Appendix 3

Correspondence

THE HON ANGUS TAYLOR MP
MINISTER FOR LAW ENFORCEMENT AND CYBER SECURITY

MS18-001465

Mr Ian Goodenough MP
Chair
Parliamentary Joint Committee on Human Rights
Parliament House
CANBERRA ACT 2600

Dear Mr ~~Goodenough~~ Ian

Thank you for your correspondence of 28 March 2018 in which further information was requested on the *Anti-Money Laundering and Counter- Terrorism Financing Amendment Instrument 2017 (No. 4)* and *Legislation (Deferral of Sunsetting- Australian Crime Commission Regulations) Certificate 2017.*

I have attached the response to the *Parliamentary Joint Committee on Human Rights' Report 3 of 2018* as requested in your letters.

Thank you for raising this matter.

Yours sincerely

ANGUS TAYLOR

Anti-Money Laundering and Counter-Terrorism Financing Rules Amendment Instrument 2017 (No. 4) [F2017L01678]

Committee comment

1.17 The right to a fair trial and fair hearing may be engaged and limited by the measure. The preceding analysis raises questions as to whether the measure is compatible with these rights.

1.18 Accordingly, the committee requests the advice of the Attorney-General as to whether the measure is compatible with the right to a fair trial and fair hearing including:

- **whether an exemption granted by the AUSTRAC CEO could permit law enforcement officers (acting through reporting entities) to incite or encourage the commission of an offence (including whether there are any safeguards in place);**
- **if the right to a fair trial and fair hearing may be limited by the measure:**
    - **how the measure is effective to achieve (that is, rationally connected to) its stated objectives; and**
    - **whether any limitation is a reasonable and proportionate means of achieving the stated objective (including whether there are adequate and effective safeguards in place, such as, to ensure that law enforcement officers are not able to incite or encourage the commission of an offence, or to rely on evidence that has been improperly obtained in criminal proceedings).**

Response

Background – policy objectives of the legislative instrument

The *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) (AML/CTF Act) imposes a number of obligations on persons that provide designated services (known as reporting entities). Relevantly, these obligations include:

- **Identification and verification**. Reporting entities must identify their customers, and verify those customers' identity before providing a designated service.
- **Developing and maintaining an AML/CTF Program**. Reporting entities must have and comply with anti-money laundering and counter-terrorism financing programs (AML/CTF programs), which are designed to identify, mitigate and manage the money laundering or terrorist financing (ML/TF) risks a reporting entity may reasonably face in providing a designated service.
- **Ongoing customer due diligence**. As part of its AML/CTF Program, reporting entities are required to have in place appropriate systems and controls to determine

whether additional customer information should be collected and/or verified on an ongoing basis to ensure that the reporting entity holds up-to-date information about its customers. This process is known as 'ongoing customer due diligence' (OCDD). OCDD ensures customers are monitored on an ongoing basis to identify, mitigate and manage any ML/TF risk posed by providing designated services. The decision to apply the OCDD process to a particular customer depends on the customer's level of assessed ML/TF risk.

- **Enhanced customer due diligence**. As part of OCDD, reporting entities are also required to implement a transaction monitoring program and develop an 'enhanced customer due diligence' (ECDD) program. Where a reporting entity determines that the ML/TF or other serious crime risk associated with dealing with a certain customer is high, it is required to implement a range of ECDD measures. These measures may include:
    - **seeking further information from the customer** to clarify or update existing information, obtain further information, or clarify the nature of the customer's ongoing business with the reporting entity;
    - **undertaking more detailed analysis of the customer's information** and beneficial owner information, including, where appropriate, taking reasonable measures to identify the source of wealth and source of funds for the customer and each beneficial owner; and
    - **conducting further analysis and monitoring of the customer's transactions**, including the purpose or nature of specific transactions, and the expected nature and level of transaction behaviour, including future transactions.

An issue arises where, as a result of law enforcement enquiries, a reporting entity forms a suspicion that a customer or their account is involved in or is being used to facilitate ML/TF or other serious crimes. The reporting entity is then obliged to take action in line with its OCDD/ECDD obligations under the AML/CTF Act. These actions may result in the customer being tipped-off to the fact that either they personally or their financial transactions have been flagged as suspicious and are likely under enhanced scrutiny. These customers often decide to cease their activities with the reporting entity, thereby limiting the ability of law enforcement agencies to continue to investigate and follow the financial transactions.

The amendments made by the *Anti-Money Laundering and Counter-Terrorism Financing Rules Amendment Instrument 2017 (No. 4)* (the Amendment Instrument) are intended to address this issue. The Amendment Instrument may provide reporting entities with assurance that they will not be in breach of their obligations under the AML/CTF Act if, after being alerted to the high-risk nature of a customer following law enforcement enquiries and/or at the request of law enforcement agencies, the reporting entities refrain from conducting any additional OCDD/ECDD queries and continue to provide that customer with designated services to avoid 'tipping off' the customer whilst investigation of their financial transactions is ongoing.

The Amendment Instrument also exempts reporting entities from a number of provisions in Part 12—Offences of the AML/CTF Act. The exemption from these provisions addresses a situation where, as a result of law enforcement enquiries, a reporting entity is made aware that a customer is not who they claim to be. If the reporting entity were to continue to provide

that person with a designated service, they could potentially be in breach of sections 136 (false or misleading information), 137 (producing false or misleading documents), 138 (false documents), 139 (providing a designated service using a false customer name or customer anonymity).

Reporting entities are also exempted from section 142 of the AML/CTF Act (conducting transactions so as to avoid reporting requirements relating to threshold transactions). This is necessary to ensure that they do not commit an offence when conducting transactions that they have reason to believe, following law enforcement enquiries, are likely to have been deliberately structured to avoid giving rise to a threshold transaction that would otherwise need to have been reported under section 43 of the AML/CTF Act.

Whether the measures incite or encourage the commission of an offence

The Committee's report notes that the right to a fair trial, which is guaranteed by article 14 of the International Covenant on Civil and Political Rights (ICCPR), also encompasses notions of the fair administration of justice and prohibits investigatory techniques that incite individuals to commit a criminal offence, citing the European Court of Human Rights (ECHR) cases of *Ramanauskas v. Lithuania*[1] and *Teixeira de Castro v. Portugal*[2] in support.

In *Ramanauskas,* the ECHR held that 'incitement' occurs where law enforcement officers (whether themselves or through persons acting on their instructions) do not confine themselves to investigating criminal activity in an essentially passive manner, but exert such an influence on the subject as to incite the commission of an offence that would otherwise not have been committed, in order to make it possible to establish the offence (that is, to provide evidence and institute a prosecution).[3] In other words, the Court considered whether the offence would have been committed without the authorities' involvement.[4]

In *Teixeira de Castro*, the ECHR held that law enforcement officers had not confined themselves to investigating criminal activity in a passive manner because they had instigated the offence, and there was no evidence to suggest that without their intervention the offence would have been committed. The Court distinguished the officers' actions from those of ordinary undercover agents, who may conceal their identities in order to obtain information and evidence about a crime without actively inciting its author to commit it. In reaching its conclusion, the Court emphasised that the authorities did not appear to have had any good reason to suspect Mr Teixeira de Castro of being a drug dealer: he had no criminal record and there was nothing to suggest that he had a predisposition to become involved in drug trafficking until he was approached by the police. The Court also found that there were no objective suspicions that Mr Teixeira de Castro had been involved in any criminal activity, nor was there any evidence to support the argument that he was predisposed to commit offences.[5]

The principles outlined by the ECHR in *Ramanauskas* and *Teixeira de Castro* accord with the approach taken in Australian jurisdictions in similar cases dealing with 'entrapment'. As noted by the High Court in *Ridgeway v R*, while Australia does not generally recognise entrapment as a defence to a criminal charge, the cases that have been decided "favour the view that relief should only be granted if the accused 'otherwise would not have committed or would have been unlikely to commit [the offence]'".[6]

The purpose of the Amendment Instrument is to allow law enforcement agencies to maintain their visibility over criminal wealth and financial flows through suspect accounts that may otherwise be closed by reporting entities due to perceived ML/TF risks, or abandoned by customers that had been alerted to the fact that their transactions were subject to enhanced scrutiny. The Amendment Instrument makes no provision for, and is not capable of in any way authorising or affecting, the use of particular investigatory techniques by law enforcement agencies, nor does it provide any means for law enforcement to exert influence

[1] ECHR Application No. 74420/01, 5 February 2008.
[2] ECHR Application No. 25829/94, 9 June 1998, at 1463, § 38 .
[3] Note 1 above, at 55.
[4] *Baltiņš v. Latvia*, ECHR Application No. 25282/07, 8 January 2013, at 56.
[5] Note 2 above, at 1463, § 37-39.
[6] (1995) 129 ALR 41, at 81, citing *Sloane* (1990) 49 A Crim R, at 273

over a customer or incite them to commit an offence, that is not otherwise available to them within the existing confines of the law.

The mechanism provided for by the Amendment Instrument may only be exercised where an investigation into a serious offence *has already commenced*, i.e. where law enforcement already have sound reasons to suspect the persons prior involvement in particular unlawful activities.[7] Further, it requires a requesting officer—of the requisite seniority[8]—to provide a written statement to the AUSTRAC CEO confirming that they reasonably believe that the continued provision of a designated service(s) by a reporting entity would assist with the ongoing investigation of that offence. Accordingly, the relevant law enforcement agency must already have formed the relevant suspicion and commenced an investigation in order to make an application; the exemption mechanism cannot be utilised to establish criminal intent that had previously been absent.

It is also important to note that the Amendment Instrument has no coercive or compulsive effect. The exemption mechanism provides reporting entities with the comfort of regulatory relief in the event that they choose to assist and cooperate with a law enforcement investigation into a serious offence. The Amendment Instrument does not allow law enforcement agencies to compel a reporting entity to continue to provide a designated service to a customer; that will continue to be a decision made by each reporting entity in line with its risk-based AML/CTF systems and controls.

Reasonableness and proportionality

The measures introduced by the Amendment Instrument are a reasonable and proportionate way of meeting its objectives, which are to support cooperation and collaboration among reporting entities, AUSTRAC, and other government agencies, particularly law enforcement agencies, in the detection and disruption of serious and organised crime, money laundering, and the financing of terrorism.

The measures are subject to appropriate safeguards, including requirements for applications to:

- be made by a senior official having reasonable grounds to believe that the exemption would assist in the investigation of a serious offence;
- include a declaration that the information provided in the application is true, accurate, and complete; and
- be signed off by the AUSTRAC CEO.

The operation of the exemption is also limited to a defined period of six months, starting on the date specified in the notice of the exemption decision, or until the eligible agency notifies both the AUSTRAC CEO and the exempted reporting entity or entities that the relevant investigation has ceased—whichever occurs first.

---

[7] See *Baltiņš v. Latvia*, note 4 above at 56.

[8] An application may only be made by the head of an eligible agency, a member of the eligible agency who is an SES employee or an equivalent under State or Territory legislation, or a member of an eligible agency who holds the rank of Superintendent or higher.

The Hon Dan Tehan MP
Minister for Social Services

Parliament House
CANBERRA ACT 2600

Telephone: 02 6277 7560

MC18-003606

23 MAY 2018

Mr Ian Goodenough MP
Chair
Parliamentary Joint Committee on Human Rights
Parliament House
CANBERRA ACT 2600

Dear Mr Goodenough Ian,

Thank you for your letter of 9 May 2018 regarding the Parliamentary Joint Committee on Human Rights' consideration of the Crimes Amendment (National Disability Insurance Scheme – Worker Screening) Bill 2018 (the Bill) in its Report 4 of 2018.

As you would be aware, the Bill received bipartisan support and was passed without amendment on 10 May 2018. Notwithstanding the Bill's passage, I am pleased to provide further information on National Disability Insurance Scheme (NDIS) worker screening regime as requested by the Committee.

Compatibility of the measure with the right to privacy and the right to work

The Committee has invited me to provide further information as to the proposed safeguards in relation to the criminal history checks undertaken as part of the proposed NDIS Worker Screening Check, including:

- whether the risk assessment framework outlined in the Minister's response will be set out in legislation or legislative instrument; and
- whether a decision relating to a person's suitability for employment following worker screening is able to be reviewed.

The worker screening regime is a shared responsibility of Commonwealth, state and territory governments. The Commonwealth is responsible for leading the broad national policy design and the states and territories are responsible for the implementation and operational elements of the worker screening regime, including introducing legislation establishing the worker screening units responsible for screening NDIS workers in each state and territory.

The various elements of the national policy that make up the worker screening regime are set out in an Intergovernmental Agreement ('the IGA') between the Commonwealth and state and territory governments. In relation to the risk assessment framework I referred to in my previous letter to the Committee, the framework is a national policy that will be agreed to by all participating jurisdictions. Consistent with the Council of Australian Government's division of responsibility for NDIS worker screening, states and territories will implement the risk assessment framework in their jurisdiction, including, where necessary, by amending existing legislation or introducing new legislation to give effect to the requirements under the IGA.

I note that before a state or territory worker screening unit can be prescribed for the purpose of performing NDIS worker screening checks, under the Bill the Minister needs to be satisfied that the worker screening unit:

- is required or permitted by or under a Commonwealth law, a state law or a territory law to obtain and deal with information about persons who work, or seek to work, with a person with disability; and
- complies with applicable Commonwealth law, state law or territory law relating to privacy, human rights and records management; and
- complies with the principles of natural justice; and
- has risk assessment frameworks and appropriately skilled staff to assess risks to the safety of a person with disability.

Accordingly, before a state or territory worker screening unit can be prescribed for the purpose of NDIS worker screening each jurisdiction must demonstrate it satisfies each of the above criteria, including importantly, the requirement to comply with the principles of natural justice.

As the Committee has noted, under the existing working with children checks regime, states and territories do provide review rights for those individuals who are subject to an adverse finding. The Committee may also like to note that under the IGA, state and territory worker screening units will agree to provide certain review and appeal rights to individual workers who may be subject to an adverse decision. This will enable an individual to seek review of decisions of state or territory worker screening units to:

- issue an exclusion (meaning a person cannot work in certain roles in the NDIS);
- revoke a clearance;
- apply an interim bar (or temporary exclusion); and
- suspend a clearance.

In such cases the rules of natural justice and procedural fairness will apply and where there is an intention to make an adverse decision states and territories, consistent with the IGA, will:

- disclose the reason the adverse decision is proposed, except where the NDIS worker screening unit is required under Commonwealth, state or territory law to refuse to disclose the information;
- allow the individual a reasonable opportunity to be heard; and
- consider the individual's response before finalising the decision.

I note the Committee's Report queries whether there are less rights restrictive alternatives available, including whether only 'serious offences or offences that are relevant to a person's suitability as a disability worker' should be taken into account by worker screening units. In my previous letter to the Committee I noted that even less serious offences such as shoplifting are considered directly relevant to an individual's suitability as offences of this nature are directly relevant to an individual's trustworthiness and integrity. I also note the weight given to such lesser offences will be relevant in any state and territory worker screening unit decisions. My previous letter noted this is particularly relevant when individuals employed within the NDIS will have access to the person with disability's personal belongings, finances and medication.

I reiterate that state and territory worker screening units must be provided with sufficient information in order to effectively and diligently perform their functions and discharge their duties. Limiting the criminal history information available to the worker screening unit will diminish the effectiveness of their risk assessments and would fail to give due regard to the rights of persons with disability to be protected from workers who may pose an unacceptable risk of harm. I also reiterate that the fact that an individual may have a criminal conviction for a minor offence, which occurred a long time ago, only forms one part of the analysis and risk assessment undertaken by a state or territory worker screening unit and will not necessarily prevent that worker from gaining employment with an NDIS provider.

The Committee may wish to note that during the development of the Bill, my Department consulted with the Office of the Australian Information Commissioner. In addition to Ministerial oversight of the worker screening regime through the process of prescribing state or territory worker screening units, there will also be Parliamentary oversight and scrutiny of the worker screening regime through the Bill's requirement to table two written reports of the operation of the worker screening regime. The first report is to be tabled by 31 December 2019, and the second is to be tabled by 31 December 2022.

Having regard to the objective of the worker screening regime, the supporting framework in the IGA, the risk-based worker screening assessments under legislation to be implemented by states and territories, I consider the Bill pursues the legitimate objective of ensuring persons with disability are protected from harm and the measures are reasonable, proportionate and necessary.

Compatibility of the measure with the right to equality and non-discrimination

The Committee has also invited me to provide further information as to the proposed safeguards in relation to the criminal history checks undertaken as part of the proposed NDIS Worker Screening Check, including:

- whether the risk assessment framework outlined in the Minister's response will be set out in legislation or legislative instrument; and
- whether a decision relating to a person's suitability for employment following worker screening is able to be reviewed.

In response to the Committee's specific questions I refer the Committee to my comments above. To address some of the additional concerns raised by the Committee in relation to the engagement of the right to equality and non-discrimination I provide the following further information.

The right to equality and non-discrimination is set out at articles 2(1) and 26 of the International Covenant on Civil and Political Rights (ICCPR). Article 2(1) provides that each state undertakes to respect and ensure to all individuals the rights recognised in the ICCPR, without distinction of any kind, such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status. Article 26 provides that all persons are equal before the law and are entitled without any discrimination to the equal protection of the law. In this respect the law shall prohibit any discrimination and guarantee to all persons equal and effective protection against discrimination on any ground.

The Committee has acknowledged that differential treatment (including the differential effect of a measure that is neutral on its face) will not constitute unlawful discrimination if the differential treatment is based on reasonable and objective criteria such that it serves a legitimate objective, is rationally connected to that legitimate objective, and is a proportionate means of achieving that objective.

Any differential treatment as envisaged by the Act is reasonable and proportionate. This is because the legitimate objective of the Bill is to protect persons with disability from harm. I also hold this view because of the various criteria that must be satisfied before a worker screening unit can be prescribed under the legislation, including the safeguards which have been deliberately incorporated within the Bill and the broader NDIS worker screening framework. Furthermore, any differential treatment will not constitute unlawful discrimination on the basis that there is sufficient research and objective evidence that supports the relevance of criminal records as a basis for determining an individual's risk to vulnerable people.

I also note the measures in the Bill are consistent with many of the recommendations that emerged from the Royal Commission Working With Children Checks Report. This Report along with the other findings of the Royal Commission serves to highlight the importance of Commonwealth and state and territory governments working together to ensure that our most vulnerable community members are protected from harm. The measures in this Bill will help ensure that persons with disability within the NDIS are afforded the same level of protection as is currently provided under the Working With Children Checks regime.

The Bill requires that only a prescribed person or body can receive, use or disclose information for the purpose of worker screening.

I trust this information is of assistance to the Committee and thank the Committee for its consideration of the Bill.

Yours sincerely

DAN TEHAN

The Hon Christian Porter MP
Attorney-General

MC18-003357

Mr Ian Goodenough MP
Chair
Parliamentary Joint Committee on Human Rights
PO Box 6100
Parliament House
CANBERRA ACT 2600
human.rights@aph.gov.au

27 APR 2018

Dear ~~Chair~~ Ian

Thank you for your letter of 28 March 2018 regarding Report 3 of 2018 of the Parliamentary Joint Committee on Human Rights addressing recently made extradition regulations. In the Report the Committee seeks further information on the human rights compatibility of the *Extradition Act 1988* in order to make a determination as to compatibility of the regulations with human rights. I appreciate the time you have taken to bring these matters to my attention.

I attach my response to the issues raised by the Committee. This notes that I am satisfied that the safeguards in Australia's extradition regime are adequate and appropriate for implementing Australia's human rights obligations, including through the use of discretionary powers. I trust that the enclosed information is of assistance.

Thank you for raising these matters with me.

Yours sincerely

The Hon Christian Porter MP
Attorney-General

Encl. Response to Parliamentary Committee on Human Rights Report 3 of 18

Response to the Parliamentary Joint Committee on Human Rights Report 3/18: Extradition (El Salvador) Regulations 2017; Extradition Legislation Amendment (2017 Measures No. 1) Regulations 2017

Overall comment applicable to all aspects of the Committee's report regarding discretionary power

I note that the matters raised in the Committee's Report have been canvassed and responded to in the context of previous Committee Reports. I reiterate that the Government does not accept the Committee's position that in order for Australia's domestic system to be consistent with our human rights obligations there needs to be express statutory provisions implementing the obligation. The Government is committed to ensuring that Australia's domestic extradition regime under the *Extradition Act 1988* (the Extradition Act) operates in a manner that is consistent with Australia's international law obligations, including international human rights law obligations. Under paragraph 22(3)(f) of the Extradition Act, the Attorney-General has a general discretion not to surrender a person. In exercising this discretion, an assessment of Australia's human rights obligations is undertaken on a case by case basis, which covers the matters identified by the Committee in its report. For these reasons I consider that the general discretion is an appropriate and adequate safeguard.

Balancing extradition and human rights obligations

Australia takes its human rights obligations very seriously and is committed to implementing them. Australia also has international obligations under bilateral and multilateral treaties to extradite persons in certain circumstances. Australia's extradition regime is an important part of our ability to combat domestic and transnational crimes, including serious offences such as terrorism, murder, drug trafficking and so forth. Many of these crimes impact upon community safety. Both of these sets of obligations are carefully considered when developing extradition arrangements. Human rights obligations are given a high priority and only limited where it is necessary to do so and proportionate to the objectives of ensuring Australia is not a safe haven for alleged criminals seeking to evade justice and ensuring Australia can pursue alleged criminals offshore.

EXTRADITION (EL SALVADOR) REGULATIONS 2017

1.63 The committee seeks the advice of the Attorney-General as to the adequacy of the safeguards in the El Salvador regulations and Extradition Act in relation to the extradition of persons who may be in danger of being subject to cruel, inhuman or degrading treatment or punishment upon return to the extradition country.

The safeguards in the Extradition Act adequately protect persons who may be in danger of being subject to cruel, inhuman or degrading treatment or punishment upon return to an extradition country.

Subsection 22(3) of the Extradition Act is consistent with Australia's obligations under the *Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment* (CAT). When determining whether an eligible person is to be surrendered to a foreign country, the Attorney-General must be satisfied, in accordance with paragraph 22(3)(b), that the person will not be subjected to torture on surrender of the kind falling within the scope of Article 1 of the CAT.

Similarly, even where a person has waived extradition, under paragraph 15B(3)(a) of the Extradition Act, the Attorney-General may only surrender the person if the Attorney-General does not have substantial grounds for believing that the person would be in danger of being subjected to torture, if surrendered.

Subsection 22(3) does not require explicit reference to the matters in Article 7 of the *International Covenant on Civil and Political Rights* (ICCPR) in order to fulfil Australia's obligations under that Covenant. Under paragraph 22(3)(f) of the Extradition Act, the Attorney-General has a broad, general discretion whether to surrender a person to a foreign country. In accordance with the principle of procedural fairness, a person who is the subject of an extradition request may make submissions on any matter he or she wishes the Attorney-General to take into consideration when making a surrender determination. This can include submissions regarding compatibility of the person's surrender with Australia's obligations under Article 7 of the ICCPR. In addition, in the absence of such representations, if the Attorney-General's Department was aware of any issue or situation which might engage Australia's obligations under Article 7 of the ICCPR, the Department would bring this to the Attorney General's attention. For example, the Department's analysis may consider country information, reports prepared by non-government organisations and information provided through the diplomatic network.

As noted above, I consider that the general discretion is an appropriate and adequate safeguard.

1.67 The committee seeks the advice of the Attorney-General as to the adequacy of the safeguards in place to protect the right to life of persons who may be subject to the death penalty if extradited.

Undertakings

In accordance with Australia's longstanding opposition to the death penalty, the Australian Government will not surrender a person to a foreign country in circumstances where the death penalty would be imposed. The safeguards in the Extradition Act adequately protect the right to life of persons who may be subject to the death penalty if extradited.

Paragraph 22(3)(c) of the Extradition Act provides that where an offence is punishable by a penalty of death, Australia cannot extradite a person unless an undertaking is given by the requesting party that:

- the person will not be tried for the offence
- if the person is tried for the offence, the death penalty will not be imposed on the person, or
- if the death penalty is imposed on the person, it will not be carried out.

Similarly, even where a person has waived extradition, under paragraph 15B(3)(b) of the Extradition Act, the Attorney-General may only surrender that person if he or she is satisfied that there is no real risk that the death penalty will be carried out upon the person in relation to any offence, if surrendered.

There is no discretion in the Extradition Act that would allow a person to be surrendered in the absence of an undertaking from the requesting country that the death penalty will not be imposed.

The assessment of the risk that a person might be subjected to the death penalty occurs well prior to any request for an undertaking which would satisfy paragraph 22(3)(c). An extradition request raising potential death penalty issues is identified by the Attorney-General's Department at the earliest stages of the extradition process. If the Department held any concerns about the bona fides of a death penalty undertaking, the Department would recommend that the Attorney-General did not accept and progress the request. If a death penalty undertaking is requested, it would be requested and provided by a formal Government to Government communication. The Full Federal Court decision in *McCrea v Minister for Justice and Customs [2005] FCAFC 180* sets out the test for an acceptable death penalty undertaking. The test requires that the Attorney-General be satisfied that 'the undertaking is one that, in the context of the system of law and government of the country seeking surrender, has the character of an undertaking by virtue of which the death penalty would not be carried out'.

If, notwithstanding the receipt of an undertaking, the Attorney-General considered that a real risk remained that the person will be subject to the death penalty, the Attorney-General could refuse extradition in the exercise of the general discretion under paragraph 22(3)(f) of the Extradition Act. As noted above, I consider that the general discretion is an appropriate and adequate safeguard.

These safeguards allow Australia to meet its obligations under the ICCPR and the Second Optional Protocol to the ICCPR.

Monitoring compliance with undertakings

The Department of Foreign Affairs and Trade (DFAT) is responsible for the provision of consular assistance to Australians encountering difficulties overseas. Where DFAT has been informed that an Australian citizen has been arrested, detained or imprisoned overseas, DFAT will write to the individual to offer consular assistance. On acceptance of the services offered, DFAT will provide details of local lawyers and interpreters, conduct welfare checks and, when necessary, take steps to ensure the detainee is treated fairly to the extent possible under the laws of the relevant country, given that consular assistance cannot override local laws. Australia does not monitor the status of foreign nationals who have been extradited by Australia, as Australia has no consular right of access to non-nationals. The decision to monitor a foreign national is a matter for that person's country of citizenship. With the consent of the person, Australia can inform consular authorities of their country of citizenship of their extradition to a third country. Attempts to monitor foreign nationals may be seen as infringing on the foreign country's sovereignty and criminal justice processes.

It is the Attorney-General's Department's longstanding experience that death penalty undertakings are respected. The Department is not aware of any case in which the terms of a diplomatic undertaking issued to Australia by a country pursuant to paragraph 22(3)(c) of the Extradition Act have been breached. If the Department held real concerns that a death penalty undertaking would not be honoured, it would not recommend that the Attorney-General progress the extradition request. Extradition between countries is based on reciprocity. As such, any conditions imposed are likely to be honoured by the receiving country. This is due to the Government to Government

nature of extradition, and recognition by that country that undertakings must be respected to ensure future cooperation. In the event that the Department or the Attorney-General became aware of a potential breach, this would be raised with the country at the highest diplomatic levels. The use of undertakings is an important practice that allows Australia to establish extradition partnerships with important partner countries that retain the death penalty, such as the United States.

The Attorney-General's Department has provided information on extradition matters in its annual reports to Parliament since the establishment of the Extradition Act. This information currently includes for that financial year:

- the number of extradition requests made to, granted by and refused by Australia
- the countries which had an extradition request granted by Australia (and how many for each country)
- the number and nationality of persons who have been extradited from Australia
- the number of Australian permanent residents extradited from Australia
- the major categories of offences for which extradition has been granted by Australia, and
- whether there had been any breaches of undertakings by a foreign country in relation to a person extradited from Australia.

I note that there have been no breaches of death penalty undertakings to report.

1.73 The committee seeks the advice of the Attorney-General as to:

- **the adequacy of the safeguards in place to prevent the extradition of persons who may, on surrender, suffer a flagrant denial of justice; and**
- **whether, in not requiring any evidence to be produced before a person can be extradited, and in preventing a person subject to extradition from producing evidence about the alleged offence, the El Salvador regulations and the Extradition Act are compatible with the right to a fair trial and fair hearing.**

Fair trial

As has been previously noted by the Committee and the Government, it is the Australian Government's view that Article 14 of the ICCPR does not contain *non-refoulement* obligations. In any event, the Extradition Act provides adequate safeguards to address matters relating to fair trials.

In addition to the mandatory ground of refusal relating to double jeopardy (under paragraph 22(3)(a) read together with section 7), the Attorney-General has a broad discretionary ground to refuse surrender under paragraph 22(3)(f) of the Extradition Act. This discretionary power provides a sufficient basis to refuse extradition in circumstances where there are legitimate concerns about the person's access to a fair trial. While Australia's *non-refoulement* obligations under the ICCPR do not extend to Article 14 of the ICCPR, in relevant matters, the Department would put

particular claims that a person may not receive a fair trial in light of their circumstances or any other fair trial issues before the Attorney-General as relevant considerations in exercising his or her general discretion. The relevant considerations may include the extent to which an individual would receive minimum procedural guarantees in a criminal trial in the country to which he or she is being returned. Assessment of these claims may include analysis of the person's claims and any representations or undertakings from the requesting country. The assessment may also consider country information, reports prepared by non-government organisations and information provided through the diplomatic network.

Expressly including fair trial as a ground for refusal may generate litigation about issues which are essentially attributable to differences between the bases of common law and civil legal systems. Allowing individuals to challenge extradition on this basis would also be incompatible with the international principle of comity.

As noted above, I consider that the general discretion is an appropriate and adequate safeguard.

Evidence requirements

As noted above, Article 14 of the ICCPR does not contain *non-refoulement* obligations.

Extradition is an administrative legal process whereby a person may be transferred from one country to another to face prosecution or to serve a prison sentence for offences against the law of the other country. The extradition process in Australia does not involve an assessment of guilt or innocence; it is not a criminal trial.

The purpose of an extradition hearing is to determine whether a person should be extradited; it is not to test evidence in the case against them. It is important that a person faces prosecution or serves a sentence in the country in which he or she has been accused or sentenced. The 'no evidence' standard has been Australia's preferred approach since 1988 and all of Australia's modern extradition treaties have been negotiated on this basis.

The term 'no evidence' does not mean 'no information'. Rather, it means that an extradition request needs to be supported by a statement of the offence and the applicable penalty, and a statement setting out the conduct alleged against the person in respect of each offence for which extradition is sought, but it does not require evidence to be produced which is sufficient to prove each element of each alleged offence under the laws of the requested country (such as 'prima facie' evidence including witness statements and affidavits). Given it is not the purpose of an extradition hearing to test the evidence, it is appropriate that the person sought to be extradited does not produce evidence about the alleged offence.

The 'no evidence' standard is in line with the international trend toward simplifying the extradition process and is consistent with the United Nations Model Treaty on Extradition. It has allowed Australia to enter into extradition relations with many civil law countries that would otherwise have been unable to conduct extradition with Australia. A return by Australia to a prima facie evidentiary standard would cause considerable disruption to our existing extradition relationships, and would be very counterproductive in terms of international law enforcement cooperation.

1.79 The committee seeks the advice of the Attorney-General as to:

- **whether a presumption against bail except in special circumstances is a proportionate limitation on the right to liberty;**

It is accepted international practice for a person to be held in administrative detention pending extradition proceedings. The remand of the person is not undertaken as a form of punishment and in no way relates to guilt or innocence of any offence. The validity of Australia's process of remanding a person during extradition proceedings has been confirmed by the High Court in *Vasiljković v Commonwealth [2006] HCA 40*.

The presumption against bail for persons sought for extradition is appropriate given the serious flight risk posed in extradition matters and Australia's international obligations to secure the return of alleged offenders to face justice. Unfortunately, reporting and other bail conditions are not sufficient to prevent individuals who wish to evade extradition from absconding. In extradition cases there is an increased risk of persons absconding before they can be surrendered to the requesting foreign country. If a person who has been remanded on bail absconds during extradition proceedings, it jeopardises Australia's ability to extradite the person which in turn would impede Australia's treaty obligations to return a person to the requesting country. Ultimately, it can also lead to a state of impunity where a person can disappear and continue to evade law enforcement authorities.

The High Court in *United Mexican States v Cabal [2001] HCA 60* observed that to grant bail where a risk of flight exists would jeopardise Australia's relationship with the country seeking extradition and jeopardise our standing in the international community. Bail can be granted where special circumstances exist. The courts have shown their willingness to grant bail when these special circumstances arise.

For these reasons the Government considers the current presumption that bail should only be granted in 'special circumstances' is appropriate, given the significant flight risk posed by people subject to extradition proceedings, and should be maintained. It is a reasonable and proportionate limitation on the right to liberty, necessary to achieve the legitimate objective of securing the return of alleged offenders to face justice, noting that extradition offences are serious offences, including terrorism, murder and transnational organised crimes.

- **whether, having regard to *Griffiths v Australia*, the El Salvador regulations and the Extradition Act provide an opportunity for persons to review the lawfulness of their detention pending extradition in accordance with article 9(4) of the ICCPR;**

Article 9(4) of the ICCPR provides that: "Anyone who is deprived of his liberty by arrest or detention shall be entitled to take proceedings before a court, in order that that court may decide without delay on the lawfulness of his detention and order his release if the detention is not lawful."

Following amendments to the Extradition Act in 2012, a person may make an application for bail at each stage of the extradition process (prior to the *Griffiths* matter a person could only make bail applications in the early stages of extradition proceedings). The court may grant bail if there are

special circumstances justifying the person's release, and the courts have shown their willingness to grant bail when these circumstances arise.

In addition, there are a number of other avenues for a person to review the lawfulness of their detention, including:

- the person may seek a remedy under section 39B of the *Judiciary Act 1903*
- a writ of mandamus in the High Court under section 75(v) of the Constitution, and
- a habeas corpus application.

Australia's legal framework for extradition therefore provides numerous opportunities for persons to review the lawfulness of their detention pending extradition in accordance with article 9(4) of the ICCPR.

- **whether detaining persons during the extradition process without first testing the evidence against the person is compatible with the right to liberty; and**

Article 9(1) of the ICCPR requires that persons not be subject to arrest and detention except as provided for by law, and provided that neither the arrest nor the detention is arbitrary.

As noted above, extradition is an administrative legal process whereby a person may be transferred from one country to another to face prosecution or to serve a prison sentence for offences against the law of the other country. The extradition process in Australia does not involve an assessment of guilt or innocence; it is not a criminal trial. For this reason it would not be appropriate for the evidence to be tested by Australian courts.

The extradition process is provided for by law and is not arbitrary; it is supported by a legal framework which has been designed to be proportionate to the legitimate aim of securing the return of alleged offenders to face justice, noting that extradition offences are serious offences, including terrorism, murder and transnational organised crimes.

- **whether section 6 of the El Salvador regulations, which increases the period in which a person must be brought before a magistrate or eligible Federal Circuit Court judge after being arrested from 45 days to 60 days, is a proportionate limitation on the right to liberty.**

The 60 day period is common to Australia's recent extradition practice, and has been included for a broad range of countries, including for example, the US, Canada, Mexico, Brazil, Croatia and others. This time period takes into account the time required to comply with the requirements of the Extradition Act, namely the complexities of securing the delivery of original documents and translations thereof in the correct form from foreign countries via the diplomatic channel, and the formal acceptance of the request by the Attorney-General. During this 60 day period the person can make an application for bail under section 15 of the Extradition Act, which provides that a person who is arrested under an extradition arrest warrant must be brought as soon as practicable before a magistrate or eligible Federal Circuit Court Judge in the State or Territory in which the person is arrested, and the person may be remanded on bail where there are special circumstances. As noted above, the extradition framework has been designed to be proportionate to the legitimate aim of

securing the return of alleged offenders to face justice, noting that extradition offences are serious offences, including terrorism, murder and transnational organised crimes.

1.83 The committee seeks the advice of the Attorney-General as to the compatibility of the El Salvador regulations and the Extradition Act with the right to equality and non-discrimination. In particular, the committee seeks information as to the safeguards in place to ensure:

- **a person is not extradited where their surrender is sought for the purpose of prosecuting or punishing the person on account of her or his personal attribute that is protected under article 26 of the ICCPR but not listed in section 7 of the Extradition Act; and**
- **a person is not extradited where they may be prejudiced at her or his trial, or punished, detained or restricted in her or his personal liberty, by reason of a personal attribute that is protected under article 26 of the ICCPR but not listed in section 7 of the Extradition Act.**

The Extradition Act includes grounds for refusing surrender if the person may be prejudiced by reason of his or her race, religion, nationality, political opinions, sex or sexual orientation, or where extradition is sought for the purpose of prosecuting or punishing the person on account of any of these factors. This provides a broad basis to refuse extradition where there may be adverse impacts because the person may be discriminated against. The Attorney-General's broad discretion in paragraph 22(3)(f) of the Extradition Act to refuse surrender provides a sufficient basis to refuse extradition in circumstances where there are other concerns about discrimination against a person.

As the Committee points out in its report, the grounds in Article 26 of the ICCPR that are not contained in the Extradition Act are language, colour, national or social origin, birth (although nationality and race are covered), property, other opinion, or other status. Any concerns relating to these additional grounds are more appropriately considered as part of the Attorney-General's general discretion to refuse to extradite a person. Including further grounds would significantly widen the scope for appeals of extradition decisions. For example, 'other status' has no definite meaning and the inclusion of this ground as an extradition objection under the Extradition Act would make the list of discrimination grounds non-exhaustive. This would likely generate significant litigation.

As noted above, I consider that the general discretion is an appropriate and adequate safeguard.

<u>EXTRADITION LEGISLATION AMENDMENT (2017 MEASURES NO. 1) REGULATIONS 2017</u>

<u>Removing India from the list of extradition countries in the Extradition (Commonwealth Countries) Regulations 2010</u>

1.88 The committee seeks the advice of the Attorney-General as to the compatibility of Items 2 and 3 of the Extradition Legislation Amendment (2017 Measure No.1) Regulations with human rights, having regard to the matters discussed at [1.61] to [1.83] above, in particular the:

- **prohibition against torture, cruel, inhuman and degrading treatment;**
- **right to life;**

- **right to a fair hearing and fair trial;**
- **right to liberty; and**
- **right to equality and non-discrimination.**

These matters are addressed above in relation to the *Extradition (El Salvador) Regulations 2017*.

1.89 The committee seeks the advice of the Attorney-General as to whether removing India from the list of 'extradition countries' in the Extradition (Commonwealth Countries) Regulations 2010 is a proportionate limitation on human rights, having regard to the safeguards in that regulation that are not present in the Extradition Act or the Extradition (India) Regulations 2010.

Evidence standard

The Committee identified the change from the 'prima facie' standard to the 'no evidence' standard in relation to the material required to support extradition. The 'no evidence' standard was addressed above in relation to the *Extradition (El Salvador) Regulations 2017*.

Ground for refusal

The Committee identified that the express ground for refusal in the *Extradition (Commonwealth Countries) Regulations 2010* regarding 'unjust, oppressive or too severe a punishment' is not expressly contained in the *Extradition (India) Regulations 2010*. These matters are covered by the general discretion to refuse surrender under paragraph 22(3)(f) of the Extradition Act.

The general discretion also provides a basis to refuse extradition in circumstances where there are concerns about the person's access to a fair trial. These matters are addressed above in relation to the *Extradition (El Salvador) Regulations 2017*.

As noted above, I consider that the general discretion is an appropriate and adequate safeguard.

Amendments to reflect changes made to the Convention on the Physical Protection of Nuclear Material 1979

1.94 The committee seeks the advice of the Attorney-General as to the compatibility of items 2 and 3 of the Extradition Legislation Amendment (2017 Measure No.1) Regulations with human rights having regard to the matters discussed at [1.61] to [1.83] above, in particular the:

- **prohibition against torture, cruel, inhuman and degrading treatment;**
- **right to life;**
- **right to a fair hearing and fair trial;**
- **right to liberty; and**
- **right to equality and non-discrimination.**

These matters are addressed above in relation to the *Extradition (El Salvador) Regulations 2017*.

THE HON PETER DUTTON MP
MINISTER FOR HOME AFFAIRS
MINISTER FOR IMMIGRATION AND BORDER PROTECTION

Ref No: MS18-001251

Mr Ian Goodenough MP
Chair
Parliamentary Joint Committee on Human Rights
S1.111
Parliament House
CANBERRA ACT 2600

Dear Ian,

Thank you for your letters of 28 March 2018 in which further information was requested on the *Identity-matching Services Bill 2018* (Cth) and *Migration (IMMI 18/003: Specified courses and exams for registration as a migration agent) Instrument 2018*.

I have attached my response to the *Parliamentary Joint Committee on Human Rights' Report 3 of 2018* as requested in your letters. The response to the *Identity-matching Services Bill 2018* (Cth) should be considered in conjunction with my letter dated 04 April 2018, which outlined our response to the Chair of the Senate Standing Committee on the Scrutiny of Bills.

I trust the information provided is helpful.

Yours sincerely

26/04/18

PETER DUTTON

Parliament House Canberra ACT 2600 Telephone: (02) 6277 7860 Facsimile: (02) 6273 4144

The *Identity-matching Services Bill* 2018 (the Bill) will authorise the Department to provide new biometric face matching services for a range of fraud prevention, law enforcement, national security, community safety and related activities. The Bill will help to give effect to Australian Government's commitments under the *Intergovernmental Agreement on Identity Matching Services* agreed by the Council of Australian Governments in October 2017.

Committee's Questions

The committee requests the advice of the Minister for Home Affairs as to whether the limitations on the right to privacy contained in the Identity Matching [Services] Bill are reasonable and proportionate measures to achieve the stated objective. This includes information in relation to:

Whether the provisions in the Identity Matching [Services] Bill governing access to facial images and other biometric data are sufficiently circumscribed for each of the identity matching services.

The Bill contains a number of measures to appropriately circumscribe access to data through each of the identity-matching services.

Firstly, the Bill does not authorise any agency other than the Department of Home Affairs (Home Affairs) to collect, use or disclosure identification information. The Bill is primarily intended to provide Home Affairs with legal authority to operate the interoperability hub and to host the National Driver Licence Facial Recognition Solution (NDLFRS).

The Bill does not seek to, nor does it, authorise other agencies to share information through the services. Each agency's use of information it receives through the services will be governed by its own legal authority to collect, use and disclose the information for particular purposes, including any legislated protections that apply to the agency under Commonwealth, state or territory privacy legislation.

By taking this approach, the Bill specifically avoids providing a blanket authorisation for all information-sharing that occurs through the services. Where an agency seeks to obtain information from another agency through the services, both the requesting agency and data-holding agency will need to have a legal basis to share information with the other. This is no different to current data-sharing arrangements, and ensures that the services are only available to those agencies that have a legal basis to share information through them under other legislation.

Secondly, the individual identity-matching services provided for by the Bill have more specific restrictions relevant to the particular service. For example, as noted by the Committee, the Face Identification Service (FIS) will only be able to be used by a specific list of agencies set out in the Bill. The Committee also noted that the Bill provides for the Minister to prescribe further agencies by delegated legislation. However, subclause 8(3) of the Bill restricts this power such that the Minister is only able to prescribe a new authority for access to the FIS if the authority has one or more of the functions that used to be functions of an authority already prescribed in the Bill.

The purpose of subclause 8(3) is to restrict this power to the extent that it is only available to cover situations where one of the agencies already listed in the Bill changes names as a result of machinery of government changes or for other reasons, or where their functions shift to a different authority. As set out in the explanatory memorandum, this provision is intended to supplement, rather than replace, the relevant provisions of the *Acts Interpretation Act 1901*, which already provide for the continuation of provisions naming specific government agencies when a machinery of government change occurs, if those provisions do not apply.

As a result, any substantive change to the breadth or nature of the agencies that have access to the FIS will need to be made by an amendment to the Act, rather than through the making of a rule. This will help to prevent 'scope creep' and will ensure appropriate Parliamentary oversight of any substantive changes to FIS access.

Provision of the FIS is also restricted by paragraph 8(1)(b) of the Bill, which provides that the comparison must be undertaken in the course of an identity or community protection activity covered by subsections 6(2) to 6(6). This specifically excludes two of the identity and community protection activities, namely *road safety activities* (subclause 6(7)), and *verifying identity* (subclause 6(8)).

This restriction has been imposed in recognition of the greater privacy implications of the FIS compared to the other identity-matching services provided for by the Bill. This ensures the provision of the FIS is appropriately circumscribed relative to its privacy impacts.

The other services are also limited in different ways. The Facial Recognition Analysis Utility Service (FRAUS) and the One-Person-One-Licence Service (OPOLS) are both restricted for use only by agencies that provide data into the NDLFRS, which will primarily be state and territory road agencies. This restriction is contained in the definitions of the services:

- For the FRAUS, subparagraph 9(a)(i) provides that a FRAUS relates to a request *made by an authority of a State or Territory that has supplied identification information to a database in the NDLFRS.*
- For the OPOLS, paragraph 12(b) provides that the authority [that requests the service] *issues government identification documents of a particular kind and has supplied identification information…to a database in the NDLFRS*.

In addition, the services only enable comparison against data in the NDLFRS – in the case of the FRAUS, only the data supplied by the same authority making the request (i.e. against their own data), and in the case of the OPOLS, only data relating to identification documents of the same type (i.e. driver licences).

These services are primarily designed to assist road agencies to manage their own data, and improve the integrity of their licence-issuing processes by providing a secure and automated tool to check whether the individual holds licences in other states and territories. As such, they are appropriately circumscribed for these purposes.

The Identification Data Sharing Service (IDSS) is also restricted by its definition, which limits its use to disclosures of identification information between *one authority of the Commonwealth or of a State or a Territory to another authority of the Commonwealth or of a State or a Territory* (paragraph 11(1)(c)). Although this is still quite broad compared to some of the other services, the IDSS can still only be used

for the identity and community protection activities, and agencies using the service must have their own legal basis to share this information and comply with any privacy or information protection laws that apply to them. As with the other services, the Bill is not intended to provide new powers for agencies to share information, but simply to facilitate more automated, auditable and secure information-sharing through the interoperability hub.

The last of the services, the Face Verification Service (FVS), assists users to verify a claimed or known identity by comparing information they have about an individual (often provided by the individual) with a government record matching the same details. It will be available to the broadest range of users, and is the only service that will be available to non-government users. In most cases, the system will return a match/no match response, rather than an image, and never more than one image.

Even so, the Bill contains provisions to ensure that the provision of the service is appropriately circumscribed. In particular, a number of conditions apply to local government and non-government use of the FVS, as set out in subclause 7(3). These include that the verification of an individual's identity is reasonably necessary for the functions or activities of the entity, the individual has given consent for the use and disclosure of their information to verify their identity, the entity resides or carries on activities in Australia, and privacy protections equivalent to those provided by the *Privacy Act 1988 (Cth)* apply to the entity.

Whether the *Privacy Act 1988* (Privacy Act) will apply to the operation of the Hub and, if so, whether it will act as an adequate and effective safeguard noting the various exceptions to the collection, use and disclosure of information under the Privacy Act.

The Privacy Act applies to all 'APP Entities', which includes Home Affairs. The operation of the interoperability hub by Home Affairs will therefore be subject to the Privacy Act, and Home Affairs will manage the hub consistently with its obligations under that Act.

The Privacy Act and the Australian Privacy Principles contained therein provide the privacy architecture for Australian Government entities. A key objective of the Privacy Act is to balance the protection of privacy with the interests of entities in carrying out their lawful and legitimate functions and activities. The adequacy and effectiveness of the privacy safeguards contained in the Privacy Act, including the appropriateness of the exceptions to restrictions on collection, use and disclosure of information under the Privacy Act, have been considered by the Parliament in the development of the Act and subsequent amendments to it. To the extent that various exemptions in the Privacy Act may apply to the operation of the interoperability hub, this is consistent with the application of the Privacy Act across the many entities to which it applies.

In addition, the interoperability hub will be subject to other privacy safeguards under the *Intergovernmental Agreement on Identity Matching Services* (IGA) and the policy and administrative arrangements supporting the services that will increase the overall adequacy and effectiveness of the privacy framework governing the operation of the hub.

For example, under the IGA, the interoperability hub will not retain any facial images or other identity information – it acts purely as a router to transmit information between participating entities. The only data that will be retained by the hub will be

that required for auditing purposes. This 'hub and spoke' design feature is consistent with the 'privacy by design' approach to the identity-matching services, in that it avoids the need for the Department to build a new database combining visa and citizenship, passport and state and territory identification information in one place. Instead, the interoperability hub simply provides an interface to connect end-users with separate databases, enable them to make queries against each of the databases separately but simultaneously. In turn, this minimises the amount of information retained by Home Affairs, as it is not necessary for Home Affairs to retain the information contained in the queries or responses routed through the interoperability hub to and from the databases.

Furthermore, the interoperability hub will be subject to independent penetration and vulnerability tests and security reviews, as well as a range of stringent user access arrangements under a common Face Matching Services Participation Agreement between all participating Commonwealth, state and territory agencies, which will provide a legally binding framework for participation in the services. This includes measures to protect privacy such as a set number of user accounts per agency, user training and accountability requirements, and regular auditing.

Whether the Identity Matching [Services] Bill contains adequate and effective safeguards for the purposes of international human rights law.

Under international human rights law, individuals have a right to privacy, including the right not to be subjected to arbitrary or unlawful interference with their privacy, family, home or correspondence, and the protection of the law against such attacks[1]. However, the right to privacy may be subject to permissible limitations that are authorised by law, are not arbitrary, and which are a necessary and proportionate means of pursuing a legitimate objective.

As set out in the Statement of Compatibility with Human Rights that accompanies the Explanatory Memorandum to the Bill, the Bill engages and limits the right to privacy, but the limitation is permissible on the basis that it is reasonable, necessary and proportionate to achieving the legitimate objectives of each of the services. Privacy safeguards contained in the Bill help to ensure that the limitation in each case is restricted only to that which is necessary to the objectives of the particular service. For example, in relation to the FIS (which has the greatest privacy implications), the Bill imposes additional safeguards including restricting the agencies that can access the service and the activities for which it can be used.

In addition to specific restrictions on the individual services, the Bill also contains further safeguards that help to protect the right to privacy of individuals whose information is shared through any of the services. In particular, clause 21 creates an offence for unauthorised recording or disclosure of information by employees of Home Affairs (including secondees, and contractors working on the NDLFRS or interoperability hub). This creates an effective safeguard against unlawful interference with a person's right to privacy by people who may have access to identification information contained in the NDLFRS or shared through the interoperability hub. Annual reporting on use of the services and a requirement for a review to be commenced within 5 years provide further safeguards to ensure that any arbitrary or unlawful interference is detected, and subject to public scrutiny.

[1] *International Covenant on Civil and Political Rights*, Article 17

The privacy safeguards in the Bill are also supported by a range of further measures under the IGA, the Face Matching Services Participation Agreement referred to above, and an NDLFRS Data-Hosting Agreement, which will provide the framework for Home Affairs to host state and territory data in the NDLFRS. These include annual audits of each participating agency, strict access controls on users of the services, additional authorisation requirements for the FIS, and privacy impact assessments.

Whether, in light of the number, types and sources of facial images and other biometric data that may be collected, accessed, used and disclosed through the Hub and the NDLFRS, these measures are the least rights restrictive approach (including whether having facial images of the vast majority of Australians searchable via the Hub is the least rights restrictive approach and whether there are restrictions as to the sources from which facial images may be collected).

The biometric face matching services that will be provided through the interoperability hub and NDLFRS have been developed to address increasing incidences, and sophistication of, identity misuse and fraud in Australia, which has wide-ranging impacts for individual privacy, as well as law enforcement and national security.

Under the *Intergovernmental Agreement to a National Identity Security Strategy* agreed by the Council of Australian Governments in 2007, the Commonwealth implemented a national Document Verification Service (DVS). The DVS enables government and non-government users to compare the claimed identity information of a customer or client with a government record to verify their identity. The DVS matches key biographic details about the individual and their Australia-issued identifying credentials (such as a passport or driver licence), and provides a 'yes' or 'no' match response.

The DVS is currently used by around one hundred government entities and seven hundred businesses, including all major finance and telecommunications companies, with more than 30 million DVS transactions processed in 2017. The DVS has a limited impact on individual privacy because it only provides for one-to-one verification of a claimed identity, does not return biographic information (users receive a 'yes'/'no' match result only), and operates on a consent basis.

Whilst expanding use of the DVS has made it harder for criminals to use fictitious identities, it is also creating incentives for them to use documents in stolen identities that have genuine biographic details (which will pass a DVS check) combined with a fraudulent photo. The biographic-based DVS cannot detect these fraudulent identities, creating a need for a different solution to tackle the growing use and sophistication of these stolen identities.

The misuse of this personal information for criminal purposes causes substantial harm to the economy and individuals each year. The *Identity Crime and Misuse in Australia Report 2016* prepared by the Attorney-General's Department, in conjunction with the Australian Institute of Criminology, indicated that identity crime is one of the most common and costly crimes in Australia, impacting around 1 in 20 Australians every year (and around 1 in 5 Australians throughout their lifetime), with an estimated annual cost of over $2.2 billion.

In addition to financial losses, the consequences experienced by victims of identity crime can include mental health impacts, wrongful arrest, and significant emotional distress when attempting to restore a compromised identity. In some cases where complete takeover of a victim's identity has occurred, the report indicates that it took victims over 200 hours to obtain new credentials and resolve other issues associated with the compromise of their identity.

Identity crime is also a key enabler of serious and organised crime, including terrorism. Australians previously convicted of terrorism related offences are known to have used fraudulent identities to purchase items such as ammunition, chemicals that can be used to manufacture explosives, and mobile phones to communicate anonymously to evade detection. An operation by the joint Australian Federal Police and New South Wales Police Identity Security Strike Team found that the fraudulent identities seized from just one criminal syndicate were linked to 29 high profile criminals linked to historic or ongoing illicit drug investigations; more than $7 million in losses associated with fraud against individuals and financial institutions; and more than $50 million in funds that were laundered offshore and were likely to be proceeds of crime.

Current methods for verifying an identity or identifying an individual using facial images can be slow, difficult to audit, and often involve manual tasking between requesting agencies and data holding agencies. In some cases, this can take several days or longer. Given the significant impact that identity crime has on individuals and on the safety and security of Australians more broadly, it is imperative that government agencies, and private sector organisations (which operate at the frontline of day-to-day identity verification), have access to the modern tools necessary to continue to detect and prevent identity fraud, including using facial matching.

The face matching services that will be supported by the Bill have been developed to balance the need to address this threat with the privacy rights of individual Australians. The design of the services and the systems that support them, including the 'hub-and-spoke' model of service delivery through the interoperability hub, ensure that the services take the least rights restrictive approach to addressing the serious issue of identity fraud.

By delivering the services through the establishment of a central hub that connects to a number of separate databases, the Government has specifically avoided a need to develop a single, central database of identification information. In addition, although the Commonwealth is hosting a national driver licence database (the NDLFRS) to centralise driver licence information for the purpose of the services, under the IGA the Commonwealth will not have direct access to view the data stored within the national database. State and territory road agencies will provide their data into partitioned sections of the database, and will retain control over access to that data.

Furthermore, users access the services on a query and response basis, where a user submits query information into the hub interface, which is then transmitted to the relevant database/s for matching with the results returned to the user. This ensures that users only have access to the information that is relevant to their query, and cannot go looking for additional information directly within the databases. To provide a further safeguard for the information transmitted through the hub, the hub itself does not store any of the identification information contained in the query or the response.

Alternative options to the provision of the face matching services through the interoperability hub include a continuation of the status quo, through which agencies that need to share information for identity verification or identification purposes do so through existing manual methods of data-sharing – via hard copy or email or other electronic transmission. These ad-hoc methods vary amongst agencies, as does the security and auditability of the transmissions. By providing a single tool through which participating agencies can share identification information, the interoperability hub will improve the consistency of data-sharing and enable it to be more easily monitored, managed and audited.

The Government acknowledges that the face matching services may cause privacy concerns for some individuals. However, the services and the systems that support them have been designed to minimise those impacts and improve the security and accountability of data-sharing between participating agencies. The identification information being made available for matching through the services is already held by government across multiple agencies, and shared between agencies consistent with their legislative authorities. The face matching services will enable agencies to use that information more securely and effectively to protect Australians from national security and criminal threats, identity crime, and other threats, in the least rights restrictive way.

The Committee has also asked whether there are restrictions on the sources from which facial images may be collected. The databases to which the interoperability hub will initially connect will be the visa and citizenship database maintained by Home Affairs, the passports database maintained by the Department of Foreign Affairs and Trade, and the NDLFRS to be hosted by Home Affairs, containing replicated state and territory licence information. Due to some states and territories holding information about other licence types within the same databases as their driver licence information (for example, marine licences or proof of age cards), this information may also be replicated in the NDLFRS, where there is a legal basis to do so.

Although the Bill does not explicitly restrict the connection of other databases to the interoperability hub in future, the availability of other data sources would, as with all aspects of the services, be subject to the information-sharing authorisations of participating agencies. That is, an agency providing access to its database through the hub would need the legal authority to share the information with other agencies for the purposes for which the face matching services are provided, and a participating agency wishing to access the information would also need to have a legal basis to do so.

Whether the hub could be connected to other databases in the future will also be limited by the general purpose for which the face matching services are being provided, and the practicalities of facial recognition, which requires high quality images to achieve the most accurate matching results. The services are intended to assist participating agencies to determine the genuine identity of an individual, based on facial image comparison. This is why the initial databases to which the hub will connect are databases of identification information related to primary identification documents containing facial images. These databases provide a reliable source of identification information that can assist agencies to confirm a person's true identity.

The nature of the processes for obtaining these identification documents also ensures that the majority of facial photographs in these databases are of sufficiently

high quality for facial recognition purposes. Facial recognition software relies heavily on the availability of high quality, front-on, unobscured facial images, to enable the most accurate matching. The integrity of the face matching services is therefore directly related to the quality of the images in the databases used for matching. This practical issue will likely limit the types of databases that may be connected to the services in future.

Whether the measures are a proportionate limitation on the right to privacy with reference to the potential relevance of international jurisprudence such as that outlined at [1.148] – [1.149].

As set out above, and in more detail in the Statement of Compatibility with Human Rights included in the Explanatory Memorandum to the Bill, the Bill contains a range of measures to ensure that the provision of each of the face matching services is proportionate to the legitimate objectives it pursues. Respectfully, the case law cited by the Committee at [1.148] – [1.149] of its Report does not alter that fact.

A number of the cases referenced[2] deal with the matter of collection of biometric information directly from members of the public and the retention of that information for law enforcement purposes. With reference to these cases, it is important to note that the Bill does not seek to govern the collection of identification information, including biometrics, from individuals, nor the handling of identification information by agencies other than the Department of Home Affairs (as the operator of the systems authorised by the Bill).

The face matching services authorised by the Bill are simply tools to enable agencies to more securely share and match information with each other. Participating agencies must have their own legal basis to collect, use and disclose the information both when using the services as a requesting agency or an agency providing access to its data. This also applies to their collection of the primary biometric information from an individual (such as the collection of CCTV footage or passport photos).

As part of the existing legal framework that already applies to the collection, use and disclosure of identification information by agencies that will participate in the face matching services, agencies must comply with data retention regimes that apply to them with respect to the storage and destruction of that information. This will continue to be the case with respect to identification information an agency obtains through using the services. The Face Matching Services Participation Agreement (mentioned above) that will govern participation in the services will reiterate this by requiring agencies to only retain information for as long as they require it for the purpose for which it was collected, or for the minimum period required by law.

The Committee also refers to European cases dealing with retention of communications data, and its own comments on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014[3]. The issues raised

[2] *S and Marper v United Kingdom*, European Court of Human Rights Applications 30562/04 and 30566/04 (2008), *NK v Netherlands*, UN Human Rights Committee CCPR/C/120/D/2326/2013 (2017), and *Wood v Commissioner of Police for the Metropolis* [2009], United Kingdom Court of Appeal EWCA Civ 414 (2009).

[3] *Secretary of State for the Home Department v Watson MP & Ors* [2018] EWCA Civ 70 (30 January 2018), *Digital Rights Ireland Limited v Minister for Communications, Marine and Natural Resources & Others* and *Seitlinger and Others* [2014] EUECJ C-293/12, and Parliamentary Joint Committee on Human Rights' *Fifteenth Report of the 44th Parliament* (14 November 2014).

in relation to metadata largely relate to concerns about the retention of significant amounts of data not previously retained, and the purposes for which it can be accessed.

As set out above, the Bill is not intended to deal with the collection and retention of data from individuals – it provides for information-sharing between agencies and organisations. The data intended to be transmitted through the services is information that is already collected and retained by participating agencies, and shared in accordance with their legislative authority to do so. In this way, it is not analogous with the establishment of large databases of new metadata not already retained.

Whilst it is possible that identification information obtained through the services may reveal some limited additional information about a person (which the Committee raises concerns about at [1.147]), this must be considered in the context of the legitimate objectives that the Bill pursues. In particular, the face matching services facilitated by the Bill are designed to assist in verification of identity or the identification of unknown individuals in the context of the identity and community protection activities set out in clause 6 of the Bill. Given the services are for use in identification and identity verification, the disclosure of some identifying information about an individual is unavoidable.

However, the Bill imposes a number of restrictions to ensure that the disclosure of identification information is proportionate to its objectives. This includes restricting the types of identification information that Home Affairs is authorised to collect, use and disclose in providing the services (and specifying particular information that is not authorised because it is not relevant to identification or identity verification), restricting access to the FIS (which discloses identification information about more than one individual in response to a query), and imposing conditions on local government and private sector access to the services so that they can only obtain identification information through the services with the consent of the individual concerned.

The Committee also notes that the European cases relating to communications data raise the issue of access to information without a requirement for prior review by a court of independent administrative authority. The Bill is not seeking to authorise participating agencies other than Home Affairs to access identification information through the services. Those agencies will need to have their own legal basis to do so. Many participating agencies already have a legal basis to share this information, in most cases without prior review by a court or independent administrative authority. It is not appropriate for the Bill to impose this additional requirement on participating agencies – this would be a matter for other legislative processes relevant to those agencies, or their particular jurisdictions.

For the reasons set out above, and in the Statement of Compatibility with Human Rights, the measures in the Bill are a proportionate limitation on the right to privacy notwithstanding the referenced jurisprudence.

The extent to which historical facial images will be subject to the Hub, and whether the Identity Matching [Services] Bill provides adequate and effective protection against misuse and in respect of vulnerable groups.

Historical facial images may be contained in databases to which the hub connects. However, specific safeguards exist to protect people with legally assumed or

protected identities, and the nature of the services will also limit the risk of revealing a former identity in many cases.

The Bill provides specifically for Home Affairs to share information for the purposes of protecting individuals with legally assumed or protected identities. This will help to protect individuals who have been issued with an assumed or protected identity by an authorised Commonwealth, state or territory agency, from being inadvertently identified. Data about these individuals contained in each database connected to the interoperability hub is sanitised directly by the agencies responsible for the assumed/protected identity prior to agencies having access to the database through the FIS (which allows for identification of individuals without knowing their name).

In relation to other vulnerable groups that may have changed their identities but do not have a legally assumed or protected identity, the structure of the services will help to prevent their former identities from being revealed in most circumstances. For example, the most widely available service, the FVS, only provides for one-to-one verification of an identity. In order to receive a match, the user will need to provide biographic details about the individual (such as their name and date of birth), which will then be checked against one or more databases and results only returned if the biographic details match a record in the database. Although some databases may contain, and return, known alias information, this will only be returned to certain users with a need for that information (such as police) based on their user access arrangements.

Access to the FIS, which allows for identification of an unknown individual, is much more restricted to protect the privacy of individuals whose details may be returned because of a possible facial match with a person of interest. Only a prescribed set of law enforcement, national security and anti-corruption agencies will have access to this service, and within those agencies access will also be restricted to users with a need to use it and training in facial recognition. This will help to ensure that if an individual's former identity is revealed through these services, only those with a strict need to know that information will have access to it. Other strict access controls on the FIS, including a requirement to enter the particular purpose for which it is being used in each instance, will help to prevent any misuse of the service to identify a person other than for the activities provided for by the Bill.

Under the Face Matching Services Participation Agreement, FIS access is also subject to additional supervision and authorisation requirements. All users of the FIS must be monitored by a supervising officer when using the service. In addition, a more senior authorising officer (at Australian Public Service Executive Level 2/Director level or equivalent) must approve certain FIS requests, including all queries for community safety activities, queries relating to a person under the age of 18 years, and queries to identify witnesses to a crime.

In addition, the NDLFRS, which is the only database being built specifically for use in these services, is designed only to rely on the most recent image of an individual for facial matching. In addition, this data will be updated daily through direct connections between the NDLFRS and the state and territory databases from which the data is drawn, to ensure that the images being used for matching are the most up-to-date.

These controls provide adequate and effective protection for vulnerable groups by ensuring that only those with a need to identify an individual for specific activities will have access to identification information through the services. Although it may be possible that the results of a query may reveal sensitive information about an

individual, it is not possible to entirely avoid this without undermining the purpose for which the services have been developed, which is to assist with identifying and verifying the identity of individuals. The Bill, and the design of the services that will be facilitated by it, puts in place a regime of strict controls and tiered safeguards that appropriately balance the need to protect vulnerable groups with the effectiveness of the services as a tool for identity resolution.

In relation to the Face Identification Service (FIS), whether allowing images of unknown individuals to be searched and matched against government repositories of facial images through the Hub is the least rights restrictive approach to achieve the stated objective.

The FIS is designed to assist Australia's law enforcement, national security and anti-corruption agencies to identify unknown persons of interest in the course of their identity fraud prevention and detection activities, and their national security, law enforcement, protective security and community safety activities. This could include, for example, identifying a suspect from a still image taken from CCTV footage of an armed robbery, identifying an individual suspected to be involved in terrorist activities or in siege situation, or determining if a person of interest is using multiple fraudulent identities.

As detailed above, many of these agencies already share this information, and can request matching against various databases. However, this currently occurs on an ad-hoc basis which can be slow and difficult to audit. The Bill does not seek to expand the legal basis on which these agencies are authorised to share information with each other – they will still need to have a separate legal basis to do so before using the services. The services provide these agencies with a faster, secure tool for transmitting these requests to multiple data sources at once and receiving the results as quickly as possible, with a clear audit trail for accountability purposes.

In many law enforcement and national security scenarios, it is imperative that a person of interest is identified quickly to prevent a new or ongoing threat to the public. In the current environment, this is often not possible, and the various different methods agencies use to share information with each other are inefficient and make auditing and oversight difficult. By providing agencies with a tool to help them resolve the identity of a person of interest quickly, and in an auditable way, the services will help to ensure that these agencies can operate effectively and continue to keep Australians safe, whilst being accountable to the Australian public.

THE HON JULIE BISHOP MP

Minister for Foreign Affairs

Mr Ian Goodenough MP
Chair
Parliamentary Joint Committee on Human Rights
PO Box 6100
CANBERRA ACT 2600

Dear Chair

Thank you for your letter of 28 March 2018 regarding the human rights compatibility of the *Australian Passports Amendment (Identity-matching Services) Bill 2018*.

I attach a response to the request for information from the Parliamentary Joint Committee on Human Rights (the Committee), as set out in the Committee's *Report 3 of 2018*.

I note that the Committee has requested similar advice from my colleague, the Minister for Home Affairs and the Minister for Immigration and Border Protection, on the *Identity-matching Services Bill 2018*. In most cases, the information requested applies equally to both Bills; we have coordinated our responses where appropriate.

Should you require further information, the responsible officer for this matter in my Department is Mr Stephen Gee, Assistant Secretary, Passport Policy and Integrity Branch, who can be contacted on (02) 6261 3075.

I trust this information is of assistance.

Yours sincerely

Julie Bishop

+61 2 6277 7500 Parliament House, Canberra ACT 2600, Australia foreign.minister@dfat.gov.au

Responses to questions from the Parliamentary Joint Committee on Human Rights in its *Report 3 of 2018* in relation to the *Australian Passports Amendment (Identity-matching Services) Bill 2018*

The Committee asked the advice of the Minister as to:

- **whether the limitation on the right to privacy by the measures in the *Passport Amendment Bill* are a reasonable and proportionate measure to achieve the stated objective. This includes information in relation to:**
  - **whether the *Privacy Act 1988* (Privacy Act) will apply to DFAT's disclosure of photographs and biographical information and, if so, whether it will act as an adequate and effective safeguard for the purposes of international human rights law noting the various exceptions to the collection, use and disclosure of information under the Privacy Act;**
  - **whether the *Passport Amendment Bill* contains adequate and effective safeguards and is sufficiently circumscribed for the purposes of international human rights law;**

The Privacy Act applies to all 'APP entities', which includes the Department of Foreign Affairs and Trade (DFAT). DFAT's disclosure of photographs and biographical information will therefore be subject to the Privacy Act. Nothing in the Bill exempts DFAT from these requirements.

The Privacy Act and the Australian Privacy Principles contained therein provide the privacy architecture for Australian Government agencies. The adequacy and effectiveness of the privacy safeguards contained in the Privacy Act, including the appropriateness of the exemptions to restrictions on collection, use and disclosure of information under the Privacy Act, have been considered by the Parliament in the development of the Act and subsequent amendments to it. To the extent that various exemptions in the Privacy Act may apply to DFAT's disclosure of photographs and biographical information, this is consistent with the application of the Privacy Act to the many entities that are subject to it.

The Privacy Act is not the only legislation relevant to the collection, use and disclosure of photographs and biographical information by DFAT in the passports context. Australian Privacy Principle 6.2(b) provides, relevantly, that personal information (including sensitive information) may be used and disclosed for a secondary purpose (to the purpose for which the information was collected, in this case being the processing of an application for an Australian travel document) where it is required or authorised by or under an Australian law.

The *Australian Passports Act 2005 (Cth)* and *Australian Passports Determination 2015 (Cth)* relevantly provide the primary legislative framework for the collection, use and disclosure of passport-related personal information and sensitive information. The *Australian Passports*

Act 2005 (Cth) and its related Australian Passports Determination 2015 (Cth) set out various permitted collections, uses and disclosures of personal information and sensitive information in the passports context and already provide a legal basis, although not sufficiently workable, for most of the types of disclosures envisaged by DFAT's participation in the biometric face matching services. The primary intention of the Bill is to augment into one, workable, comprehensive legal basis the various existing, but fragmented, legal bases that currently exist to permit disclosures of passport-related information (addressed below).

The Bill provides for DFAT's participation in identity-matching services that will be subject to other privacy safeguards under the Intergovernmental Agreement on Identity Matching Services (IGA). In addition, the policy and administrative privacy safeguards, including requirements for privacy impact assessments before agencies access the services and compliance audits, will help to ensure the use of the services remains proportionate to the need, and prevent any misuse of identification information.

The principle governing these arrangements is that the minimum necessary information is disclosed to meet the legitimate purpose of the services. The IGA provides that strict privacy controls, accountability and transparency must apply to all the services. Within this framework, data-holding agencies retain discretion to determine specific purposes for which, entities to which, and other circumstances under which, they make their data available through the services.

These and other privacy, accountability and transparency measures provide appropriate safeguards against unnecessary impositions on the right to privacy as a result of the Minister making Australian travel document data available for all the purposes of, and by the automated means intrinsic to, the services.

The Privacy Act, the *Australian Passports Act 2005 (Cth)* and the *Australian Passports Determination 2015 (Cth)* already provide various legal bases to cover DFAT's disclosures of passport-related personal information and sensitive information to agencies and organisations participating in the biometric face matching services. However, legal complexities inherent to applying various existing legal bases in the context of the biometric face matching services (including the diverse nature of participating organisations and the multiple purposes for disclosure) means the only practical way for DFAT to participate in the biometric face matching services as a data holding agency is to augment the various existing legal bases for disclosure into a single, comprehensive legal basis for disclosure for the purposes of participating in the biometric face matching services, as is proposed by the Bill.

The Bill's provision for certain automated decision-making in relation to passport-related information disclosures is intended to supplement DFAT's current ability to make manual decisions to disclose personal or sensitive information so as to allow DFAT's participation in the proposed automated 'hub and spoke' model inherent to the biometric face matching

services. The Department of Home Affairs has outlined separately the automated nature of the biometric face matching service's operation, and the reasons for this.

The safeguards inherent to the use, collection and disclosure of passport-related personal and sensitive information have already been assessed as adequate and effective by parliament in the context of the *Australian Passports Act 2005 (Cth)* and its related *Australian Passports Determination 2015 (Cth)*. The Bill augments the existing legal framework. As such, those privacy safeguards already assessed as adequate and effective in the context of disclosures of passport information will continue to be adequate and effective.

- **whether, in light of the number, types and sources of facial images and other biometric data that may be shared and matched, these measures represent the least rights restrictive approach to achieving the stated objectives (including whether having facial images of the vast majority of Australians searchable via the identity matching services is the least rights restrictive approach);**

The biometric face matching services have been developed to address increasing incidences, and sophistication of, identity misuse and fraud in Australia, which has wide-ranging impacts for individual privacy, as well as law enforcement and national security.

Robust identity-checking practices have significant benefits for individuals and for the community. They help to secure the legitimate identities of individuals by enabling agencies and organisations to detect and prevent the use of stolen, fake or fraudulent identity documentation.

The use of fraudulent identities is also a key enabler of organised crime and terrorism. Australians previously convicted of terrorism-related offences are known to have used fake identities to purchase items such as ammunition, chemicals that can be used to manufacture explosives, and mobile phones to communicate anonymously to evade detection.

In addition to combating identity and related crimes, there are a range of other situations in which identity verification is essential to law enforcement, national security and community safety. This may include verifying the identity of a person suspected of committing a criminal offence, a person seeking authorisation to access a government facility, or a person who is believed to be a missing person. In circumstances such as these, there is a clear need to be able to verify the person's identity in order to protect the community or the individual themselves.

Many agencies and organisations already have data-sharing arrangements for the purpose of manual facial matching. However, these arrangements can be ad-hoc, often relying on manual processes, may not be secure and may be difficult to audit. By contrast, the services will be delivered through an interoperability hub. The hub will capture audit trail information of all services, to support accountability and transparency measures including regular audits and annual reporting.

The identity-matching services will therefore provide a fast and secure tool for identity verification by government and non-government authorities in support of the legitimate objectives of combatting identity crime and supporting national security, law enforcement and community safety. DFAT's participation in the services are necessary to support these objectives because current identity verification practices are inadequate to deal with sophisticated fraudulent identity documents, and to support fast, secure and auditable information-sharing.

Where national security or law enforcement agencies have information about potential threats, it is essential that they can act quickly and efficiently to assess the nature of the threat, including identifying any individuals involved. This is particularly important where agencies may not have sufficient information about the known identity of the individual to verify their identity using the services. This may occur where the agency has a facial image of a suspect but no other identification information about the individual.

There is a clear need for government and private sector service providers to improve their identity-verification processes to ensure they can continue to detect these increasingly sophisticated fraudulent identity documents. The services, and DFAT's participation in them, will assist with this by ensuring that the use of a wider range of fraudulent identification documents can be prevented in a fast, automated and secure way.

The Government acknowledges that the face matching services have privacy implications for individuals. However, the services and the systems that support them have been designed to minimise those impacts and improve the security and accountability of data-sharing between participating agencies. The identification information being made available for matching through the services is already held by government across multiple agencies, and shared between agencies consistent with their legislative authorities and legal frameworks. The face matching services will enable agencies to use that information more securely and effectively

to protect Australians from national security and criminal threats, identity crime, and other threats, in the least rights restrictive way.

- **whether the measure is a proportionate limitation on the right to privacy with reference to the potential relevance of international jurisprudence such as that outlined at [1.148]-[1.149];**

As set out above, the Bill contains a range of measures to ensure that the limitation on the right to privacy arising from DFAT's participation in the identity-matching services is proportionate to the legitimate objectives it pursues. Respectfully, the case law cited by the Committee at [1.148] – [1.149] of its Report does not alter that fact.

A number of the cases referenced deal with the matter of collection of biometric information directly from members of the public and the retention of that information for law enforcement purposes. The identity-matching services that the Bill allows DFAT to participate in are simply tools to enable agencies to more securely disclose (and collect) information to each other.

As part of the existing legal framework that already applies to the collection, use and disclosure of identification information in the passport context, DFAT will still have to comply with data retention regimes that apply to it with respect to the storage and destruction of that information.

Furthermore, the services will be subject to a range of stringent user access arrangements under a common Face Matching Services Participation Agreement between all participating Commonwealth, state and territory agencies, which will provide a legally binding framework for participation. This will include, *inter alia*, requiring agencies to only retain information for as long as they require it for the purpose for which it was collected, or for the minimum period required by law.

The Committee also refers to European cases dealing with retention of communications data, and its own comments on the *Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014*. The issues raised in relation to metadata largely relate to concerns about the retention of significant amounts of data not previously retained, and the purposes for which it can be accessed.

As set out above, the Bill is not intended to deal with the collection and retention of data from individuals – it provides for information-sharing between DFAT and other participating agencies. The data to be transmitted through the services is information that DFAT will have already collected from individuals with their consent and retained. In this way, the services

are not analogous with the establishment of large databases of new metadata not already retained.

As each data holding agency, including DFAT, will retain control over the data it holds (including ensuring adequately information security measures are in place pursuant to Australian Privacy Principle 11), no new data mining or metadata issues should arise other than those which already exist in relation to DFAT's collection, use and disclosure of passport-related information under existing legal authority.

Whilst it is possible that identification information obtained through the services may reveal some limited additional information about a person (which the Committee raises concerns about at [1.147]), this must be considered in the context of the legitimate objectives that the Bill pursues. In particular, the face matching services that the Bill allows DFAT to participate in are designed to assist in verification of identity or the identification of unknown individuals in the context of the identity and community protection activities. Given the services are for use in identification and identity verification, the disclosure of some identifying information about an individual is unavoidable.

The Committee also notes that the European cases relating to communications data raise the issue of access to information without a requirement for prior review by a court of independent administrative authority. The Bill is not seeking to authorise participating agencies to "access" DFAT's identification information through the services. No broad "access" will be possible under the services that is not consistent with the hub and spoke model under which participating data holding agencies maintain control over their data holdings. Rather, a request for disclosure of certain information will be made to DFAT by a requesting agency and DFAT will either disclose that information or not pursuant to pre-agreed conditions. Those agencies requesting information from DFAT will need to have their own legal basis to collect information that DFAT discloses to it. Most (if not all) participating agencies already have a legal basis to collect this information from DFAT, in most cases without prior review by a court or independent administrative authority. It is not appropriate for the Bill to impose this additional requirement on participating agencies – this would be a matter for other legislative processes relevant to those agencies, or their particular jurisdictions.

For the reasons set out above, and in the Statement of Compatibility with Human Rights, I consider that the measures in the Bill are a proportionate limitation on the right to privacy notwithstanding the referenced jurisprudence.

- **the extent to which DFAT's historical facial images will be subject to the identity matching services, and whether the Passport Amendment Bill or other Australian laws provide adequate and effective protection against misuse and in respect of vulnerable groups; and**

Acknowledging the importance of providing adequate and effective protection against misuse and in respect of vulnerable groups, DFAT will only provide access to individuals' most recent facial images through the services.

In addition, the Department of Home Affairs' Identity-Matching Services Bill 2018 provides specifically for Home Affairs to share information for the purposes of protecting individuals with legally assumed or protected identities. This will help to protect individuals who have been issued with an assumed or protected identity by an authorised Commonwealth, state or territory agency, from being inadvertently identified. Data about these individuals contained in each database connected to the interoperability hub is sanitised directly by the agencies responsible for the assumed/protected identity prior to agencies having access to the database through the FIS (which allows for identification of individuals without knowing their name).

In relation to other vulnerable groups that may have changed their identities but do not have a legally assumed or protected identity, the structure of the services will help to prevent their former identities from being revealed in most circumstances. For example, the most widely available service, the FVS, only provides for one-to-one verification of an identity. In order to receive a match, the user will need to provide biographic details about the individual (such as their name and date of birth), which will then be check against one or more databases and results only returned if the biographic details match a record in the database. Although some databases may contain, and return, known alias information, this will only be returned to certain users with a need for that information (such as police) based on their user access arrangements.

Access to the FIS, which allows for identification of an unknown individual, is much more restricted to protect the privacy of individuals whose details may be returned because of a possible facial match with a person of interest. Only a prescribed set of law enforcement, national security and anti-corruption agencies will have access to this service, and within those agencies access will also be restricted to users with a need to use it and training in facial recognition. This will help to ensure that if an individual's former identity is revealed through these services, only those with a strict need to know that information will have access to it. Other strict access controls on the FIS, including a requirement to enter the particular

purpose for which it is being used in each instance, will help to prevent any misuse of the service to identify a person other than for the activities provided for by the Bill.

These controls provide adequate and effective protection for vulnerable groups by ensuring that only those with a need to identify an individual for specific activities will have access to identification information through the services. Although it may be possible that the results of a query may reveal sensitive information about an individual, it is not possible to entirely avoid this without undermining the purpose for which the services have been developed, which is to assist with identifying and verifying the identity of individuals. The identity-matching services will have in place a regime of strict controls and tiered safeguards that appropriately balance the need to protect vulnerable groups with the effectiveness of the services as a tool for identity resolution.

- **in relation to the Face Identification Service (FIS), whether allowing images of unknown individuals to be searched and matched against DFAT facial images through the Hub is the least rights restrictive approach to achieve the stated objective.**

The FIS is designed to assist Australia's law enforcement, national security and anti-corruption agencies to identify unknown persons of interest in the course of their identity fraud prevention and detection activities, and their national security, law enforcement, protective security and community safety activities. This could include, for example, identifying a suspect from a still image taken from CCTV footage of an armed robbery, identifying an individual suspected to be involved in terrorist activities or in siege situation, or determining if a person of interest is using multiple fraudulent identities.

In recognition of the greater privacy implications of the FIS, it will only be able to be used by a restricted and specific list of agencies set out in the Department of Home Affairs' *Identity-Matching Services Bill 2018*. Any substantive change to the breadth or nature of the agencies that have access to the FIS will need to be made by an amendment to the Act, rather than through the making of a rule. This will help to prevent 'scope creep' and will ensure appropriate Parliamentary oversight of any substantive changes to FIS access.

Many of these agencies already share this information, and can request matching against various databases. However, this currently occurs on an ad-hoc basis which can be slow and difficult to audit. DFAT's participation in the identity-matching services will provide it with a

faster, secure tool for transmitting these requests to multiple data sources at once and receiving the results as quickly as possible, with a clear audit trail for accountability purposes.

In many law enforcement and national security scenarios, it is imperative that a person of interest is identified quickly to prevent a new or ongoing threat to the public. In the current environment, this is often not possible, and the various different methods agencies use to share information with each other are inefficient and make auditing and oversight difficult. By providing agencies with a tool to help them resolve the identity of a person of interest quickly, and in an auditable way, the services will help to ensure that these agencies can operate effectively and continue to keep Australians safe, whilst being accountable to the Australian public.

THE HON ALEX HAWKE MP
ASSISTANT MINISTER FOR HOME AFFAIRS

Ref No: MS18-001844

Mr Ian Goodenough MP
Chair
Parliamentary Joint Committee on Human Rights
S1.111
Parliament House
CANBERRA ACT 2600

Dear Mr Goodenough

Thank you for your letters of 9 May 2018 in which further information was requested on the:

- Home Affairs Legislation Amendment (Miscellaneous Measures) Bill 2017 (the Home Affairs Legislation Amendment Bill); and
- Migration (IMMI/003: Specified courses and exams for registration as a migration agent) Instrument 2018 [F2017L01708] (the Migration Instrument).

My response to both requests are attached.

I trust the information provided is helpful.

Yours sincerely

ALEX HAWKE

24 / 5 / 2018

Parliament House Canberra ACT 2600 Telephone: (02) 6277 4430 Facsimile: (02) 6277 8522

Migration (IMMI 18/003: Specified courses and exams for registration as a migration agent) Instrument 2018

Committee's Comment

- ***How the measures are effective to achieve (that is, rationally connected to) the stated objectives; and***

- ***Whether the measures are reasonable and proportionate to achieving the stated objectives of the instrument (including how the measures are based on reasonable and objective criteria, whether the measures are the least rights-restrictive way of achieving the stated objective and the existence of any safeguards).***

The Department seeks to ensure that the migration agent industry is able to service a clientele that may have little or no English language capability. The capacity of a migration agent to convey instructions and information to and from the Department on behalf of a vulnerable client is often critical to the outcome of the visa application.

The duties of migration agents include, not just the completing of forms and the handling of funds on behalf of visa applicants, but also interpretation of complex legislation and its application to the circumstances of a particular applicant. Migration agents are also required to provide clear advice and information, prepare detailed submissions and review of visa applications provided for in the *Migration Act* 1958 (Cth).

The current legislative instrument states that if a person is not in a class of persons specified, an English language proficiency exam is required to be completed. In order for an individual to be exempt from sitting the English language exam, the individual must have been resident in one of the specified countries (Australia, New Zealand, United Kingdom, Republic of Ireland, United States of America, Republic of South Africa or Canada) for the duration of the specified schooling. This is similar to previous legislative instruments introduced in 2012 (FR2012L01932 IMMI 12/097 and prior to that F2012L01343 IMMI 12/035) which also included the specified class of persons.

The Department does not consider the specified class of persons being exempt from undergoing the English language exam as unreasonable or disproportionate. Requiring migration agent applicants who have not completed educational requirements whilst being resident in the five specified countries to complete the English language exam, is rationally connected to the legitimate aim of ensuring migration agents are able to convey instructions and information to, and from, the Department on behalf of their clients.

The New Zealand Immigration Advisers Authority also requires educational requirements to be delivered in the English language and completed while applicants are living in the specified countries (New Zealand, Australia, Canada, Ireland, UK and the US), in their Competency Standard 5.

Similarly, to Australia, English is the common language (ie the majority of the population are native English speakers) in the USA, UK, Canada, Ireland and New Zealand. According to publically available information in 2015, 54 sovereign states and 27 non-sovereign entities had English as an official language, however only six had English as the common language (Australia, USA, UK, Canada, Ireland and New Zealand). A common language in any given country gives prominence over other languages spoken inside the country by the people. Often it is one that is spoken by the majority of the population of the country (e.g. Australia, USA). Therefore it is considered by the Department that people from the specified countries are more likely to meet the English language requirement.

The intended purpose of this requirement is to reduce the unnecessary regulatory burden on migration agent applicants who *were* educated in English in one of the specified countries whereby the need for them to undertake English testing is unnecessary duplication. The Department's recognition of English as a 'common language' in these countries and acknowledgment that a level of education in English contributes to higher English language proficiency, achieves a balance between the necessity of migration advice standards assurance and reduction of regulatory burden.

The 2007-08 Review of Statutory Self- Regulation of the Migration Advice Profession (the Review) recommended that English language proficiency equivalent to an IELTS score of 7 should be the required level of English proficiency for both new and repeat applicants for registration as a migration agent (recommendation 16).

The Department relies on both the specified countries and the fact that individual's education was conducted in English as a reliable assurance that the potential migration agent will have English language proficiency equivalent to the score of IELTS 7, and therefore does not need to be subject to over regulation through English testing.

Senator the Hon Matthew Canavan

Minister for Resources and Northern Australia

Ian Goodenough MP
Chair
Parliamentary Joint Committee on Human Rights
Parliament House
CANBERRA ACT 2600

22 MAY 2018

human.rights@aph.gov.au

Dear Mr Goodenough Ian,

Thank you for your letter of 9 May 2018 concerning comments made by the Parliamentary Joint Committee on Human Rights in its Report 4 of 2018 on the recently introduced proposed legislation: Offshore Petroleum and Greenhouse Gas Storage Amendment (Miscellaneous Amendments) Bill 2018.

You requested a response from me by 23 May 2018 in relation to particular aspects of the proposed legislation and its human rights compatibility.

My detailed response addressing the Parliamentary Joint Committee's concerns is attached.

Yours sincerely

Matthew Canavan

Encl. (1)

Response to Report 4 of 2018 of the Parliamentary Joint Committee on Human Rights in relation to comments on the Offshore Petroleum and Greenhouse Gas Storage Amendment (Miscellaneous Amendments) Bill 2018

Regulatory Context

The task of regulators of the offshore resources industry is difficult given the remote location and high hazard nature of the industry's key operations. For this reason, providing effective and comprehensive compliance and enforcement tools to the regulator is vital in order to deliver human health and safety and environmental protection outcomes. Furthermore and of relevance in consideration of a human rights protection context, it is regulation pertaining, by and large, to large multinational companies as opposed to individuals. The companies who participate in this industry are well resourced, sophisticated and voluntarily engaging in activities for profit.

Offence Specific Defences

The Offshore Petroleum and Greenhouse Gas Storage Amendment (Miscellaneous Amendments) Bill 2018 (the Bill) contains a number of offence provisions which have corresponding offence specific defences:

- it is a defence to the offence of breaching a direction given by NOPSEMA, if the defendant proves that they took all reasonable steps to comply with the direction (the breach of directions defence); and
- it is a defence to the offence of refusing or failing to do anything required by a 'well integrity law' if the defendant proves that it was not practicable to do that thing because of an emergency prevailing at the relevant time (the well integrity defence).

These defences operate as optional exceptions to the criminal responsibility regime established under the *Offshore Petroleum and Greenhouse Gas Storage Act 2006* (the Act). Both of these defences are already substantively contained in the Act:

- Breach of Directions Defence: The inclusion of the breach of directions defence in the current Bill represents an expansion of an existing defence (section 584 of the Act) to reflect new measures in the Bill relating to the transfer of regulatory responsibility for greenhouse gas operations from the Minister to NOPSEMA.
- Well Integrity Defence: The inclusion of the well integrity defence is a mirrored application to a well integrity law of an existing defence for a failure to comply with OHS (clause 92 of Schedule 3) and environmental management laws (clause 18 of Schedule 2A). This is in connection with the measure in the Bill to create a new Schedule 2B to provide a complete and comprehensive suite of compliance powers relating to the well integrity function, which was transferred to NOPSEMA in 2011.

The committee requests the advice of the minister as to:

- **whether the measure is aimed at achieving a legitimate objective for the purposes of human rights law;**
- **how the measure is effective to achieve (that is, rationally connected to) that objective;**
- **whether the limitation is a reasonable and proportionate measure to achieve the stated objective (including whether it is the least rights restrictive approach and whether reversing the legal burden of proof rather than the evidential burden of proof is necessary); and**

- **whether consideration could be given to amending the measures to provide for a reverse evidential burden rather than a reverse legal burden**

Human Rights Objectives

The Act, in part, establishes a regulatory framework for the management of remote and high hazard industry activities associated with offshore resources exploration and production. These activities, if not conducted properly, have the potential to result in serious injury or death and/or extraordinary environmental harm. The robustness of the regulatory regime, including an effective compliance and enforcement framework, is critical to achieving this objective. The objective of both the breach of directions defence and the well integrity defence assist in achieving the objective of ensuring the safety of persons in the industry as well as the protection of the environment. As such, the regulatory regime positively engages with the right to life, and helps to protect other human rights which would be negatively affected by significant environmental damage.

Effectiveness

A direction issued by NOPSEMA is an enforcement tool designed to achieve a very particular outcome, to direct the industry participant to either do or refrain from doing something in order to deliver OHS, environmental management or well integrity outcomes. Directions are not used frequently – they are used in extraordinary circumstances, usually to deal with a specific emergent risk that the regulations do not adequately cover, and their application and use is taken very seriously. The defence in connection with the offence of non-compliance with a direction allows an optional exception; it is an opportunity for the defendant to prove that they took all reasonable steps to comply with the direction. As a result, the measure is effective in achieving the objectives of the Act.

Well integrity laws relate specifically to the regulatory oversight of the structural integrity of wells, the management of which is seen as posing the greatest risk to both OHS and the environment. A failure in well integrity can result in the death of workers and widespread damage to the environment, such as that recently seen in the Gulf of Mexico with the explosion of the Macondo rig. Strict compliance with these laws is deemed critical and a central tenet of the offshore regime. However, this defence acknowledges and provides for an exception to strict compliance in emergency circumstances. As a result, the measure is effective in achieving the objectives of the Act.

Reasonable and Proportionate

Both of these defences are not related to issues essential to culpability, but instead provide exceptions or an excuse for the conduct. In addition, both defences relate to the serious potential consequences of non-compliance (as outlined above – risks of serious injury or death and/or major environmental consequences). Conduct resulting in the offence would, in most circumstances, take place at a remote location and without the ability for the regulator to immediately or even quickly gain access in order to ascertain the facts directly relating to these defences. As a result, the facts and information directly relevant to the defence is entirely within the defendant's knowledge; only the defendant, with their particular knowledge of, and involvement in, the circumstances happening in the event of the failure to comply with the direction, or during a well integrity emergency, is able to prove the requisite and exception-based matters of reasonable steps or practicable actions.

Both defences are likely to be used by companies with significant resources, who are more than capable of shouldering the legal burden if they wish to claim a defence. The industry is highly regulated and companies involved have chosen to voluntarily participate in this regulated environment on a for profit basis. In addition, in relation to the breach of directions defence, the penalties are generally 100 penalty units and do not involve imprisonment.

As a result, both measures contain a limitation that is both reasonable and proportionate to the achievement of the relevant objective. It is also the least rights restrictive approach while still balancing the ability of the measures to effectively achieve their objective.

Merely Reversing Evidential Burden is Insufficient

Allowing for a reversal of the evidential burden of proof only would create internal inconsistencies in the Act and its established treatment of offences and defences. It is essential to avoid any perception by the offshore petroleum and greenhouse gas storage industries that the Commonwealth is 'soft' on compliance. Defences should be available only to those who have genuinely done everything in their power to avert the occurrence of an adverse event and can demonstrate that they have done so.

To provide the ability of a defendant to simply point to evidence that suggests a reasonable possibility that reasonable steps were taken to comply with a direction or that compliance with well integrity laws was not practicable in the face of an emergency would result in the regulator being unable to successfully and meaningfully take enforcement action in the case of an offence being committed, and this would undermine the legitimate objective in question.

In the aftermath of an event where one or more workers may have suffered serious injury or may have died, or where significant environmental damage may have occurred, it is appropriate that a titleholder should have to demonstrate, on the balance of probabilities, that the titleholder took all available action to prevent the occurrence, rather than merely to meet the evidential burden relating to the possibility of having done so.

Due to the remote occurrence of the regulated activities, the regulator is not able to, at the relevant time, independently assess and verify what is reasonable or practicable in the event of non-compliance. Accordingly, the defence would almost always succeed without the real ability of the prosecution to contest its veracity. The relevant facts are entirely within the defendant's knowledge and not at all within the regulator's knowledge. This puts the regulator at a significant disadvantage when attempting to establish the chain of causation of an adverse event and to meet a legal burden of proof that a defence cannot be relied upon. This would ultimately lead to suboptimal outcomes for OHS of offshore workers and protection of the marine environment.