneficiaries and third parties, being aware of legal obligations, and ensuring internal processes of transparency and accountability. In 2013 the AGD issued a fact sheet about the ongoing violence in Syria; the document focuses primarily on the Australian sanctions obligations and the best way to donate funds for humanitarian support. Both documents focused mainly on DFAT-lists requirements.

Terrorist asset seizure and confiscation (criminal justice measures)

4.42. Two TF cases have been referred to CACT since its establishment to recover TF related assets. No seizures or confiscations resulted from these referrals. These outcomes do not seem commensurate with the overall TF risk.

Overall conclusions on Immediate Outcome 10

4.43. Australia demonstrates some characteristics of an effective system in this area. Terrorists and terrorist organisations are being identified in an effort to deprive them of the resources and means to finance terrorist activities.

4.44. An area of strong technical compliance is the legal framework for TFS against persons and entities designated by the UNSC (UNSCR 1267) and under Australia's sanctions law (for UNSCR 1373). Australia has co-sponsored designation proposals to the UNSCR 1267/1989 Committee and adopted very effective measures to ensure the proper implementation of UN designations without delay. Australia has also domestically listed individuals and entities pursuant to UNSCR 1373 (including most recently two Australians fighting overseas for terrorist entities) and received, considered and given effect to third party requests. Australia actively works to publicly identify terrorists and terrorist organisations.

4.45. Furthermore, the TFS regime is administered robustly. Australia has procedures for:

i. identifying targets for listing,

ii. a regular review of listings, and

iii. the consideration of de-listing requests and sanctions permits.

iv. The authorities make a concerted effort to sensitize the public to Australian sanctions laws and to assist potential asset holders in the implementation of their obligations.

4.46. However, the private sector is not supervised for compliance with TFS requirements and was unable to demonstrate that the legal framework is effectively implemented. Effective implementation is difficult to establish in the absence of freezing statistics, financial supervision, supervisory experience, and feedback on

practical implementation by the private sector. Designating Australians previously convicted for terrorism or terrorist financing, who openly join designated terrorist organisations, could improve the system's effectiveness.[4]

4.47. NPOs are an area for improved efforts and specific action. According to the NRA, charities and NPOs are a key channel used to raise funds for TF in or from Australia. However, the lack of a targeted TF review and subsequent targeted TF-related outreach and TF-related monitoring of NPOs leaves NPOs and Australia vulnerable to misuse by terrorist organisations. Since 2010, no effort has been directed at NPOs to sensitise them to the potential risk of misuse for TF. While the ACNC actively works to improve transparency, it has no specific TF mandate and it has not conducted outreach to the NPO sector regarding TF risks.

4.48. **Australia has been rated for a moderate level of effectiveness for IO.10.**

4.5 Effectiveness: Immediate Outcome 11 (PF financial sanctions)

Targeted financial sanctions related to proliferation financing

4.49. Australia's legal system and processes for implementing UNSCRs 1718 and 1737 (as required by Recommendation 7 and assessed in this IO) are identical to those for implementing UNSCR 1267 (as required by Recommendation 6 and assessed in IO.10). The same key findings apply: a sound legal system and process exist. However, the assessors were unable to ascertain effective implementation of the requirements due to the absence of a supervisory or other compliance testing framework, the absence of implementation feedback from the financial sector, and the absence of freezing actions (including for false positives).

4.50. In addition, Australia has a proliferation-related autonomous sanctions regime, as described in the paragraphs below. This capability, and the process Australia undergoes to identify proliferation-financing targets, contributes to the overall effectiveness in preventing persons and entities involved in the proliferation of WMDs from raising, moving, and using funds.

Domestic cooperation to implement obligations to combat the financing of proliferation

4.51. DFAT takes the lead on domestic coordination regarding operational threats, cases, and international cooperation in relation to proliferation financing. DFAT discusses operational issues with domestic partners, and reaches out to the businesses that are involved. Part of this work relates to the authority of DFAT to grant licences that relate to UNSCR 1718 and 1737.

4.52. With respect to UNSCR 1718 and 1737, DFAT considers applications for sanctions permits for trade in goods and services as well as for financial transactions, and has implemented a unified system that facilitates a holistic approach to any proposed activity. Consideration of applications for sanctions permits for trade in goods and services includes seeking information about related financial transactions to ensure DFAT bases decisions about proposed activities on full information.

4.53. In considering sanctions permit applications, DFAT coordinates principally with Defence (including the Defence Export Control Office, DECO), the Australian Customs and Border Protection Agency (ACBPS) and the Australian Intelligence Community, and other agencies as appropriate. DFAT's Sanctions Section's contacts with relevant agencies appear well developed, which facilitates early identification of possible cases of proliferation financing concern and a coordinated whole-of-government response. The monthly inter-agency Non-Proliferation Coordination Group, co-chaired by DFAT's Arms Control and Counter-Proliferation Branch and attended by the Sanctions Section, is the primary mechanism for raising and discussing issues of concern, whether these are individual cases or emerging trends. All relevant agencies, including ACBPS,

4 At the time of the on-site, two of these individuals were under consideration by the government for designation. Designation of these two persons subsequently took place on 13 November 2014, after the onsite.

DECO, and AUSTRAC attend these meetings. The Sanctions Section is also in direct daily contact with ACBPS and DECO, and has established standard operating procedures in agreement with these agencies to facilitate coordination of sanctions permit applications.

4.54. As reflected under IO. 10, all financial institutions were aware of their obligations to freeze (often referred to as the "UN, OFAC and DFAT lists") and confirmed that they were not supervised for compliance with their sanctions obligations. However, there was strong evidence that the financial institutions were actively seeking to comply with TFS obligations due to the possible reputational risks and legal penalties flowing from contravening Australian sanction laws as well as concerns connected to supervisory action that had taken place in other jurisdictions for non-compliance with IO.11 / PF-related TFS obligations. DFAT is the competent authority for processing informal inquiries and formal applications relating to sanctions permits. Since 2010, DFAT has received only one application in relation to targeted financial sanctions under UNSC Iran or DPRK sanctions, which was refused. DFAT has received 276 inquiries and 873 applications in relation to trade in goods and services under UNSC and Australian autonomous DPRK and Iran sanctions. Of the 873 applications, 404 were granted, 36 denied, 326 withdrawn, and 107 never required a permit. In considering inquiries and applications, DFAT checks its own sanctions lists and the AUSTRAC database, and may also reach out to the intelligence services and – as required – to the UN. DFAT also coordinates with universities to ensure that export controlled knowledge is not acquired by sanctioned countries.

Overall conclusions on Immediate Outcome 11

4.55. Australia demonstrates to a large extent the characteristics of an effective system in this area. The issues listed under IO.10 and that relate to UNSCR 1267 also apply to IO.11.

4.56. Even though IO.11 suffers from the same issues as IO.10, IO.10 has additional shortcomings in relation to NPOs that do not apply to IO.11. In addition, the overall domestic cooperation in relation to country sanction programmes for Iran and DPRK seems sound, which may have a positive effect on the targeted financial sanctions implementation that are related to these country programmes. This domestic cooperation benefit does not apply in the case of IO.10 / UNSCR 1267, as it is not a country programme.

4.57. **Australia has been rated for a substantial level of effectiveness for IO.11.**

4.6 Recommendations on Terrorist Financing and Financing of Proliferation

Investigating and prosecuting terrorist financing (IO.9)

- Australia should give consideration, where appropriate, to actively prosecuting different types of TF offences.

Targeted financial sanctions on TF (IO.10) and financing of proliferation (IO.11)

- Australia should ensure financial institutions are actively supervised for implementation of DFAT lists, ideally through a legislative amendment to the statute identifying and authorising the agency responsible for supervision. Specifically, supervision should include a focus on those issues that other countries' supervisors have detected in relation to non-compliance with targeted financial sanctions requirements by global financial institutions, such as the facilitation of sanctions evasion by financial institutions (IO.10 and IO.11) (see also IO.3).
- Australia should ensure that government entities implement and/or supervise the targeted financial sanctions requirements of DFAT. This includes monitoring AUSTRAC's and ASIC's databases for possible matches (IO.10 and IO.11).
- Australia should take comprehensive measures to ensure that DNFBPs can also be supervised or monitored for compliance with targeted financial sanctions requirements (IO.10 and IO.11).

- Australia should continue using its preventive designation powers against identified (self-declared) members of designated terrorists groups, or propose the names of these persons for designation to the UN (IO.10).

- Australia should implement a targeted approach in relation to preventing NPOs from TF abuse. As a first step, Australia needs to undertake a thorough review of the TF risks that NPOs are facing (beyond the issues already covered in the NRA) and the potential vulnerabilities of the sector to terrorist activities. Australia should then apply the required measures to those NPOs that are at risk and that account for a significant portion of the financial resources under control of the NPO sector, and a significant share of the sector's international activities (IO.10).

4. TERRORIST FINANCING AND FINANCING OF PROLIFERATION

Recommendation 5 - Terrorist financing offence

a4.1. Australia was rated largely compliant for Special Recommendation II (criminalisation of terrorist financing). The main shortcoming at the time was that the collection of funds for a terrorist organisation and the collection or provision of funds for an individual terrorist, were not covered.

a4.2. **Criteria 5.1, 5.2, and 5.5 –** Australia has criminalised TF, mainly on the basis of the TF Convention. Terrorist acts are defined in the CC under section 100.1, and section 103.1 criminalises the financing of these acts. Section 102.6 criminalises the financing of a criminal organisation, and section 103.2 targets the financing of a terrorist.

a4.3. Section 103.1 CC criminalises the collection or provision of funds (without specifying that this could be directly or indirectly) if the person is reckless as to whether the funds will be used to facilitate or engage in a terrorist act. Under section 100.1, an act has to meet three conditions to be considered a "terrorist act": 1) it falls into a category of behaviours such as causing serious harm to a person or property, endangering another person's life, creating a serious risk to public health or safety, interfering or disrupting an electronic system; 2) there is the intention of advancing a political, religious or ideological cause; and 3) there is the intention of coercing or intimidating the federal, State, Territory or foreign government or intimidating the public.

a4.4. In relation to the first condition, Australia did demonstrate how each of the acts in the Convention annex is criminalised in Australia. However, the acts must also meet the two additional intent elements to come within the Australian definition of terrorist act, whereas Article 2(1)(a) of the Convention requires that these should be considered as terrorist acts as described in the CT Conventions, and some of these Conventions do not allow terrorist intent to be a condition for a conduct to be considered terrorism (e.g. the theft of nuclear material should be considered terrorism no matter what the actual intent of the suspect is). The Australian definition of terrorist act does not cover all acts in Article 2(1)(b) of the CTF Convention ("any other act, intended to cause death or serious bodily injury…") either, since the second condition above is not foreseen in Article 2(1)(b), and the third condition does not cover intimidating/influencing an international organisation as foreseen in Article 2(1)(b). Furthermore, subsection 100.1(3) clarifies that acts in relation to lawful advocacy, protest, dissent or industrial action are not terrorist acts unless they are intended to cause serious harm etc. to a person or create a risk to the health or the safety of the public, although this is more of an issue of effectiveness.

a4.5. Section 103.2 criminalises making funds intentionally available to, or collecting funds for (both directly and indirectly) another person while being reckless as to whether the other person will use the funds to facilitate or engage in an act. However, the collection or provision of funds to an individual terrorist to be used for any other purpose is not covered. In addition, Australia has criminalised getting funds to, from, or for a terrorist organisation in section 102.6 CC. "Terrorist organisation" can be specifically designated by regulation or more generally be one that engages in, prepares, or assists in fostering terrorist acts. Section 102.6 covers intentional support / receipt, whether directly or indirectly, and either knowledge or recklessness that the organisation is a terrorist organisation. For all three provisions (103.1, 103.2 and 102.6) intention, knowledge and recklessness are covered in section 5. 2-4 CC. Recklessness requires the prosecution to establish that a person is aware of a substantial risk that the funds would be used, and that having regard to the circumstances known at the time to the person, taking the risk was unjustifiable. Section 5.4 CC also provides that proof of knowledge or intention satisfy the recklessness element (although proof of knowledge itself caries a higher penalty than recklessness).

a4.6. **Criterion 5.3 –** All funds are covered under section 100.1 CC (the broad definition covers property and assets of any kind, tangible or intangible, movable or immovable, however acquired, as well as legal

documents and instruments in any form, titles and financial or monetary instruments). The source (legitimate or illegitimate) is irrelevant.

a4.7. **Criterion 5.4 –** Section 103 CC specifically indicates that offences are committed even if an act does not occur, or the funds will not be used in a specific act, or if the funds will be used for more than one act.

a4.8. **Criterion 5.6 –** The maximum penalty for natural persons under 103.1 and 103.2 CC is life imprisonment, and under 102.6 it is 25 years (when the persons knows it is a terrorist organisation) or 15 years (when the person is reckless as to whether the organisation is a terrorist organisation).

a4.9. **Criterion 5.7 –** See also criterion 3.10 for the basics on corporate criminal liability. Sentencing is based on a formula from imprisonment to financial penalty, all based on 4B(2), (2A) and (3) Crimes Act. This means that the maximum penalties for legal persons under 103 CC is AUD 1.7 million (knowledge and recklessness), under 102.6 it is AUD 1 275 000 (knowledge) or AUD 765 000 (recklessness). Fines are calculated in penalty units; section 4AA defines a penalty unit to be AUD 170.

a4.10. **Criterion 5.8 –** 2.4 CC extends criminal responsibility to attempt, aiding and abetting, incitement, and conspiracy to commit an offence, and to participation as an accomplice (through aid, abet, counsel, procure the commission of, section 11.2 CC) and organisation and directing (through joint commission, commission by proxy, incitement or conspiracy, sections 11.2A and 11.5).

a4.11. **Criterion 5.9 –** All TF offences meet the threshold for predicate offences. See Recommendation 3.

a4.12. **Criterion 5.10 –** TF offences apply regardless of geographic location (CC 15.4, 102.9, and 103.3).

Weighting and Conclusion

a4.13. Australia's TF criminalisation largely follows the TF Convention; the financing of terrorist acts and terrorist organisations for any purpose is covered, as is the financing of individuals while being reckless as to whether the other person will use the funds to facilitate or engage in a terrorist act. However there are shortcomings: the Australian definition of terrorist act is somewhat narrower than the definition in Articles 2(1)(a) and (b) of the TF Convention, and the provision or collection of funds to be used by an individual terrorist for any purpose is not covered. **Recommendation 5 is rated largely compliant.**

Recommendation 6 - Targeted financial sanctions related to terrorism and terrorist financing

a4.14. Australia was rated largely complaint for Special Recommendation III (freezing of terrorist assets). The main shortcoming was that Australian law did not explicitly cover funds of terrorists and those who finance terrorism or terrorist organisations outside of specific terrorist acts.

a4.15. **Criterion 6.1:** Sub-Criterion 6.1a – DFAT is responsible for proposing entities to the 1267/1989 and 1988 Committees for designation, based on the Administrative Arrangements Order (AAO) of 12 December 2013 (relations and communications with the UN). Sub-Criterion 6.1b – DFAT (coordination), AFP, AGD, ASIO and other intelligence agencies are responsible for identifying targets, each on the basis of the AAO, or their organic law. Sub-Criterion 6.1c – The legal framework allows an evidentiary standard of reasonable grounds in deciding whether or not to make a proposal for designation is applied, and there is no legal requirement that designations would be conditional upon the existence of criminal proceedings. Sub-Criterion 6.1d – The authorities indicate that the procedures and standard forms for listing are used (and required by the UN in the case of UNSCR 1989), also as a basis for domestic awareness outreach. Sub-Criterion 6.1e is not applicable as no names have been unilaterally proposed by Australia to date.

a4.16. **Criterion 6.2:** Sub-Criteria 6.2a and 6.2d – Section 15(1) and (2) of the *Charter of the United Nations Act 1945* (CotUNA) identify the Minister for Foreign Affairs as the competent authority to be responsible for designating entities that meet the requirements of the CotUNA. In addition, Section 20 of the *Charter of the United Nations (Dealing with Assets) Regulations 2008* (DAR) links the designation of a person to the relevant

criteria of UNSCR 1373. These sections also provide that any determination and listing must meet the standard of "reasonable grounds". No listing is linked to or conditional upon a criminal procedure. Sub-Criterion 6.2b – Same authorities and legal basis as criterion 6.1a; DFAT's Counter-Terrorism Branch and the Sanctions Section coordinate the review of (de)listing proposals and 3-yearly review, and advise on legal issues. Sub-Criterion 6.2c – The list of persons and entities designated by Australia under UNSCR 1373 includes listings done at the request of foreign governments. The process of considering a request commences the day it is received (through DFAT's Counter-Terrorism Branch). Sub-Criterion 6.2e is not applicable as no such request has yet been made.

a4.17. **Criterion 6.3:** Sub-Criterion 6.3a **–** Relevant government agencies have the legal authority and procedures to collect, solicit and share information to identify persons and entities that meet the criteria for designation (*Privacy Act 1988*, Australian Privacy Principles, Schedule 1, principle 3.1, AAO 6.1a and 6.1b, and section 35 of the CotUNA). Sub-Criterion 6.3b – The authorities indicate that designations are made ex parte, there is no legal or judicial requirement to hear or inform the potential designee.

a4.18. **Criterion 6.4 –** The *Charter of the United Nations (Sanctions – The Taliban) Regulations 2013* (Taliban Regulations) and the *Charter of the United Nations (Sanctions Al-Qaida) Regulations 2008* (Al-Qaida Regulations) contain provisions that prohibit dealing with or making available assets of designated persons and entities (regulations 9 and 10, or 10 and 11). Designated persons and entities are defined in article 3 as any person or entity listed by the UN under UNSCRs1267/1988/1989 and the designations are therefore automatically incorporated into Australian law. In the case of listings under UNSCR 1373, a listing takes effect as soon as the person or entity is listed in the Gazette (section 15(6) CotUNA), which takes place as soon as practicable after the Minister's decision, usually the following business day.

a4.19. **Criterion 6.5:** Sub-Criterion 6.5a – The requirement to freeze is contained as a prohibition to deal with designated persons or entities in regulation 11 (Al-Qaida Regulations, UNSCRs 1267/1989), regulation 10 (UNSCR 1988, Taliban Regulations) and section 20 CotUNA (UNSCR 1373). Freezing is ex parte and without delay as soon as the legal obligation exists. The prohibition to transfer, conversion, disposition or movement is covered through the prohibition to deal with assets (dealing is a broad term used in other laws as well). Sub-Criterion 6.5b – To cover this criterion, Australia uses the exact language used in each of the relevant UNSCRs. Each UNSCR uses slightly different language to cover the same concepts, language that is slightly different from the general language used in Recommendation 6. The definition of controlled asset (regulation 4 of the Al-Qaida and regulation 3 of the Taliban Regulations for UNSCRs 1267/1988/1989) covers an asset of a designated person or entity; and funds derived from an asset owned or controlled (which includes whole and joint ownership), directly or indirectly, by a designated person or entity; or a person acting on behalf of or at the direction of a designated person or entity.

a4.20. The definition of freezeable asset (section 14 CotUNA for UNSCR 1373) covers assets owned and controlled (whole and joint ownership) (control includes acting on behalf and at the direction of others) by a listed entity, and assets derived or generated from those assets, either directly or indirectly. The definition of asset in CotUNA (Section 2) applies to all sanction regimes. The prohibition requirements are contained in regulation 10 (Al-Qaida Regulations, UNSCRs 1267/1989), regulation 9 (UNSCR 1988, Taliban Regulations) and section 21 CotUNA (UNSCR 1373). DFAT maintains a Consolidated List of designated persons and entities subject to UNSCRs and Australian autonomous sanctions (www.dfat.gov.au/sanctions), with a possibility to receive notices if an amended list is issued. DFAT also provides software to assist those that may be holding assets to identify listed assets/entities. Additional guidance is available on the DFAT website. Also, the AFP is designated to assist to guide those that may be holding assets (regulation 41 of the DAR). Regulation 42 of the DAR requires anyone with an opinion about a targeted asset to inform the AFP. AFP, together with the ABA, has developed a referral form for possible matches. Bona fide rights are protected under section 25 CotUNA.

a4.21. **Criterion 6.6 –** Under regulation 16 CotUNA, the Minister for Foreign Affairs has the authority to revoke designations that no longer meet the designation requirements (in relation to autonomous sanctions under UNSCR 1373). Under article 15A CotUNA, the Minister for Foreign Affairs has to review all autonomous listings every three years, before they automatically cease to have effect. DFAT informs listed persons and entities of the availability of the UN Ombudsperson (Al-Qaida) or Focal Point (Taliban). One false positive was so far discovered, which was resolved using the procedure highlighted above.

a4.22. **Criterion 6.7 –** The Minister for Foreign Affairs is able to authorise access to frozen funds or other assets in accordance with UNSCR 1452. See for UNSCR 1267/1989 regulation 12 of the Al-Qaida Regulations, for UNSCR 1988 regulation 11 of the Taliban Regulation and for UNSCR 1373 section 22 of CotUNA and regulations 30 and 31 of the DAR.

Weighting and Conclusion

a4.23. **Recommendation 6 is rated compliant.**

Recommendation 7 – Targeted financial sanctions related to proliferation

a4.24. This is a new requirement that was not part of the previous assessment. Australia has implemented one system for targeted financial sanctions related to terrorism and TF (Recommendation 6), although specific regulations differ because they target different UNSCRs.

a4.25. **Criterion 7.1 –** Pursuant to its authority under subsection 2B (1) of the CotUNA, the Minister for Foreign Affairs has issued and periodically updated two regulations dealing with the requirements in Recommendation 7: The *Charter of the United Nations (Sanctions—Democratic People's Republic of Korea) Regulations 2008* ("the DPRK Regulations") and the *Charter of the United Nations (Sanctions — Iran) Regulations 2008* ("the Iran Regulations"). These regulations contain provisions that prohibit dealing with assets of designated persons and entities. Designated persons and entities are defined in regulation 4 of both regulations as any entity listed by the UN under article 8(d) of UNSCR 1718 for DPRK) and in the Annex to UNSCR 1737 or designated by the UNSC pursuant to paragraph 12 of UNSCR 1737 (for Iran). Therefore, as the UN periodically updates its designations, targeted financial sanctions automatically apply to these persons and entities in Australia.

a4.26. **Criterion 7.2 –** The requirements to freeze are contained in regulation 13 for DPRK Regulations and article 16 for the Iran Regulations. These articles prohibit using or dealing with the asset; allowing the asset to be used or dealt with; or facilitating the use of or the dealing with the asset of the designated person or entity. Freezing is without delay as soon as the legal obligation exists. Other parts of the obligations are similar to those described under criterion 6.5a. Sub-Criterion 7.2b – To cover this criterion, Australia uses the exact language used in each of the relevant UNSCRs. Each UNSCR uses slightly different language to cover the same concepts, language that is slightly different from the general language used in Recommendation 7. The definition of controlled asset (regulation 4 of the Iran and DPRK Regulations) covers an asset owned or controlled by a designated person or entity (whole and jointly), or a person or entity acting on behalf of or at the direction of a designated person or entity. The Iran Regulation covers in addition assets owned or controlled by an entity owned or controlled by a designated person or entity. "Asset" is defined in the CotUNA (section 2), applicable to the Iran and DPRK Regulations. The prohibition requirements are contained in regulations 12 and 14 for DPRK and 15 and 17 for Iran. The first article in each Regulation deals with the prohibition, the second with the licencing.

a4.27. **Criterion 7.3 –** Section 30 of CotUNA provides that the head of a designated federal entity (either DFAT, the Department of Defence, the ACBPS or AUSTRAC) may for the purpose of determining whether a UN sanction enforcement law is being complied with, require by written notice, the production of information or documents. Section 32 provides that failure to comply with such a notice is an offence punishable by imprisonment for 12 months. See also Recommendations 26 and 27.

a4.28. **Criterion 7.4 –** On its public website, DFAT informs listed entities that they can submit de-listing requests either through the focal point process outlined in UNSC resolution 1730 or through their State of residence or nationality. A link to the Focal Point website is included. A procedure to permit access to assets for humanitarian reasons is established in regulation 14 for DPRK and 17 for Iran. Regulation 5 of the DAR brings these in line with conditions and procedures set out in UNSCRs 1718 and 1737.

a4.29. **Criterion 7.5 –** For the Iran sanction regime, this is covered (regulation 5(5), DAR as required also in OP14 of UNSCR1737). For the DPRK regime, this is covered through the general freezing provisions which Australia indicates permit the freezing of interests or other earnings due on an account through addition to

these accounts, in line with UNSCR 1718. Sub-Criterion 7.5b – Regulation 17, and specifically 17(8) of the Iran and DPRK Regulations cover these requirements.

Weighting and Conclusion

a4.30. **Recommendation 7 is rated compliant.**

Recommendation 8 – Non-profit organisations

a4.31. Australia was rated partially compliant for Special Recommendation VIII (non-profit organisations). The main shortcomings that were noted at the time related to the lack of follow-up to NPO sector reviews, and the lack of effective implementation of a system to address TF-related NPO risks.

a4.32. **Criterion 8.1 –** Several reviews of the adequacies of NPO laws have been undertaken, but none of these relate to TF abuse risks. No comprehensive reviews were undertaken in order to identify the features and types of NPOs that are particularly at risk of being misused for TF or other forms of terror support. In addition, the regulator of the Australian NPO sector (ACNC) has some information on those NPOs that voluntarily register for tax purposes but none of this relates to TF. The term "terrorism" did not feature on the ACNC's public website until during the on-site (when a link to an AGD brochure was added). The TF NRA that was provided notes that current conflicts, such as in Syria, may raise the number of NPOs that are misused. However, none of this is a domestic review of the NPO sector; it does not provide the authorities with the capacity to obtain timely information on the NPOs' activities, size, and other relevant features, as a basis to identify the features and types of NPOs that may at risk for TF. There is no evidence that NPO TF vulnerabilities are periodically assessed.

a4.33. **Criterion 8.2 –** The government has only provided outreach to NPOs in relation to TF in the form of a brochure (non-binding guidance) in 2009, which was not available on the website of the ACNC until the on-site. It explains that there is a risk for NPOs to be misused and lists some of the measures that could be taken, but then focuses on Recommendation 6 issues. The ACNC has not issued any information in relation to terrorism or TF. A fact sheet in relation to Syria was developed, but it focuses on targeted financial sanctions breaches by citizens and is therefore not relevant for Recommendation 8.

a4.34. **Criterion 8.3 –** Although the main objectives of the *Australian Charities and Not-for-Profits Commission Act 2012* (ACNC Act) are to promote minimum governance standards for NPOs, these standards only apply to those NPOs that voluntarily register for tax purposes (approximately 40 000 of the estimated 140 000 known NPOs that have taken legal personality and 20 000 without legal personality have done so, for tax purposes). The ACNC Act does not relate to terrorism, except in relation to external conduct standards of designated terrorist organisations (which is related to the general prohibitions in Recommendation 6).

a4.35. **Criterion 8.4: Sub-Criterion 8.4a –** Firstly, it is not known whether the provisions in the ACNC Act (and therefore all the requirements in Criteria 8.4(a)-(f)) apply to (i) a significant portion of the financial resources under the control of the sector or (ii) a substantial share of the sector's international activities. It is also not known to what extent they cover the set of charities that should be targeted under this Recommendation (charities that may be at risk for TF may not be the ones that register to seek tax benefits). The ACNC allows certain NPOs to register voluntarily for tax reasons, and in this case they must register certain information and keep certain records. The aim of the information that is recorded is to promote public confidence in the sector (not related to counter terrorism purposes). The voluntary registration information includes the charity's responsible persons (which include directors, trustees, administrators, receivers) but not information on the purpose and objectives of the stated activities. Although these shortcomings negatively affect most criteria for Recommendation 8, these are not repeated throughout this section to allow for a more succinct presentation of the analysis. Sub-Criterion 8.4b – Medium and large charities that voluntarily register must file annual financial reports and annual information statements; small charities must provide annual information statements. Basic religious charities are excluded from the requirement to provide non-financial information even if registered. However, they must still provide non-financial information in annual information statements. Sub-Criterion 8.4c: see sub-criterion 8.4b. Sub-Criterion 8.4d – There is no licencing or registration requirement. Registration is voluntary and for tax purposes, and is only for charities and not

for other NPOs. Sub-Criterion 8.4e – see sub-criterion 8.4b. Sub-Criterion 8.4f – Record keeping requirements (e.g. sections 55-5(1) and (2)), which includes financial records that explain transactions and financial position and performance) apply only to those that voluntarily register.

a4.36. **Criterion 8.5 –** The ACNC has law enforcement powers for those charities that voluntarily register for tax purposes.

a4.37. **Criterion 8.6 –** The domestic cooperation and coordination agreements that ACNC has concluded only cover its work on the charities that voluntarily register for tax purposes. Although ACNC has access to information of NPOs, this only covers those charities that voluntarily register for tax purposes. Although there are information-sharing mechanisms in place, these do not focus on TF. In addition, the information sharing only relates to information that is available on those charities that voluntarily register for tax purposes.

a4.38. **Criterion 8.7 –** Australia uses the general procedures and mechanisms for international cooperation to handle requests relating to NPOs, and does not identify specific points of contact or procedures for requests involving NPOs. The assessment of Recommendations 37-40 has not identified any substantial problems which would affect cooperation regarding NPOs (if there would be a domestic recipient for such requests)

Weighting and Conclusion

a4.39. According to the NRA, charities and NPOs are a key channel used to raise funds for TF in or from Australia. However, the lack of a comprehensive sectorial risk assessment (as required by Recommendation 8), the lack of subsequent outreach in relation terrorist financing to the sector, and the lack of adequate preventive requirements or a supervisory framework that covers all relevant NPOs are all shortcomings. **Recommendation 8 is rated non-compliant.**

Table of Acronyms

ABN	Australian business number
ABR	Australian business register
ACA	Australian Central Authority
ACBPS	Australian Customs and Border Protection Service
ACC	Australia's Crime Commission
ACNC	Australian Charities and Not-for-Profits Commission
AFP	Australian Federal Police
AGD	Attorney General's Department
AIC	Australian Intelligence Community
AML	Anti-money laundering
APG	Asia/Pacific Group on Money Laundering
APRA	Australian Prudential Regulation Authority
ARSN	Australian registered scheme number
ASIC	Australian Securities and Investment Commission
ASIO	Australian Security Intelligence Organisation
ATO	Australian Taxation Office
AUSTRAC	Australian Transaction Reports and Analysis Centre
CACT	Criminal Asset Confiscation Taskforce
CDD	Customer due diligence
CDPP	Commonwealth Director of Public Prosecutions
CFT	Countering the financing of terrorism
CotUNA	Charter of the United Nations Act
CT	Combat terrorism
DAR	Dealing with assets regulation
DFAT	Department of Foreign Affairs and Trade
DNFBP	Designated non-financial businesses and professions
FIU	Financial intelligence unit
FTR	Financial transaction report
IDC	Interdepartmental Committee
IFTI	International fund transfer instructions
ILGA	Independent Liquor and Gaming Authority

TABLE OF ACRONYMS

IMP	Information management policy
IOSCO	International Organisation of Securities Commissions
KYC	Know your customer
MACMA	Mutual Assistance in Criminal Matters Act 1987
ML	Money laundering
MLA	Mutual legal assistance
MMOU	Multilateral memoranda of understanding
NOCRP	National organised crime response plan
NPO	Non-profit organisations
NRA	National risk assessment
NTA	National threat assessment
OCTA	Organised crime threat assessment
OSAS	Online sanctions administration system
PEPs	Politically exposed persons
PSPF	Protective security policy framework
REG	Reporting entity group
REs	Reporting entities
RNP	Remittance network provider
SMR	Suspicious matter report
SUSTR	Suspect transactions
TF	Terrorist financing
TFIU	Terrorism financing investigations unit
TFS	Targeted financial sanctions
TTR	Threshold transaction report
UNSC	United Nations Security Council
UNSCR	United Nations Security Council Resolution