Appendix 3

Correspondence

The Hon Christian Porter MP
ATTORNEY-GENERAL

The Hon Peter Dutton MP
MINISTER FOR HOME AFFAIRS
MINISTER FOR IMMIGRATION AND BORDER PROTECTION

MC18-006014

13 AUG 2018

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

Dear ~~Chair~~ Ian

Thank you for your letter of 27 June 2018 regarding the consideration by the Parliamentary Joint Committee on Human Rights (the Committee) of the Counter-Terrorism Legislation Amendment Bill (No. 1) 2018 (the Bill).

The Committee has requested further information to inform its consideration of the measures contained in the Bill and their consistency with Australia's human rights obligations. We apologise for the delay in responding to your correspondence. The enclosed document responds to the Committee's request for further information.

We thank the Committee for its robust consideration of the Bill and trust the additional information enclosed will assist the Committee.

Yours sincerely

The Hon Christian Porter MP
Attorney-General

The Hon Peter Dutton MP
Minister for Home Affairs

Encl. Response to Report 6 of 2018 of the Parliamentary Joint Committee on Human Rights, concerning the Counter-Terrorism Legislation Amendment Bill (No. 1) 2018.

Response to the Parliamentary Joint Committee on Human Rights' Report 6 of 2018 concerning the Counter-Terrorism Legislation Amendment Bill (No. 1) 2018

Background

The Counter-Terrorism Legislation Amendment Bill (No. 1) 2018 (the Bill) extends the operation of a range of critical counter-terrorism provisions in the *Criminal Code*, the *Crimes Act 1914* (Crimes Act), and the *Australian Security Intelligence Organisation Act 1979* (ASIO Act) to ensure that law enforcement and security agencies continue to have they powers they need to respond to the ongoing threat of terrorism in Australia.

The Bill extends for a further three years the following regimes which are scheduled to sunset on 7 September 2018:

- the control order regime in Division 104 of the *Criminal Code*
- the preventative detention order (PDO) regime in Division 105 of the *Criminal Code*
- the declared areas provisions in sections 119.2 and 119.3 of the *Criminal Code*, and
- the stop, search and seize powers in Division 3A of Part IAA of the Crimes Act.

In doing so, the Bill also implements the Government's response to the recommendations of two independent reviews of these sunsetting provisions.

Firstly, three reports of the Independent National Security Legislation Monitor (INSLM) were tabled on 16 October 2017: the review of the declared areas provisions, the review of Divisions 104 and 105 of the *Criminal Code* (including the interoperability of the control order regime with the continuing detention order (CDO) regime in Division 105A of the *Criminal Code*), and the review of Division 3A of Part IAA of the Crimes Act (INSLM Report).

Secondly, on 1 March 2018, the Parliamentary Joint Committee on Intelligence and Security (PJCIS) tabled two reports reviewing the operation of the sunsetting provisions:

- a review into police stop, search and seize powers, the control order regime and the PDO regime (PJCIS Powers Report), and
- a review into the declared areas provisions (PJCIS Declared Areas Report).

The Bill also extends for a further 12 months the operation of the Australian Security Intelligence Organisation's questioning, and questioning and detention powers in Division 3 of Part III of the ASIO Act.

Control orders

The Parliamentary Joint Committee on Human Rights (the Committee) has requested further advice as to whether:

- the control order regime as a whole is effective to achieve (that is, rationally connected to) its stated objective, and
- the limitations on human rights imposed by the control order regime is a reasonable and proportionate measure to achieve the stated objective (including whether it is necessary, whether it is the least restrictive approach, and whether there are adequate and effective safeguards in place in relation to its operation).

Rationally connected to achieving a legitimate purpose

The control order regime achieves the legitimate objective of preventing serious threats to Australia's national security interests, including in particular, the prevention of terrorist acts. Preventative powers such as control orders play an important part of ensuring that law enforcement agencies are able to take proactive steps to mitigate terrorist threats in an ever evolving national security environment. The Committee recognised that the prevention of terrorist acts constitutes a legitimate objective for the purposes of international human rights law.[1]

Control orders are a measure of last resort, which are only relied upon when traditional law enforcement options such as arrest, charge and prosecution are not available. As noted by the PJCIS Powers Report, the limited use of the control order regime demonstrates that the preference of law enforcement agencies is to employ traditional law enforcement methods to more comprehensively address the threat posed by an individual.

In the INSLM Report, the INSLM referred to controls placed on one individual as having a deterrent effect and a beneficial impact on that individual by effectively diverting them from radicalisation. In another example, the INSLM noted that the controls protected the community by enabling law enforcement to prevent criminal acts from occurring.[2] The Committee's report acknowledges that these examples give "some evidence that the imposition of a control order could be capable of being effective in particular individual cases", but states that "some questions remain as to whether the control order regime as a whole is rationally connected to its objective..". The Government respectfully disagrees with this assessment, noting that the INSLM Report proffered these examples to "demonstrate their effectiveness in pursuing the objects of the regime".[3]

Six control orders have been made to date. This indicates there will be circumstances where law enforcement agencies may have sufficient information or intelligence to establish a serious concern regarding the threat posed by an individual that falls short of the evidentiary burden to commence criminal prosecution. However, without an appropriate preventative mechanism, law enforcement agencies have limited means to manage the threat in the short to medium term. Use of a control order is considered in conjunction with, and is complementary to, criminal prosecution, and allows a balance to be achieved between mitigating the risk to community safety and allowing criminal investigations to continue.

The limitations on human rights imposed by a control order are rationally connected to achieving the legitimate purpose of preventing a terrorist act. When determining which conditions to impose on an individual under a control order, the issuing court must consider whether the proposed obligation, prohibition or restriction is 'reasonably necessary, and reasonably appropriate and adapted' for the purposes of achieving one of the permitted purposes for a control order, such as protecting the public from a terrorist act (paragraph 104.4(1)(d)). This requires the issuing court to be satisfied that each condition under a control order must be effective in addressing the risk posed by the individual. Where a condition is not effective or necessary in addressing this threat, the issuing court may not impose that condition, or if it does impose the condition, may at a later time, upon application by the subject of the control order, determine that that condition is no longer necessary or effective to address the threat posed by the individual.

---

[1] Parliamentary Joint Committee on Human Rights (PJCIS), Report 6 of 2018, para 1.20.
[2] Independent National Security Legislation Monitor (INSLM), Report 3 of 2017, para 8.19.
[3] Ibid.

Accordingly, the control order regime ensures that each of the limitations on a human right that may be imposed under a control order is rationally connected to minimising serious threats to Australia's national security, including in particular, the prevention of terrorist acts.

Reasonable and proportionate measure to achieve the legitimate purpose

The control order regime contains a number of safeguards to ensure that it represents the least restrictive way to achieve the legitimate purpose of preventing a serious threat to Australia's national security interests, including in particular, the prevention of terrorist acts.

Firstly, a control order is made by a judicial authority, being either the Federal Court or the Federal Circuit Court. This guarantees effective judicial oversight of the making of a control order. These courts are well placed to undertake the exercise of balancing the protection of the community with safeguarding individual rights and liberties.

Secondly, paragraph 104.4(1)(d) of the *Criminal Code* provides that the issuing court must be satisfied on the balance of probabilities that each of the obligations, prohibitions or restrictions to be imposed on the person by the control order is reasonably necessary, and reasonably appropriate and adapted for the purpose of achieving one of the permitted purposes for a control order, such as protecting the public from a terrorist. This ensures that only the obligations, prohibitions and restrictions directly capable of achieving the objective of the control order are imposed by the issuing court. This means that the control order is no more restrictive than it needs to be for the purpose of achieving the legitimate objective.

Thirdly, the control order regime allows for each application to be dealt with flexibly, and based on the circumstances of each case. For instance, for control order applications in relation to young persons between the age of 14 and 17, the issuing court must consider the best interests of the young person when determining whether each of the obligations, prohibitions or restrictions to be imposed on the individual is reasonably necessary, and reasonably appropriate and adapted to the protecting the public from a terrorist act (paragraph 104.4(2)(b)). Subsection 104.4(2A) outlines specific matters that the issuing court must take into account when determining what is in the best interest of the young person, including their age, maturity, background, the right of the person to receive an education, the benefit to the person of having a meaningful relationship with his or her family and friends and the physical and mental health of the individual.

In addition, paragraph 104.4(2)(c) provides that the issuing court must consider the impact of each of the proposed obligations, prohibitions or restrictions on the person's circumstances (including the person's financial and personal circumstances). This enables the control order regime to provide sufficient flexibility to treat the circumstances of each control order application differently, rather than imposing a blanket restriction on human rights without regard to the specific needs of the individual, or the threat they pose.

Fourthly, the control order regime contains mechanisms for assessing the ongoing need for a control order, and each of its obligations, prohibitions and restrictions. An individual subject to a control order may apply at any time to have a confirmed control order revoked or varied. The issuing court can revoke a control order if it is no longer satisfied on the balance of probabilities that the control order would substantially assist in the prevention of a terrorist act. Alternatively, the issuing court may remove certain obligations, prohibitions and restrictions in relation to an individual if it is no longer satisfied that the condition is reasonably necessary, and reasonably appropriate and adapted to achieving the purpose of protecting the public from a terrorist act. These review mechanisms ensure that the

intrusions on human rights that may be occasioned by a control order are no greater than necessary to achieve the legitimate objective.

The control order regime represents a reasonable and proportionate means of achieving the legitimate objective of preventing serious threat of Australia's national security interests, including in particular, the prevention of terrorist acts. The restrictions on human rights occasioned by a control order are not indiscriminate or disproportionate intrusions, but rather tailored to the specific threat being mitigated, and the individual circumstances of the individual who is the subject of the restrictions.

Extending the minimum duration of the time between and interim and confirmation proceeding

The Bill proposes to extend the minimum duration of time from the making of an interim control order to the confirmation proceeding from 72 hours to seven days. While this has the potential to limit the subject of the control order's right to contest the interim control order as soon as practicable, consistent with the right to a fair hearing, it also provides greater opportunity for the subject of the control order to prepare to present their case to the court.

Confirmation proceedings are complex, and may take both parties a substantial amount of time to prepare for. While subsection 104.5(1B) allows the issuing court to consider a range of factors when determining the date of the confirmation hearing, subsection 104.5(1A) enables the issuing court to set the confirmation date as early as 72 hours after the making of an interim control order. This could prevent both the subject of the control order and the AFP from being adequately prepared for the confirmation hearing.

To date, the issuing court, the AFP and the subject of the control order application, have been satisfied in holding confirmation proceedings several months after the making of an interim control order. In light of this reality, the proposed extension of time between the making of an interim control order and the confirmation date from 72 hours to seven days is unlikely to amount to an undue delay in an individual's right to contest the interim control order.

Preventative detention orders

The Committee has requested further advice as to:

- how the PDO regime is effective to achieve (that is, rationally connected to) its stated objective, and
- whether the limitation is a reasonable and proportionate measure to achieve the stated objective (including whether it is necessary, whether it is the least rights restrictive approach and whether there are adequate and effective safeguards in place in relation to its operation).

Rationally connected to achieving a legitimate purpose

The PDO regime achieves the legitimate objective of preventing serious threats to Australia's national security and, in particular, preventing terrorist acts. The Committee recognised that preventing serious terrorist attacks is likely to constitute a legitimate objective for the purposes of international human rights law.[4]

Under a Commonwealth PDO, a person can be detained for up to 48 hours to:

[4] Parliamentary Joint Committee on Human Rights (PJCIS), Report 6 of 2018, para 1.50, p. 14.

- prevent a terrorist act that is capable of being carried out, and could occur, within the next 14 days from occurring, or
- preserve evidence of, or relating to, a recent terrorist act.

In the current threat environment, there is a heighted risk of smaller-scale opportunistic attacks, undertaken principally by lone actors or small groups. While there is still the need to prepare for more complex attack plots, simple attack methodologies that enable individuals to act independently and with a high degree of agility remain the more likely form of terrorism in Australia. The simple nature of these attacks means preparation may not involve activity that is concerning enough to come to the attention of authorities immediately. In such circumstances, law enforcement agencies need to act quickly and decisively to disrupt terrorist acts and prevent catastrophic consequences to the community. As acknowledged in the INSLM Report, a PDO regime is necessary and proportionate to this threat environment as a means of protecting the public.[5]

As with control orders, the PDO is a measure of last resort, which is only sought in exceptional circumstances before a terrorist act occurs, or after an act of terrorism occurs to preserve evidence. As noted in the PJCIS Powers Report, the lack of use of the PDO regime reflects the understanding by the AFP that the PDO regime is only anticipated to be used 'in times of an unfolding emergency (or in its immediate aftermath) and when the traditional investigative powers available to law enforcement are inadequate to contain the threat'.[6]

While the Commonwealth PDO regime is yet to be used, there are scenarios when its use may be necessary and appropriate. In its supplementary submission to the PJCIS, the Attorney-General's Department (AGD) and the AFP provided the following example of when a PDO is an effective means of responding to a terrorist act:

> Consider there has been an explosion in a crowded place in the Melbourne central business district. There are significant casualties. Police arrest a person suspected of causing the explosion and establish that the terrorist suspect had called an unknown associate around the time of the attacks. The associate is previously unknown to police, and at this stage, there is insufficient information to reach the threshold for arrest, and further investigation is required. A Commonwealth PDO is issued by a senior AFP member to the associate.[7]

In this scenario, the detention of the associate is rationally connected to the prevention of a further terrorist act. The rational connection to the prevention of a terrorist act is outlined in the legislation itself which requires an analysis by the AFP member and the issuing authority of whether the PDO would 'substantially assist' in preventing a terrorist act occurring (paragraph 105.4(4)(c)). This ensures that a PDO can only be made if it is likely to be effective in achieving its objective of addressing a serious terrorist threat.

Similarly, each of the restrictions on human rights occasioned by the making of a PDO is rationally connected with preventing a terrorist act, or preserving evidence in the immediate aftermath of a terrorist act. For instance, the restrictions on communications with others, and the making of prohibited contact orders, are intended to assist in achieving the legitimate objective of preventing a terrorist act, or preventing the destruction of vital evidence in the aftermath of a terrorist act. These limitations on human rights are permissible to the extent that they are effective in achieving the legitimate objective of the PDO regime. The INSLM

---

[5] Independent National Security Legislation Monitor (INSLM), Report 3 of 2017, para 10.13
[6] Parliamentary Joint Committee on Intelligence and Security, Review of police stop, search and seize powers, the control order regime, and the preventative detention order regime, para 4.78, p. 103.
[7] Attorney-General's Department and Australian Federal Police, Supplementary Submission to the Parliamentary Joint Committee on Intelligence and Security, p. 3.

Report also acknowledged the adequate protections of individual rights under the PDO regime.[8]

Based on the current nature of the terrorist threat, and the serious consequences to the public if a terrorist act were to occur, the PDO regime is rationally connected to the legitimate purpose of preventing serious threats to Australia's national security and, in particular, preventing terrorist acts.

Reasonable and proportionate measure to achieve the legitimate purpose

The PDO regime contains a number of safeguards to ensure that it represents the least restrictive way to achieve the legitimate purpose of preventing serious threat of Australia's national security interests, including in particular, preventing terrorist acts.

Firstly, the test for seeking a PDO by an AFP member, and making a PDO by an issuing authority[9], ensures that a PDO can only be exercised when necessary and appropriate. Subsection 105.4(4) provides that to obtain a PDO, an AFP member must:

- suspect on reasonable grounds that the subject of the PDO will:
    - engage in a terrorist act
    - possess a thing connected with the preparation for, or the engagement of a person in, a terrorist act, or
    - has done an act in preparation for, or planning, a terrorist act
- be satisfied that making the PDO would substantially assist in preventing a terrorist act occurring, and
- be satisfied that detaining the individual for the period for which the individual is to be detained under the PDO is reasonably necessary for the purpose of preventing a terrorist act.

The 'terrorist act' referred to must be one that is 'capable of being carried out, and could occur, within the next 14 days' (subsection 105.4(5)).

The test for seeking and making a PDO also requires both the AFP member and the issuing authority to undertake a proportionality analysis. The PDO can only be sought and made where it would 'substantially assist' in preventing a terrorist act occurring. The AFP member and issuing authority must also consider whether detention of the individual under a PDO is 'reasonably necessary' for the underlying purpose of making a PDO. These criteria require the AFP member and issuing authority to weigh the effectiveness of the PDO against other measures that are available to prevent or respond to a terrorist threat. Accordingly, the test for seeking and making a PDO is targeted and narrowly framed, to ensure it is only used where it is likely to be effective, and in circumstances where it can prevent terrorist acts which are likely to occur within a short period of time.

A similar proportionality analysis is undertaken where a PDO is sought and made for the purposes of preserving evidence in the immediate aftermath of a terrorist act. In such circumstances, the AFP member and issuing authority must be satisfied that a terrorist act has occurred within the last 28 days, that it is necessary to detain the person to preserve evidence of, or relating to the terrorist act, and that detention is reasonably necessary to achieve this objective (subsect 105.4(6)).

---

[8] Independent National Security Legislation Monitor (INSLM), Report 3 of 2017, para 10.13

[9] An 'issuing authority' for the purposes of an initial PDO is a senior AFP member. An 'issuing authority' for the purposes of a continued PDO is outlined in section 105.2.

Secondly, under the PDO regime, the AFP member must continue to justify the detention of an individual following the expiry of the initial PDO. An initial PDO, which is made by a senior AFP member as the issuing authority, can last for up to 24 hours. Should the AFP wish to extend the period of detention under a PDO for a further 24 hours, the AFP member must apply to an issuing authority for a continued PDO. An 'issuing authority' for the purposes of a continued PDO is defined in section 105.2 and includes a person who is a judge of a State or Territory Supreme Court, or a person who is a Judge of the Federal Court of Australia or of the Federal Circuit Court of Australian, who is acting in their personal capacity. In making a continued PDO, the issuing authority must consider afresh the merits of making the order, and be satisfied, after taking into account relevant information (including information that has become available since the initial PDO was made), of the test in subsection 105.4(4) or (6). This ensures that after the first 24 hours, the basis for a PDO must again be considered and can only be extended where the original test for a PDO continues to be satisfied. This ensures that an individual detained under a PDO is not subject to greater detention than is necessary to achieve the legitimate objectives of the PDO regime.

Thirdly, the PDO regime allows for flexibility in its application for different cases – such as individuals under the age of 18 and those incapable of managing their own affairs (section 105.29). For instance, a person who is under the age of 18 or incapable of managing their own affairs is entitled to have contact with a parent or guardian, or another person who is able to represent the person's interest. A person under the age of 18 who is detained under a PDO must also not be detained with persons who are 18 years or older, unless there are exceptional circumstances (section 105.33A).

Fourthly, while a detainee's right to contact others while under a PDO is necessarily limited so as to not undermine the effectiveness of the PDO in preventing or responding to a terrorist act, the detainee may still have contact with a range of individuals so as to communicate they are safe. These individuals include: family members, employers, business associates, lawyers, and any other person that the police officer detaining the individual agrees to (sections 105.35 and 105.36). The detainee may also contact the Commonwealth to make a complaint if necessary (section 105.36).

Fifthly, the PDO regime also provides that an individual detained under a PDO has the right to be treated with humanity and respect for human rights, and not to be subject to cruel, inhuman or degrading treatment (section 105.33). A contravention of this by a police officer is an offence and carries a maximum penalty of up to two years imprisonment (section 105.45).

Finally, the PDO regime also contains important review mechanisms such as the detainee's right to apply, on expiration of the PDO, to the Security Division of the Administrative Appeals Tribunal to seek merits review of the decision to make or extend a PDO. The detainee may also bring proceedings in a court for a remedy in relation to the PDO, or for their treatment under the PDO (section 105.51).

The PDO regime is proportionate to the legitimate purpose of preventing serious threats to Australia's national security interests, including in particular, preventing terrorist acts. It requires the AFP member and issuing authority to carefully consider whether the measure is necessary and whether the making of a PDO is the most effective means of preventing or responding to a terrorist act. The regime strikes the appropriate balance between safeguarding the community, and ensuring that the interference with an individual's rights is not greater than necessary to achieve the legitimate purpose of the regime.

Stop, search and seize powers

The Committee has requested further advice as to whether:

- each of the stop, question, search and seizure powers, and their proposed extension, is effective to achieve (that is, rationally connected to) its stated objective, and
- each of the stop, question, search and seizure powers, and their proposed extension, is a reasonable and proportionate measure for the achievement of that objective (including whether it is necessary, whether it is the least rights restrictive approach and whether there are adequate and effective safeguards in place in relation to its operation).

Rationally connected to achieving a legitimate purpose

The stop, search and seize powers in Division 3A of Part IAA of the Crimes Act achieves the legitimate purpose of protecting Australia's national security, including in particular, preventing terrorist acts. The Committee recognised that this is likely to constitute a legitimate objective for the purposes of international human rights law.[10]

Law enforcement agencies can use the stop, search and seize powers where an individual is located in a Commonwealth place (such as an airport or a defence establishment), and the police officer suspects on reasonable grounds that the person might have just committed, might be committing or might be about to commit a terrorist act (section 3UB). Alternatively, these powers can be used where there is a prescribed security zone declaration in respect of a Commonwealth place. A declaration for a prescribed security zone can only be made if the Minister considers that the declaration would assist in preventing a terrorist act occurring, or in responding to a terrorist act that has occurred (section 3UJ).

Section 3UEA is the only power in Division 3A that may be exercised by law enforcement agencies outside of a Commonwealth place. Section 3UEA provides that a police officer may enter premises without a warrant if the police officer suspects on reasonable grounds that:

- it is necessary to search the premises for a thing, or seize a thing, in order to prevent the thing that is on the premises from being used in connection with a terrorism offence, and
- it is necessary to exercise the power without a search warrant because there is a serious and imminent threat to a person's life, health or safety.

The limitations on human rights that are occasioned by the exercise of the stop, search and seize powers are rationally connected to achieving the legitimate purpose of preventing a terrorist act. Each of these powers is intended to provide law enforcement agencies with additional information, or means, to prevent a terrorist act from occurring, or to respond to a terrorist act that has occurred. These powers are largely confined in their application to Commonwealth places, which are generally places of national significance, or areas of mass gathering (or both), where a terrorist act could have potentially catastrophic consequences. As stated on the Government's national security website in relation to Australia's National Terrorism Threat Advisory System, the symbolic appeal of an attack against a government or authority – such as the military, police and security agencies – elevates the threat to these entities.[11]

---

[10] Parliamentary Joint Committee on Human Rights (PJCHR), Report 6 of 2018, para 1.26, p. 23.
[11] https://www.nationalsecurity.gov.au/securityandyourcommunity/pages/national-terrorism-threat-advisory-system.aspx

As noted in the PJCIS Powers Report, the stop, search and seize provisions are emergency powers which are only likely to be used 'in rare and exceptional circumstances'[12] to enable police to 'respond rapidly to terrorism incidents'.[13] While these powers have not yet been used by law enforcement agencies, they 'fill a critical, albeit narrow, gap in state and territory emergency counter-terrorism powers, by enabling law enforcement agencies to act immediately in the event of a terrorist threat to, or terrorism incident within, a Commonwealth place'.[14] In the joint submission from AGD and the Australian Federal Police (AFP) to the PJCIS, a hypothetical scenario was outlined in which the stop, search and seize powers would be an effective measure and markedly improve the capability of law enforcement agencies to respond to the threat of a terrorist act:

> AFP provides a Uniformed Protection Function at Garden Island Defence Precinct (NSW). The AFP's function in that regard is to provide for the safety and security of the Precinct and its population along with providing a first response capability in the event of a critical incident.
>
> In this hypothetical example, intelligence indicates that an unidentified person is planning to commit an edged weapon terrorist attack at the Precinct. A suspect is identified loitering in the public area for a prolonged period of time, constantly keeping his hands in his pocket and trying to secret himself from view of CCTV cameras with a black and white flag visible in his rear pocket.
>
> In this scenario reasonable grounds to suspect the person might be about to commit a terrorist act exist to exercise powers under Division 3A. The suspect is approached and required to provide their name and reason for being at the Precinct under section 3UC. The person provides their name and shows a NSW driver's licence. Intelligence checks identify that they are an associate of a known terrorism suspect. Meanwhile, police search the person under section 3UD, and seize a knife and Islamic State flag found in their possession. The person is arrested on suspicion of planning a terrorist act.[15]

In the current terrorism threat environment, an attack on a Commonwealth place is not unlikely.[16] It is therefore vital that law enforcement agencies have appropriate and targeted powers to prevent or respond to terrorist acts in Commonwealth places. The stop, search and seize powers are rationally connected to the legitimate purpose of preventing serious threats to Australia's national security and, in particular, preventing terrorist acts. Each of the limitations on human rights occasioned by the exercise of the stop, search and seize powers is necessary in achieving the legitimate objective of preventing a terrorist act.

Reasonable and proportionate measure to achieve the legitimate purpose

The stop, search and seize powers contain a number of safeguards to ensure that they represent the least restrictive way to achieve the legitimate purpose of preventing serious threat of Australia's national security interests, including in particular, preventing terrorist acts.

---

[12] Parliamentary Joint Committee on Intelligence and Security, Review of police stop, search and seize powers, the control order regime, and the preventative detention order regime, para 2.32, p. 17.
[13] Ibid, para 2.62, p. 26.
[14] Australian Federal Police, Submission to the Parliamentary Joint Committee on Intelligence and Security, para 15, p. 2.
[15] Attorney-General's Department and Australian Federal Police, Submission to the Parliamentary Joint Committee on Intelligence and Security, pp. 2-3.
[16] Ibid, p. 2.

Firstly, as noted in the PJCIS Powers Report, the stop, search and seize powers are only likely to be exercised in emergency scenarios. Under such circumstances, it is anticipated that traditional law enforcement powers are unlikely to be as effective in responding to the terrorist threat. In a rapidly evolving threat scenario, the stop, search and seize powers are likely to represent the most effective means of responding to a terrorist threat, and therefore may represent the least restrictive way to achieve the legitimate objective of safeguarding the community from a terrorist act.

Secondly, the stop, search and seize powers are, with the exception of the emergency entry into premises power in section 3UEA, narrowly confined in their application to Commonwealth places. Accordingly, these powers are not broadly applicable and are limited in their exercise to locations which are generally of national significance or places of mass gathering (or both). Similarly, while section 3UEA is not limited in its application to a Commonwealth place, the circumstances in which it may be applied are narrowly confined to emergency scenarios, where rapid law enforcement action is necessary because there is a serious and imminent threat to a person's life, health or safety.

Thirdly, in exercising the stop and search power in section 3UD, a police officer must not use more force, or subject the person to greater indignity, than is reasonable and necessary in order to conduct the search (subsection 3UD(2)). Furthermore, a person must not be detained longer than is reasonably necessary for a search to be conducted (subsection 3UD(3)). Similarly, in searching a thing (including a vehicle), a police officer may use such force as is reasonable and necessary in the circumstances, but must not damage the thing by forcing it, unless the person has been given a reasonable opportunity to open the thing, or it is not possible to give that opportunity (subsection 3UD(4)). These safeguards ensure that the stop, search and seize powers are exercised in a proportionate manner and cause the least amount of interference with an individual's rights.

Fourthly, a police officer who is responsible for an item seized under section 3UE or section 3UEA must, within seven days, serve a seizure notice on the owner of the thing (or, if the owner cannot be found, the person from whom the thing was seized), to enable the owner to request for the return of the item (section 3UF).

Fifthly, where the Minister makes a declaration for a prescribed security zone in respect of a Commonwealth place, the Minister is subject to an ongoing requirement to revoke the declaration as soon as there is no longer a terrorism threat that justifies the declaration being continued, or if it is no longer required to respond to a terrorist act that has already occurred (subsection 3UJ(4)). This ensures that the inference with human rights that may be occasioned through the making of a prescribed security zone declaration does not last any longer than necessary to achieve the legitimate objective of the preventing or responding to a terrorist act.

Finally, the stop, search and seize powers are subject to important oversight mechanisms. For instance, complaints on the use of these powers by the AFP could be investigated by the Commonwealth Ombudsman or the Australian Commission for Law Enforcement Integrity. Similarly, the use of these powers by state and territory police can be reviewed by the appropriate jurisdictional oversight bodies, such as state and territory Ombudsman. In addition, the INSLM has the power to review the operation of counter-terrorism legislation, which includes the power to request information or produce documents for the purposes of performing the INSLM's function. This enables the INSLM to seek information and review documents associated with the exercise of stop, search and seize powers by the AFP.

The Bill strengthens these oversight arrangements by also requiring that as soon as possible after the exercise of the stop, search and seize powers by an AFP police officer, the Commissioner of the AFP must provide a report about the use of the powers to the Minister, the INSLM and the PJCIS. Furthermore, the Bill also introduces a new annual reporting requirement for the exercise by the AFP of the stop, search and seize powers.

These safeguards ensure that the stop, search and seize powers are targeted in their application and do not cause greater interference with human rights than is necessary to achieve the legitimate objective of preventing serious threat of Australia's national security interests, including in particular, preventing terrorist acts.

The Hon Christian Porter MP
Attorney-General

MC18-008568

31 AUG 2018

Mr Ian Goodenough MP
Member for Moore, LP
Parliament House
CANBERRA ACT 2600
Human.rights@aph.gov.au

Dear ~~Mr Goodenough~~ Ian

Thank you for your letter of 15 August 2018 in relation to the issues identified by the Parliamentary Joint Committee on Human Rights (the Committee) in Report 7 of 2018 regarding the Office of National Intelligence Bill 2018 (the Bill) and the Office of National Intelligence (Consequential and Transitional Provisions) Bill 2018.

I offer the following information for the Committee's consideration.

I appreciate the Committee's consideration of these Bills, and trust this information will be of assistance to the Committee.

Yours sincerely

The Hon Christian Porter MP
Attorney-General

Encl. Response to the Parliamentary Joint Committee on Human Rights (including Attachments A and B)
CC. The Prime Minister, the Hon Scott Morrison MP

Parliament House, Canberra ACT 2600 • Telephone (02) 6277 7300 Fax (02) 6273 4102

Response to the Parliamentary Joint Committee on Human Rights

Office of National Intelligence Bill 2018

Office of National Intelligence (Consequential and Transitional Provisions) Bill 2018

Offences for unauthorised use or disclosure of information

Compatibility of the measures with the right to freedom of expression

Committee Comment

The Parliamentary Joint Committee on Human Rights (Committee) has raised questions about whether the measures in the Office of National Intelligence Bill 2018 (Bill) relating to offences for unauthorised use or disclosure of information are compatible with the right to freedom of expression.

The Committee sought advice as to:

- how the measures are effective to achieve (that is, rationally connected to) the stated objectives of the bill; and
- whether the limitations are reasonable and proportionate to achieve the stated objectives.

The Committee also sought advice as to whether it would be feasible to amend the secrecy offences to:

- appropriately circumscribe the scope of information subject to the prohibition on unauthorised disclosure or use under proposed sections 42 and 44;
- appropriately circumscribe the definition of what causes harm to national security for the purposes of proposed section 43;
- expand the scope of safeguards and defences; and
- reduce the severity of the penalties which apply.

Response

The development of the ONI Bill overlapped with the consideration by the Parliamentary Joint Committee on Intelligence and Security (PJCIS) of the National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017 (EFI Bill). Noting the PJCIS' recommendations on the EFI Bill, and the form in which that Bill passed Parliament, the ONI Bill including its Explanatory Memorandum will be amended to remove section 43 (the offence of subsequent communications of certain information) in its entirety. On that basis, this response only deals with clauses 42 and 44 of the Bill.

The offences in clauses 42 and 44 of the Bill are almost identical to the existing secrecy offences in sections 40A, 40J and 40K of the *Intelligence Services Act 2001* (I S Act) that currently apply to the communication of, and dealing with, information acquired by or on behalf of the Office of National Assessments (ONA) in connection with its functions. They are also consistent with the secrecy offences in the IS Act that apply in relation to other intelligence agencies.

Replication of the existing secrecy provisions through clauses 42 and 44 of the Bill is reasonable, necessary and proportionate to achieve the legitimate objectives of protecting national security; protecting the right to privacy of individuals whose information may be provided to ONI; and enabling ONI to perform its functions.

In order to effectively perform its functions, ONI will need to have access to wider range of information (frequently of a sensitive and classified nature) from a broader range of agencies than is currently required for ONA's functions. The offences in clauses 42 and 44 are part of a range of safeguards contained in the Bill to ensure that this information, as well as information generated by

ONI, is appropriately protected from unauthorised disclosure, particularly given the potentially devastating consequences that unauthorised disclosures and compromises of intelligence-related information can have.

Limiting the scope of the offences to ONI information of a particular security classification would be insufficient to provide adequate protection against harm to national security. It is well-recognised that the information handled by intelligence agencies is so sensitive that even isolated disclosures of seemingly innocuous information could cause harm; as these may be analysed collectively to reveal significant matters. Limiting the scope of the offences to the communication of information would be also insufficient to provide sufficient protection as it would not capture the full continuum of behaviour that may result in the unauthorised disclosure of information, limiting the ability of authorities to take steps to prevent significant harm to national security.

The offences in clauses 42 and 44 will only apply where the information or matter came into the person's knowledge or possession by reason of one the following circumstances: that the person is or was a staff member of ONI, that the person has entered into any contract, agreement or arrangement with ONI, or that the person has been an employee or agent of a person who has entered into a contract, agreement or arrangement with ONI.

This is in recognition of the special duties and responsibilities that apply to ONI staff and people with whom the agency has an agreement or arrangement, and the strong and legitimate expectation that those persons will handle all information obtained in that capacity in strict accordance with their authority at all times.

The offences do not constitute an absolute bar on the disclosure of ONI information and contain appropriate safeguards to facilitate the communication of ONI information in appropriate circumstances including:

- with the approval of the Director-General of National Intelligence (Director-General) or a staff member with authority to give such approval; and
- to an Inspector-General of Intelligence and Security (IGIS) official for the purpose of that official exercising a power, or performing a function or duty as such an official. This will include disclosures to the Office of the IGIS under the *Public Interest Disclosure Act 2013* that relate to an intelligence agency.

Given the existing exceptions and the limited application of the offences, the inclusion of a general public interest defence is not considered necessary.

The maximum penalties are consistent with the penalties that apply to the existing secrecy provisions in the I S Act and reflect the higher level of culpability on the part of persons who obtain ONI information in their capacity as an ONI staff member, or through a contract, arrangement or agreement with ONI.

The secrecy offences therefore represent a reasonable and proportionate limitation on the right to freedom of expression.

Compatibility of the measures with the right to be presumed innocent

Committee Comment

The Committee raised questions as to the compatibility of the offences that involve an offence-specific defence with the right to be presumed innocent. The Committee sought advice as to:

- whether these offences are aimed at achieving a legitimate objective for the purposes of international human rights law;
- how these offences are rationally connected to this objective;
- whether the limitation is a reasonable and proportionate measure to achieve the stated objective; and
- whether it would be feasible to amend the measures so that the relevant matters are included as elements of the offence or, alternatively, to provide that despite section 13.3 of the Criminal Code, a defendant does not bear an evidential (or legal) burden of proof in relying on the offence-specific defences.

Response

The offence specific-defences are a reasonable and proportionate measure to achieving the legitimate objectives of protecting national security, the privacy of individuals and enabling ONI to perform its functions. Including the matters in the exceptions to the offences as elements of the offences would impact on the effectiveness of the offences in achieving these legitimate objectives. This is because it would be significantly more difficult and costly for the prosecution to prove, beyond a reasonable doubt (and in every case), that the circumstances in the exceptions did not exist.

In addition, as outlined above, the offences only apply to ONI staff and people with whom the agency has an agreement or arrangement. These individuals will be well aware of the sensitivity of the information being communicated or dealt with and the importance of ensuring appropriate authorisation when communicating and dealing with that information.

The reversal of proof provisions are proportionate, as the prosecution will still be required to prove each element of the offence beyond a reasonable doubt before a defence can be raised by the defendant. In circumstances where evidence in relation to an offence-specific defence is raised by the defendant, the prosecution will also need to disprove that evidence beyond a reasonable doubt.

Information gathering powers

Compatibility of the measures with the right to privacy

Committee Comment

The Committee raised questions as to whether the information gathering powers are a proportionate limitation on the right to privacy.

The Committee sought advice as to whether the measures are reasonable and proportionate to achieve the stated objectives, including:

- whether each of the information gathering powers are sufficiently circumscribed and accompanied by adequate and effective safeguards;
- how the measures constitute the least rights restrictive approach;
- in relation to the power to collect open source information, whether a copy of the proposed rules could be provided; and
- what safeguards will be in place in relation to the power to collect open source information from people who are not Australian citizens or permanent residents.

Response

As outlined above, in order to effectively perform its functions, ONI will need to have access to wider range of information (frequently of a sensitive and classified nature) from a broader range of agencies than is currently required for ONA's functions. In particular, ONI is likely to require access to a wide range of information from other agencies in the national intelligence community for the purposes of performing its enterprise management role, including administrative and expenditure information, capability information and information from third parties.

As outlined in detail in the statement of compatibility, the Bill contains a number of important safeguards to ensure that the measures are a reasonable and proportionate limitation on the right to privacy. This was reflected in the independent Privacy Impact Assessment (**Attachment A**) undertaken by the Australian Government Solicitor which concluded the following:

- Key aspects of the ONI Bill are positively directed towards the management and protection of personal information and privacy, but in a manner which is seen as appropriate to the functions of ONI as a national intelligence agency.
- ONI's information collection and reporting functions are such that it can be expected to collect more information than ONA. This is recognised in the ONI Bill, which provides a stronger, more transparent regime for the handling and protection of personal information than currently exists for ONA.

The Privacy Impact Assessment also noted that the secrecy provisions in the ONI Bill are more restrictive of the communication of ONI's information, including personal information, than the provisions in the *Privacy Act 1988* (Privacy Act) relating to the disclosure of personal information.

A copy of the draft privacy rules was previously provided to the PJCIS to assist in its inquiry into the Bill. It is also attached (the reference to the Prime Minister has been updated) for the Committee's information (**Attachment B**).

In addition to the ability for the privacy rules to include requirements regarding the collection of open source information relating to non-Australian persons, there are a number of other relevant safeguards in the Bill including:

- ONI's collection role under paragraph 7(1)(g) is limited to the collection of information relating to matters of political, strategic, or economic significance to Australia that is accessible to any section of the public. The function does not authorise ONI to undertake unlawful activity to obtain the information.
- The disclosure of such information will be subject to the secrecy provisions in the Bill.

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

Committee comment

The Committee raised questions as to whether the differential treatment is compatible with the right to equality and non-discrimination.

The Committee sought advice as to:

- whether there is reasoning or evidence that establishes that the stated objective addresses a pressing or substantial concern or whether the proposed changes are otherwise aimed at achieving a legitimate objective;
- how the measures are effective to achieve that objective; and
- whether the measures are reasonable and proportionate to achieving the stated objective of the bill.

Response

Clause 53 of the Bill, which is the enabling provision for the privacy rules, is based upon section 15 of the Intelligence Services Act which requires the responsible Ministers for the Australian Secret Intelligence Service (ASIS), the Australian Signals Directorate (ASD) and the Australian Geospatial-Intelligence Organisation (AGO) to make privacy rules to protect Australians. This privileged status is thus consistent with other Intelligence Services Act agencies.

ONI information related to non-nationals will only be collected for the purposes of performing the statutory functions of ONI. This information will also be protected under the secrecy provisions in the ONI Bill. As detailed above, the Privacy Impact Assessment into the ONI Bill noted that these secrecy provisions are more restrictive of the communication of ONI's information, including personal information, than the provisions in the Privacy Act relating to the disclosure of personal information. Further, the Bill does not prevent the Prime Minister from also making privacy rules concerning non-nationals, should he/she wish to.

As the comments raised by the Committee would impact intelligence agencies more widely than just ONI, this topic may be best addressed by the Comprehensive Review of the Legal Framework Governing the National Intelligence Community, announced by the Attorney-General on 30 May 2018.

Cooperation with entities in connection with ONI's performance of functions

Compatibility of the measure with the right to privacy

Committee comment

The Committee raised questions as to whether the measure about cooperation with entities in connection with ONI's performance of functions is compatible with the right to privacy.

The Committee sought advice as to:

- whether the measure is aimed at achieving a legitimate objective for the purposes of international human rights law;
- how the measure is effective to achieve that objective; and
- whether the limitation is a reasonable and proportionate measure to achieve the stated objective.

Response

ONA has established guidelines and practices in place for the communication of information with foreign partners. As ONI is stood up, the Office will develop new internal policies (in consultation with the IGIS) to govern ONI's cooperation with foreign partners.

The Director-General (or his or her delegate) will be required to authorise ONI's cooperation with an authority from another country before such cooperation takes place. Once an authorisation has been given, it will remain in place until amended or revoked by the Director-General or cancelled by the Prime Minister under subclause 13(5). Subclause 13(3) provides that the Director-General (or his or her delegate) must notify the Prime Minister on a monthly basis of each approval given during the month, and each variation or revocation made during the month.

These requirements are based upon existing requirements that apply to the Australian Security Intelligence Organisation (ASIO) and agencies under the I S Act in respect of their cooperation with foreign authorities — with some modification to reflect ONI's cooperation is much less likely to be operational in nature than is the case with these agencies. The measures included in the ONI Bill are thus consistent with others across the intelligence community.

Furthermore, ONI information will be protected under the secrecy provisions in the ONI Bill. As detailed above, the Privacy Impact Assessment into the ONI Bill noted that these secrecy provisions are more restrictive of the communication of ONI's information, including personal information, than the provisions in the Privacy Act relating to the disclosure of personal information. Further, the Bill does not prevent the Prime Minister from also making privacy rules concerning non-nationals, should he/she wish to.

These matters will also remain subject to IGIS oversight, who will review ONI activity to ensure ONI acts legally and with propriety, complies with ministerial guidelines and directives, and respects human rights.

Compatibility of the measure with the right to life and the prohibition on torture, cruel, inhuman, or degrading treatment or punishment

Committee comment

The Committee raised questions as to whether the measure about cooperation with entities in connection with ONI's performance of functions is compatible with the right to life and the prohibition on torture, or cruel, inhuman and degrading treatment or punishment. The Committee sought advice on the compatibility of the measure with these rights.

Response

The Director-General (or his or her delegate) will be required to authorise ONI's cooperation with an authority from another country before such cooperation takes place. Once an authorisation has been given, it will remain in place until amended or revoked by the Director-General or cancelled by the Prime Minister under subclause 13(5). Subclause 13(3) provides that the Director-General (or his or her delegate) must notify the Prime Minister on a monthly basis of each approval given during the month, and each variation or revocation made during the month.

The Director-General (and the Prime Minister as part of their consideration of whether to revoke an authorisation) would consider a range of factors when deciding whether it would be appropriate for such an authorisation to be given, including the human rights record of the country/particular foreign authority.

These requirements are based upon existing requirements that apply to ASIO and agencies under the I S Act in respect of their cooperation with foreign authorities — with some modification to reflect ONI's cooperation is much less likely to be operational in nature than is the case with these agencies. The measures included in the ONI Bill are thus appropriately adapted from the practices of the broader intelligence community.

Furthermore, ONA has established guidelines and practices in place for the communication of information with foreign partners. As ONI is stood up, the Office will develop new internal policies (in consultation with the IGIS) to govern ONI's cooperation with foreign partners. These policies will ensure that consideration is given to the human rights records of the country and this will be factored into the internal approval mechanisms required to share information.

REPORT

PRIVACY IMPACT ASSESSMENT: ESTABLISHING THE OFFICE OF NATIONAL INTELLIGENCE

19 June 2018

To:
Home Affairs and Intelligence Review Implementation Taskforce
Department of the Prime Minister and Cabinet

Justin Hyland
Senior Executive Lawyer
(02) 6253 7417
justin.hyland@ags.gov.au

Danielle Chifley
Senior Lawyer

Kate McLaren
Lawyer

CONTENTS

REPORT

PRIVACY IMPACT ASSESSMENT – ESTABLISHMENT OF OFFICE OF NATIONAL INTELLIGENCE

1. INTRODUCTION

1.1. The Department of the Prime Minister and Cabinet (**the Department**) has asked AGS to conduct an independent privacy impact assessment (**PIA**) of the establishment of the new Office of National Intelligence (**ONI**). The creation of ONI was a primary recommendation of the 2017 Independent Intelligence Review. The Review also recommended that a new position of Director-General of National Intelligence[1] be established to head ONI and the national intelligence community and be the principal advisor to the Prime Minister on intelligence community issues.

1.2. The Department is leading the development of the Office of National Intelligence Bill 2018 (**ONI Bill**) and the Office of National Intelligence (Consequential and Transitional Provisions) Bill 2018 (**C&T Bill**) to establish ONI and the position of Director-General.

1.3. In practical effect, the existing Office of National Assessments (**ONA**) will continue in existence under the new name of ONI. It is proposed that ONA's governing legislation, the *Office of National Assessments Act 1977* (**ONA Act**), be repealed and replaced by the ONI Act. ONI will absorb the current roles, functions and staff of ONA, and be given some new functions and powers. The C&T Bill would make consequential amendments to update other Commonwealth legislation and provide for necessary transitional arrangements.

1.4. Currently, ONA's functions include:

a. preparing assessments and reports on international matters that are of political, strategic or economic significance to Australia

b. co-ordinating Australia's foreign intelligence activities, and matters of common interest to Australia's foreign intelligence agencies

c. conducting evaluations of Australia's foreign intelligence activity.[2]

1.5. The ONI Bill expands ONA's existing functions encompassing assessment, coordination and evaluation and also makes provision for ONI to provide leadership in the 'national intelligence community'(**NIC**), defined in cl ^4 of the ONI Bill to mean the ONI, each intelligence agency and each agency with an intelligence role or function. Read with the definitions of 'intelligence agency' and 'agency with an intelligence role or function' in cl ^4, the NIC therefore extends to the 6 'traditional'

---

1 References to 'the Director-General' in this PIA are to be read as references to the Director-General National Intelligence, unless otherwise specified – for example, 'Director-General of ONA'.

2 ONA Act s 5.

agencies of the Australian Intelligence Community[3], as well as the Australian Criminal Intelligence Commission (**ACIC**), and the following agencies with an intelligence role or function:

— the Australian Transaction Reports and Analysis Centre (**AUSTRAC**)

— the Australian Federal Police (**AFP**),

— the Department of Home Affairs

— the Department of Defence (other than AGO or DIO).

The Director-General will not only head ONI, but also lead the NIC.[4]

Scope of this PIA

1.6. The purpose of this PIA is to assess and make observations about the potential privacy implications of the establishment of ONI as proposed under the ONI Bill and the consequential amendments to the *Privacy Act 1988* (**Privacy Act**) proposed under the C&T Bill.

1.7. ONA is not subject to the Privacy Act, and it is proposed that ONI also not be subject to the Privacy Act.[5] Nonetheless, the Department has consulted with the Office of the Australian Information Commissioner and considers that it is appropriate for a PIA to be conducted to assess the privacy impacts of the ONI and C&T Bills.

1.8. The focus of this PIA is the privacy implications of the ONI Bill and the proposed consequential amendments to the Privacy Act that would be effected by the C&T Bill. It has been prepared with reference to the instructions we have received from the Department about the settled policy position of the Government as reflected in the draft Bills. The purpose of the PIA is limited to analysing and making observations concerning the potential impact of the draft Bills as drafted on the privacy of individuals, in particular by comparison with the current operation of ONA.

Assumptions made

1.9. We have prepared this PIA on the assumption that the ONI Bill and the C&T Bill so far as it would amend the Privacy Act are enacted in their current form.[6] For this reason, the comments we make and the conclusions we reach in this PIA should be taken to apply only to the Bills as presently proposed. If the ONI Bill is amended before it is enacted or the C&T Bill amends the Privacy Act in a different way to what

---

3 ONA/ ONI, the Australian Security Intelligence Organisation (**ASIO**), Australian Secret Intelligence Service (**ASIS**), Australian Signals Directorate (**ASD**), Australian Geospatial-Intelligence Organisation (**AGO**) and Defence Intelligence Organisation (**DIO**).

4 See in particular cl 15 and cl 16 of the ONI Bill.

5 See discussion below at 4.1-4.3.

6 Draft ONI Bill dated 12 June 2018 at 08.32 AM; draft C&T Bill dated 7 June 2018 at 11.14 AM.

is currently proposed, then we recommend the Department consider obtaining a further or updated PIA to address the effect of those changes.

2. EXECUTIVE SUMMARY

2.1. The ONI Bill expands ONA's existing functions and in carrying out its information collection and reporting functions ONI may be involved in the collection of more information. However, to the extent this includes personal information of Australians, relevant provisions of the ONI Bill are positively directed towards enhancing the protection of personal privacy compared to the current position with ONA.

2.2. While ONI will not be subject to Privacy Act, the ONI Bill establishes a legislative framework for ONI's handling of information, including a secrecy regime and privacy rules for the protection of 'identifiable information'. This term is defined in essentially the same way as 'personal information' in the Privacy Act,[7] except that:

- it is limited to information about Australian citizens and permanent residents
- considering the definition of 'permanent resident' in cl ^4, it extends to certain bodies corporate.[8]

2.3. The proposed privacy rules are intended to be analogous to those applicable to other intelligence agencies. The relevant responsible Ministers in relation to ASIS, AGO and ASD are under s 15 of the *Intelligence Services Act 2001* to make written rules regulating the communication and retention of intelligence information concerning Australian persons, having 'regard to the need to ensure that the privacy of Australian persons is preserved as far as is consistent with the proper performance by the agencies of their functions.' Clause ^53 of the ONI Bill is in similar terms, including a requirement that in making the proposed privacy rules, the Prime Minster must first consult with the Inspector-General of Intelligence Security (**IGIS**) and the Attorney General (the Minister responsible for the Privacy Act).

2.4. The ONI Bill also includes provisions which specifically require ONI to consider, and take steps to protect, personal privacy. For example, there is an express requirement to consider privacy in the exercise of ONI's compulsory information gathering power.

2.5. Amendments to the Privacy Act in the C&T Bill and certain provisions of the ONI Bill will facilitate government agencies, including certain agencies with an intelligence function as defined in the ONI Bill, providing information, including personal information, to ONI. However, ONI will be required to handle any information it obtains in accordance with the information handling and secrecy regimes established under the ONI Bill and the privacy rules.

---

7 Whenever the term 'personal information' is used in this PIA, it has the meaning given to that term in s 6 of the Privacy Act.

8 See the definition of 'identifiable information' in cl ^4 of the ONI Bill as compared with the definition of 'personal information' in s 6 of the Privacy. The only material difference is that 'identifiable information' is limited to information about Australian citizens and permanent residents, and 'permanent residents' includes certain bodies corporate. See also the discussion below at paragraph 5.42.

2.6. Overall, in our view the relevant provisions of the ONI Bill provide a stronger and more transparent regime for the handling and protection of personal information than currently exists for ONA.

3. METHODOLOGY

3.1. In preparing this PIA, we have considered the following material:

- Office of National Intelligence Bill 2018[9]
- Office of National Intelligence (Consequential and Transitional Provision) Bill 2018[10]
- 'ONA Guidelines to Protect the Privacy of Australians' (23 June 2017)
- Preliminary draft 'Rules to protect the privacy of Australians'[11]
- *Office of National Assessments Act 1977*
- *Privacy Act 1988.*

4. NON-APPLICATION OF THE PRIVACY ACT

4.1. The Privacy Act does not apply to ONA, and it is not proposed that it will apply to ONI. Instead, a separate regime for the handling of personal information and the protection of privacy will be established by the ONI Bill, adapted to the functions and operation of ONI including its function of providing leadership in the NIC.

4.2. The ONA Act currently does not impose any obligations or make any provisions in relation to privacy, although the Director-General of ONA has published privacy guidelines.[12] What is proposed under the ONI Bill is a regime that we understand has been developed with the intention of providing the maximum possible protection of personal privacy without, consistent with the approach in relation to other intelligence agencies, requiring ONI to comply with the Privacy Act.

4.3. In this section we consider the current application of the Privacy Act, and the amendments proposed to the Privacy Act by the C&T Bill. We consider the significance of these changes further below at 4.10 - 4.11.

Currently

Acts and practices of ONA and some other NIC agencies not covered by Privacy Act

4.4. The acts and practices of particular 'intelligence agencies' are effectively exempt from the operation of relevant provisions of the Privacy Act.[13] 'Intelligence agency' is

---

9 Draft dated 12 June 2018 at 8.32 AM.

10 Draft dated 7 June 2018 at 11.14 AM.

11 We have only been provided with a preliminary draft of these Rules which may therefore be amended and differ from the form in which we have seen them when finalised.

12 See further below at 5.41.

13 Privacy Act s 7(1)(a)(i)(B) - read with *Freedom of Information Act 1982,* Div 1 of Pt 1 of Sch 2 – and s 7(2)(a).

defined in s 6(1) of the Privacy Act to mean ONA, ASIO and ASIS. The acts and practices of the ACIC,[14] DIO, AGO and ASD[15] are similarly excluded.

4.5. The acts and practices of other agencies and organisations relating to records that originated with or which have been received from these 7 agencies are also excluded from the operation of the Privacy Act.[16]

Disclosure of personal information by other agencies to ONA subject to Privacy Act

4.6. If an agency or organisation to which the Privacy Act applies discloses personal information to ONA, it is required to comply with the disclosure provisions in Australian Privacy Principle (APP) 6.

4.7. In contrast, the Privacy Act includes a specific exemption for acts or practices that involve disclosure of personal information to ASIO, ASIS or ASD.[17] This means that the Privacy Act has no application to, and therefore does not constrain, the disclosure of personal information to those agencies.

Proposed amendments to Privacy Act under the C&T Bill

Acts and practices of ONI not covered by Privacy Act

4.8. It is proposed that the definition of 'intelligence agency' in the Privacy Act be amended by substituting ONI for ONA.[18] Accordingly, like ONA, ONI will be effectively exempt from the operation of the Privacy Act.

Further exemption for disclosure of personal information by some agencies

4.9. It is proposed that the Privacy Act be amended to provide an exemption for the provision of personal information to ONI by agencies with an intelligence role or function, as defined in the ONI Bill. The term is defined in the ONI Bill to mean AUSTRAC, the AFP, the Department of Home Affairs and the Department of Defence (other than AGO and DIO) to the extent the agency performs specific functions relating to intelligence.[19] These 4 agencies are the only agencies within the NIC that are not otherwise exempt from the operation of the Privacy Act.[20]

Implications of proposed amendments to the Privacy Act

4.10. Under the proposed amendments, ONI would, as ONA is now, be exempt from the operation of the Privacy Act. This is consistent with other key intelligence agencies which are also exempt from the operation of the Privacy Act. This in part reflects the

---

14 Privacy Act ss 7(1)(a)(iv), 7(2)(c).

15 Privacy Act s 7(1)(ca) – read with *Freedom of Information Act 1982*, Div 2 of Pt 1 of Sch 2 – and s 7(2)(b).

16 Privacy Act s 7(1)(f), (g) and (h).

17 Privacy Act s 7(1A).

18 C&T Bill, cl 85.

19 C&T Bill cl 86, read with definition of 'agency with an intelligence role or function' in cl ^4 of the ONI Bill.

20 See cl ^4 of the ONI Bill, definition of 'national intelligence community'.

unique nature of the work of these agencies in relation to intelligence and information collection.

4.11. The other amendment to the Privacy Act proposed in the C&T Bill would have the effect of exempting acts or practices involving the disclosure of personal information to ONI by the other agencies with an intelligence role or function as specified in the ONI Bill. At present, such acts or practices for those agencies are covered by the Privacy Act. While this change restricts the application of the Privacy Act, it is limited in scope. Only the acts or practices of the 4 relevant agencies would be exempt from the operation of the Privacy Act.

5. OVERVIEW OF IMPLICATIONS OF THE ONI BILL FOR PROTECTION OF PRIVACY

5.1. There are 4 ways in which the establishment of ONI in accordance with the ONI Bill has the potential to impact on personal privacy:

a. ONI will be established with statutory functions that mean it can be expected to collect more information than ONA, including more personal information

b. the ONI Bill makes provision for ONI to gather and for other government agencies to provide it with information, and imposes obligations on ONI with regard to the use and protection of information provided to it in these ways

c. the ONI Bill contains secrecy provisions restricting the communication of ONI information

d. the ONI Bill provides for the making, and ONI's compliance with, privacy rules relating to identifiable information.

5.2. In the discussion that follows, we will consider each of these matters in turn and will:

- describe what is proposed and compare it with the existing regime in the ONA Act
- identify the implications for the handling, or flow, of personal information
- analyse the privacy implications of the proposal.

5.3. This discussion concerns the privacy implications of the relevant aspect of the ONI Bill, and the mechanisms for handling information and protecting privacy that would be established by the ONI Bill. ONI will need to comply with these mechanisms when dealing with personal information it collects, either intentionally or incidentally, in the performance of its functions.

a. ONI's statutory functions compared with ONA

5.4. The statutory functions of ONI under the ONI Bill have implications for the amount of personal information the new agency will handle.

Existing arrangements under the ONA Act

5.5. Section 5(1) of the ONA Act sets out the functions of ONA, and relevantly includes the function:

'to assemble and correlate information relating to international matters that are of political strategic or economic significance to Australia and [to prepare reports and assessments]' (s 5(1)(a)).

The ONI Bill

5.6. ONI's functions are set out in cl ^7 of the ONI Bill and relevantly include:

> (c) to:
>
> (i) assemble, correlate and analyse information relating to international matters that are of political, strategic or economic significance to Australia, including domestic aspects relating to such matters; and
>
> (ii) prepare assessments and reports in relation to such matters in accordance with the Government's requirements;
>
> (d) to:
>
> (i) assemble, correlate and analyse information relating to other matters that are of political strategic or economic significance to Australia; and
>
> (ii) prepare assessments and reports in relation to such matters in accordance with the Government's requirements;
>
> if doing so would support the performance of any other function or the Director-General's functions, or complement the work of other intelligence agencies;
>
> ...
>
> (g) to collect, interpret and disseminate information relating to matters of political, strategic or economic significance to Australia that is accessible to any section of the public;

5.7. There are 2 key ways in which ONI's functions, as compared with ONA, may have privacy implications.

5.8. First, ONA's functions refer to dealing with 'information relating to international matters that are of political strategic or economic significance to Australia'. The Bill clarifies that ONI's functions include 'domestic aspects' that relate to such international matters (cl ^7(c)(i)), and to information relating to 'other matters that are of political strategic or economic significance to Australia' (cl ^7(d)).

5.9. Secondly, ONA does not have a specific statutory function of collecting, interpreting and disseminating information relating to matters of political, strategic or economic significance to Australia in relation to publicly accessible information. ONA's Open Source Centre collects, analyses and researches publicly available information (which may include personal information) concerning international developments that affect Australia's national interests in support of its functions. However, consistent with the scope of the agency's current functions, we understand ONA's open source collection activities are focussed on the collection of information or intelligence relevant to the activities of persons outside Australia.

5.10. The changes in cl ^7(1)(g) of the ONI Bill will support ONI's operation of the Open Source Centre by making it clear that ONI's functions include collecting, interpreting

and disseminating information that is publicly accessible. This recognises the agency's current activities in relation to publicly available information. The collection of publicly accessible 'identifiable information' will be regulated by privacy rules.[21] Through amendments to be made to the *Crimes Act 1914* (Crimes Act) in the C&T Bill,[22] for the purposes of ONI carrying out its function under cl ^7(1)(g),[23] this collection could lawfully be effected where necessary via an assumed identity under and in accordance with Part IAC of the Crimes Act. This brings ONI broadly in line with ASIO and ASIS as being an intelligence agency that may apply for an authority to acquire or use an assumed identity under that Act (although with some limitations).[24]

Privacy implications

5.11. To the extent that the performance of its functions will require the collection, use or disclosure of personal information, ONI may be dealing with more identifiable information than ONA; that is, ONI may collect and handle the personal information of more Australian citizens. This means there is an increased need as compared with ONA for ONI, should it be established, to take steps to ensure the appropriate handling of such information.

5.12. Additionally, material collected using the new function in cl ^7(1)(g) is likely to be much less sensitive from its open source nature than information collected from other intelligence agencies.

b. The ONI Bill will facilitate ONI gathering of information, but impose obligations on its use and protection

5.13. ONA is not subject to a statutory information handling framework, although it has a statutory entitlement to certain kinds of information. The ONI Bill will provide ONI with a statutory right to gather certain information, which may include personal information and for other government agencies to provide it with such information, but will also impose obligations on ONI with regard to the use and protection of that information.

Existing arrangements under the ONA Act

5.14. Subject to relevant legislative and secrecy provisions, ONA may access information that relates to international matters collected by other Commonwealth agencies in accordance with their governing functions. This includes:

a. personal information about Australians for ONA's assessment or evaluation functions

---

21 See further below at 5.40 and following).

22 See cll 26-44 of the C&T Bill.

23 See proposed s 15KA(3) to be inserted by cl 32 of the C&T Bill.

24 Unlike other those other intelligence agencies, ONI will not be able to apply to a court for an order under Part IAC of the Crimes Act relating to the making of entries in a register of births, deaths or marriages (see cll 34 and 35 of the C&T Bill); it must also comply with requests from a participating jurisdiction for evidence of an assumed identity (see cl 42).

b. personal information about intelligence agency employees for ONA's evaluation functions.

5.15. More specifically, the Director-General of ONA is entitled under s 9 of the ONA Act to 'full access to all information relating to international matters that are of political, strategic or economic significance to Australia, being information in the possession of any Department, Commonwealth authority or arm of the Defence Force', except where furnishing that information would contravene the provisions of any law of the Commonwealth or any law of a Territory.

5.16. However, the ONA Act does not make any specific provision for the voluntary sharing of information with ONA by intelligence agencies or Commonwealth agencies more generally. In practice intelligence agencies and other Commonwealth agencies share information with ONA pursuant to the statutory functions and powers of those agencies and subject to any legislative or other restrictions on the disclosure of information, such as secrecy provisions and, where relevant for the particular agency, the Privacy Act.

5.17. As a matter of general administrative law principle, 'the purpose for which a power to require disclosure of information is conferred limits the purpose for which the information disclosed can lawfully be disseminated or used'.[25] Where a power to compel information is conferred under a statute, the power may only be used for the purpose for which it is conferred, whether stated expressly, or identifiable by implication. It follows that where information is obtained through the exercise of such a power, the information may not be used for purposes unrelated to the purpose for which it was obtained.

5.18. The ONA Act does not otherwise provide for any additional statutory restrictions on ONA's use of personal information. The 'ONA Guidelines to Protect the Privacy of Australians', which are currently administratively made, nevertheless provide that ONA may only communicate intelligence information concerning Australian persons 'where it is necessary to do so for the proper performance of ONA's functions or where such communications are required by law'.

The ONI Bill

5.19. The ONI Bill will give ONI the power to require Commonwealth authorities[26] to provide it with information relating to international matters in certain circumstances. The ONI Bill will also provide for the voluntary disclosure of information to ONI by:

- Commonwealth authorities for the purpose of ONI performing its functions under cl 7(1)(c) or (d)

---

25 *Johns v Australian Securities Commission* (1993) 178 CLR 408 at 423.

26 Defined in cl ^4 of the ONA Bill in a way that includes Commonwealth government agencies and Departments, the Defence Force, bodies established or continued in existence for a public purpose under a law of the Commonwealth (established bodies) and bodies corporate in which the Commonwealth or an established body has a controlling interest.

- intelligence agencies for the purposes of ONI performing its functions.[27]

Power to require the provision of information relating to international matters

5.20. Clause ^37 of the ONI Bill provides:

> **^37 Requirement to provide information, documents or things to ONI relating to international matters**
>
> (1) For the purpose of ONI performing its function under paragraph ^7(1)(c), the Director-General may make a written request that a Commonwealth authority provide information, documents or things in its possession that relate to:
>
> (a) international matters of political, strategic or economic significance to Australia; or
>
> (b) domestic aspects relating to such international matters.
>
> (2) Before making a written request of a Commonwealth authority under subsection (1), the Director-General must:
>
> (a) consult with the Commonwealth authority; and
>
> (b) consider any concerns raised by the Commonwealth authority, including concerns about:
>
> (i) a contract, arrangement or understanding that would prohibit or limit the Commonwealth authority's ability to provide information, documents or things that would otherwise need to be provided in response to a request; or
>
> (ii) the need to provide personal information (within the meaning of the *Privacy Act 1988*) in response to a request.
>
> (3) A Commonwealth authority must provide any information, documents or things to ONI in response to a written request by the Director-General under subsection (1), unless and to the extent that a law of the Commonwealth, or of a State or Territory prohibits the provision (however described) of the information, documents or things.
>
> Note: For limits on the use that ONI may make of such information, documents or things, see section ^40.

5.21. Before compelling the production of information that relates to international matters and domestic aspects relating international matters under cl ^37, the Director-General must consult with the relevant Commonwealth authority and consider any concerns raised, as specified in cl ^37(2), including any concerns about the 'need to provide personal information (within the meaning of the *Privacy Act 1988*) in response to a request' made pursuant to that provision.

5.22. Furthermore, any information provided pursuant to the compulsory information gathering power in cl ^37 may only be used for the purposes of ONI's function in cl ^7(1)(c) (i.e. analysis, assessments and reports relating to international matters). The only exception to this restriction is where the head of the Commonwealth

---

[27] Other obligations in relation to ONI's use and protection of identifiable information are also specified. These provisions are summarised below.

authority that provided the information gives written authorisation for its subsequent use in relation to the performance of another of ONI's functions, the exercise of ONI's powers, or the performance or exercise of the Director-General's functions or powers: cl ^40.

Voluntary provision of information

5.23. The ONI Bill authorises the voluntary provision of information to ONI by Commonwealth authorities and intelligence agencies, in certain circumstances. These provisions are each expressed in permissive terms, with the effect that where the agency, in its discretion, seeks to disclose information to ONI for the purposes of ONI's functions, the agency is authorised to do so, regardless of whether it could otherwise do so under the agency's own statutory functions.

5.24. Clause ^38(1) expressly provides that for the purpose of ONI performing its functions under cl ^7(1)(c) (analysis, assessments and reports relating to international matters) or (d) (analysis, assessments and reports relating to matters other than international matters), a Commonwealth authority 'may provide to ONI information, documents, or things that relate to matters of political, strategic or economic significance to Australia'.[28] Information may be provided to ONI even if doing so would not otherwise fall within the Commonwealth authority's statutory functions: cl ^38(2).

5.25. In addition, cl ^39(1) provides that for the purpose of ONI performing its functions, an intelligence agency or agency with an intelligence role or function may provide to ONI information, documents or things that relate, or may relate, to any of ONI's functions (cl ^39(1)). The relevant agency may provide information, documents or things to ONI under cl ^39 even if doing so would not otherwise fall within that agency's statutory functions (cl ^39(2)).

Use and protection of information

5.26. The ONI Bill will introduce new obligations on the Director-General in relation to the use and protection of certain information, documents or things.

5.27. As noted above at 5.22, cl ^40 ensures information, documents or things obtained in the exercise of the compulsory power in cl ^37 is only used for the purposes of the ONI's function under ^7(1)(c) unless the head of the relevant Commonwealth authority expressly agrees otherwise.

5.28. Clause ^41 of the ONI Bill makes special provision for the protection of information, documents or things provided to ONI under Division 1 of Part 1 of the Bill by intelligence agencies or an agencies with an intelligence role or function. This clause requires the Director-General to make arrangements with the head of the relevant agency for the protection of such material provided to ONI. Failing this, and subject to cl ^40, ONI must take all reasonable steps to ensure that the information,

---

[28] Note, while the draft reviewed limited cl 38(1) to matters '(other than international matters)', we understand this was a drafting error due to the express reference in that provision to cl ^7(1)(c).

documents or things provided by the relevant agencies are appropriately stored, accessed, used or further disclosed.

Privacy implications

5.29. These provisions of the ONI Bill will ensure that ONI has broad scope to collect information from other agencies, either compulsorily or voluntarily, for the purposes of its functions. This could include personal information.

5.30. The compulsory information gathering power in cl ^37 is broad and applies to 'Commonwealth authorities', itself a broadly defined term under the ONI Bill. However, the power is not entirely unconstrained. It is limited to only certain of ONI's functions. It can be exercised to compel the provision of information by Commonwealth authorities only for the purpose of the ONI performing its functions relating to international matters. Additionally, the Director-General is obliged to consider any privacy concerns raised by the relevant Commonwealth authority prior to the exercise of the power. This will ensure privacy considerations are relevantly considered in the exercise of the power.

5.31. The provisions supporting the voluntary disclosure of information relevant to the ONI's functions do not expressly require consideration of privacy. Clause ^38 is permissive of a Commonwealth authority providing information to ONI even if doing so would not otherwise fall within the scope of that authority's statutory functions.

5.32. Most Commonwealth authorities will be subject to the Privacy Act. Those agencies are subject to obligations under the Privacy Act that preclude personal information about an individual that was collected for a particular purpose being used or disclosed for a secondary purpose, unless the individual has consented to the use or disclosure, or a relevant exception applies.[29]

5.33. One such exception is where the use or disclosure of the information is 'required or authorised by or under an Australia law'. It appears that cl ^38(2) of the ONI Bill will enable Commonwealth authorities to voluntarily disclose personal information obtained for the purposes of their own functions to the ONI on the basis the disclosure will be 'required or authorised by law' for the purposes of the Privacy Act.

5.34. Clause ^39 similarly provides for the voluntary disclosure of information to ONI by intelligence agencies. As noted above when discussing the proposed amendments to the Privacy Act under the C&T Bill, these agencies will not be subject to the restrictions on the disclosure of personal information in the Privacy Act when disclosing information to ONI.[30]

---

[29] See in particular Australian Privacy Principle (APP) 6 in the Privacy Act. APP 6.1 relevantly prohibits the disclosure of personal information for a purpose other than that for which it was collected. APP 6.2 and 6.3 provide for various exceptions to the prohibition.

[30] We have not considered the implications of cll 38 or 39 for the disclosure of information to ONI other than to the extent the disclosing agency is otherwise subject to the Privacy Act. Commonwealth authorities and intelligence agencies will be subject to their own establishment legislation including applicable secrecy provisions when disclosing information to others, but any analysis of the secrecy provisions in other legislation is outside the scope of this PIA.

5.35. Significantly, ONI will have express legislative obligations in relation to the use and protection of information it collects, including personal information. Clause ^40 prohibits the use of information obtained in the exercise of the compulsory power in cl ^37 for purposes other than that for which it was obtained, except in very specific circumstances. To the extent that cl ^37 is used to compel the provision of personal information, it is expressly clear that it cannot generally be used for broader or other purposes. Furthermore, the obligation on ONI to make arrangements for the protection of information provided to ONI by other intelligence agencies emphasises the importance of proper and tailored handling and management of information, including personal information. These features of the ONI Bill are positive from a privacy management perspective.

c. The ONI Bill contains secrecy provisions restricting the communication of ONI information

5.36. ONI will be subject to a secrecy regime under which criminal penalties may be imposed in relation to unlawful communication of information. This regime will have obvious implications for the communication of personal information by ONI.

Existing arrangements under the ONA Act

5.37. ONA is subject to agency-specific offence provisions in the *Intelligence Services Act 2001* (**ISA**) relating to the unauthorised communication of information and unauthorised dealing with records and recording of information. There are also various Commonwealth laws which would restrict those working for ONA from disclosing official information.[31] However, the ONA Act itself makes no additional provision for the maintenance of confidentiality in, or secrecy of, information collected or held by the agency.

The ONI Bill

5.38. By contrast, ONI will be subject to the secrecy regime in Part 4 Division 2 of the ONI Bill. This includes a number of criminal offences relating to the unlawful communication of information:

a. Clause ^42 provides that it is an offence for a person who comes to know information held by ONI in connection to its functions, or otherwise relating to ONI's functions, because they are a staff member or contractor (or equivalent) of ONI to communicate that information within ONI unless this is in the course of their duties as a staff member or in accordance with the contract, and outside ONI unless they have authorisation.[32]

b. Clause ^43 provides that it is an offence for other persons (i.e. not current or former staff members or contractors) who come to know this type of information to communicate this information intending to cause harm to national security or

---

31 See for example s 70 of the *Crimes Act 1914*.

32 Clause ^42 is in analogous terms to existing s 40A of the ISA, which will be repealed by the C&T Bill, cl 79.

to endanger the health or safety of another person, or knowing that the communication will, or is likely to, have that effect.

c. Clause ^44 provides for offences concerning unauthorised dealing with records and unauthorised recording of this type of information.[33]

There are various exceptions to these offences, including if the information is lawfully available, or the communication is to the IGIS.

Privacy implications

5.39. It is beyond the scope of this PIA to analyse the operation of the ONI Bill's secrecy obligations and offence regime. However, it is relevant when considering the privacy impacts of the ONA Bill to observe that the secrecy provisions are more restrictive of the communication of ONI's information, including personal information, than the provisions in the Privacy Act relating to the disclosure of personal information.[34]

d. ONI will be required to comply with privacy rules in relation to 'identifiable information'

5.40. While ONA has administratively developed guidelines relating to privacy, ONI will be legislatively required to comply with privacy rules, aimed at the protection of identifiable information, promulgated for the agency by the Prime Minister following consultation with the IGIS and Attorney General.

Existing arrangements under the ONA Act

5.41. As already noted, ONA is exempt from the operation of the Privacy Act. Nothing in the ONA Act or any other legislation requires ONA to comply with any other form of privacy rules. Unlike the *Intelligence Services Act 2001* agencies (ASIS, AGO and ASD), ONA is not required by legislation to have agency specific privacy rules or guidelines in place. However, following a review of the *Intelligence Services Act 2001* co-ordinated by the Department in 2005-6, a decision was made that ONA should be subject to privacy guidelines consistent with those applicable to those other intelligence agencies. The current guidelines are the 'ONA Guidelines to Protect the Privacy of Australians' dated 23 June 2017 and available on ONA's website.

The ONI Bill

5.42. The ONI Bill requires under cl ^53 that the Prime Minister make rules (the **privacy rules**) regulating the collection of 'identifiable information' under cl ^7(1)(g) (collection, interpretation and dissemination of publicly accessible material), and the communication, handling and retention by ONI of 'identifiable information' generally. 'Identifiable information' is defined in cl ^4 in the same way as 'personal information'

---

33 Clause ^44 is in analogous terms to existing ss 44J and 44K of the ISA, which will be repealed by the C&T Bill, cl 79.

34 See in particular APP 6.

in the Privacy Act, except that it is limited to the information of Australian citizens and permanent residents[35] (rather than individuals generally).

5.43. Significantly, cl ^53(5) provides that ONI must not collect or communicate identifiable information except in accordance with the privacy rules.

5.44. In making the privacy rules, the Prime Minister must have regard to the need to ensure that the privacy of Australian citizens and permanent residents is preserved 'as far as is consistent with the proper performance by ONI of its functions' (cl ^53(3)). Further, the Prime Minister must consult with the Director-General, the IGIS and the Attorney-General before making the privacy rules, including by providing them with a copy of the proposed rules.

5.45. Draft privacy rules have been prepared which are in broadly analogous terms to the 2017 'ONA Guidelines to Protect the Privacy of Australians', and the privacy rules of ASIS, AGO and ASD. Like the ONA, ASIS, AGO and ASD privacy rules, the draft ONI privacy rules:

- state that identifiable information can only be retained, and may be communicated, where it is necessary to do so for the proper performance of ONI's functions, or where this is required or authorised by or under another Act,
- require that ONI take reasonable steps to ensure that identifiable information that ONI retains or communicates is recorded or reported in a fair and reasonable manner
- require that ONI take steps to facilitate the IGIS's oversight role, including providing IGIS access to all identifiable information held by ONI, consulting with the IGIS about communication, retention and handling of identifiable information, and advising the IGIS of any breach of these rules

5.46. In addition to these more general requirements, the draft privacy rules also impose specific obligations in relation to the collection of identifiable information under cl ^7(1)(g), including that:

a. the Director-General develop policies and procedures to be observed by ONI in the performance of this function

b. ONI obtain the authorisation of the Minister responsible for the Act before undertaking an activity for the specific purpose of collecting identifiable information, and the Minister may only give authorisation if satisfied of certain matters.

Privacy implications

5.47. The inclusion of a privacy rules regime in the ONI Bill clearly supports enhanced privacy protection. The proposed privacy rules are intended to be consistent with the analogous rules applying to other agencies in the NIC. Where necessary and

---

35 The definition of 'permanent resident' in cl ^4 includes a natural person who is a permanent resident and also certain (Australian) bodies corporate, which means 'identifiable information' in this respect has a broader meaning than 'personal information' which is limited to natural persons.

appropriate these agency specific privacy rules can be tailored in recognition of the nature and purpose of the agency's national security functions.

5.48. The privacy rules are to be made by the Prime Minister and not the agency itself. In making the proposed rules, the Prime Minister must consult not only with the Director-General of the agency, but also the IGIS and Attorney General. This consultation will ensure the rules are informed by the independent advice and consideration of both national security and broader legal perspectives, including in relation to privacy.

6. OVERALL EFFECT AND IMPACT OF THE CHANGES

6.1. Key aspects of the ONI Bill are positively directed towards the management and protection of personal information and privacy, but in a manner which is seen as appropriate to the functions of ONI as a national intelligence agency. Some of these requirements are broadly similar to those imposed on other agencies within the NIC, such as the statutory requirement to have privacy rules.

6.2. ONI's information collection and reporting functions are such that it can be expected to collect more information than ONA. This is recognised in the ONI Bill, which provides a stronger, more transparent regime for the handling and protection of personal information than currently exists for ONA.

OFFICE OF NATIONAL INTELLIGENCE RULES TO PROTECT THE PRIVACY OF AUSTRALIANS

I, Scott Morrison, Prime Minister of Australia, being the Minister responsible for the Office of National Intelligence (ONI), make these Rules in accordance with section 53 of the *Office of National Intelligence Act 2018* (the Act).

In making these Rules, I have had regard to the need to ensure that the privacy of Australian persons is preserved as far as is consistent with the proper performance by ONI of its functions. Any activity undertaken by ONI must be proportionate to a legitimate end and be necessary in the circumstances. In the execution of ONI's functions, it will adhere to the principles of necessity, proportionality and propriety; meaning that consideration of the nature and consequences of the acts to be done will be weighed against the purposes for which they are carried out.

Before making the Rules, I:

a. consulted the Director-General of ONI, the Inspector-General of Intelligence and Security (IGIS) and the Attorney-General; and
b. provided a copy of the rules I was proposing to make to the Director-General of ONI, the IGIS and the Attorney-General.

Dated this the XX day of XX 2018.

[Signed] Scott Morrison

DEFINITIONS

Expressions used in these Rules have the same meaning as in the Act.

Assumed identities regime means the provisions contained in Part IAC of the *Crimes Act 1914*.

Australian person has the same meaning as in section 3 of the *Intelligence Services Act 2001*.

Identifiable information means information or an opinion about an identified Australian person, or an Australian person who is reasonably identifiable:

a. whether the information or opinion is true or not; and
b. whether the information or opinion is recorded in material form or not.

Publicly accessible information includes information that has been published or broadcast for public consumption, is available on request to the public, is accessible online (including through social-media platforms) or otherwise to the public, is available to the public by subscription or purchase, is made available at a meeting open to the public, or is obtained by visiting any place or attending any event that is open to the public, and includes information that requires conditions to be met before it can be accessed. In order to qualify as 'publicly accessible information', information need not be available to all sections of the public.

> Note: Examples of conditions that are required to be met before information can be accessed include a requirement to pay a fee or be a member of a group.

Minister means the Prime Minister, or any minister within the Prime Minister and Cabinet portfolio.

Ministerial Privacy Approval means an approval granted under rule 2.4.

National Intelligence Community agency has the same meaning as in section 4 of the Act.

Serious crime has the same meaning as in section 3 of the *Intelligence Services Act 2001*.

RULE 1 – PRESUMPTIONS ABOUT WHO IS AN AUSTRALIAN PERSON

1.1 For the purposes of these Rules, where it is not clear whether a person is an Australian person, the following presumptions shall apply unless there is evidence to the contrary, including from the context in which the information was collected or the content of the information:

a. a person within Australia is presumed to be an Australian person; and
b. a person outside Australia is presumed not to be an Australian person.

RULE 2 – COLLECTION OF IDENTIFIABLE INFORMATION

2.1 ONI, in the performance of its functions under paragraph 7(1)(g) of the Act, may collect publicly accessible information that is of political, strategic or economic significance to Australia.

2.2 ONI's Open Source Centre (OSC) is the only part of ONI which may carry out ONI's function described in paragraph 7(1)(g) of the Act.

Note: The Director-General may develop policies and procedures in relation to the performance of ONI's functions under paragraph 7(1)(g) of the Act.

2.3 The OSC is the only part of ONI which may use the assumed identities regime. The assumed identities regime may only be used:

a. to facilitate ONI's access to online platforms; and
b. in the performance of its functions under paragraph 7(1)(g) of the Act.

Additional conditions to be met before undertaking certain collection activities

2.4 ONI must obtain the approval of the Minister before the OSC undertakes activities where the following criteria apply:

a. an assumed identity will be used; and
b. the proposed activities have the specific purpose of collecting identifiable information.

2.5 Before the Minister gives a Ministerial Privacy Approval, the Minister must be satisfied that:

a. any activities which may be done in reliance on the Ministerial Privacy Approval are necessary for the proper performance of ONI's functions under paragraph 7(1)(g) of the Act; and
b. there are satisfactory arrangements in place to ensure that nothing will be done in reliance on the Ministerial Privacy Approval beyond what is necessary for the proper performance of ONI's functions under paragraph 7(1)(g) of the Act; and
c. there are satisfactory arrangements in place to ensure that the nature and consequences of activities done in reliance on the Ministerial Privacy Approval will

be reasonable, having regard to the purposes for which the activities are carried out.

Ministerial Privacy Approvals in an emergency

2.6 If the Director-General considers it necessary or desirable for ONI to undertake activities that would require a Ministerial Privacy Approval and is satisfied that the Minister is not readily available or contactable, the Director-General may approve the activities without first obtaining a Ministerial Privacy Approval. The Director-General must be satisfied of the matters specified in rule 2.5 before giving an approval.

2.7 If the Director-General gives an approval under rule 2.6, the Director-General must notify the Minister within 72 hours after the Director-General's approval is given.

2.8 If the Minister is notified by the Director-General under rule 2.7, the Minister must consider whether to give a Ministerial Privacy Approval in relation to the activities. If the Minister does not give a Ministerial Privacy Approval within 24 hours of receiving notification, the activities must cease, and the approval granted by the Director-General under rule 2.6 is of no further force or effect.

2.9 If the Director-General gives an approval under rule 2.6, the Director-General must advise the IGIS within 96 hours of giving the approval.

RULE 3 – RETENTION AND HANDLING OF IDENTIFIABLE INFORMATION

3.1 ONI may only retain identifiable information where it is necessary to do so for the proper and lawful performance of ONI's functions, or where the retention is otherwise authorised or required by law.

3.2 Where ONI retains identifiable information, ONI must ensure that:

a. the information is protected by such security safeguards as are reasonable in the circumstances against loss, against unauthorised access, use, modification or disclosure, and against other misuse; and
b. access to the information is only provided to persons who require such access for the proper performance of an ONI function.

RULE 4 – COMMUNICATION OF IDENTIFIABLE INFORMATION

4.1 ONI may only communicate identifiable information where it is necessary to do so for the proper performance of ONI's functions or where such communication is authorised or required by or under another Act.

4.2 This rule applies in addition to rule 4.1. ONI may communicate identifiable information concerning an Australian person only where:

a. the information is publicly accessible; or

b. the information concerns activities of an Australian person in respect of which the Australian person is a representative of the Commonwealth or a State or Territory in the normal course of official duties; or
c. the communication of the identifiable information is reasonably necessary for the purposes of:
    (i) maintaining Australia's national security;
    (ii) maintaining Australia's national economic well-being;
    (iii) promoting Australia's foreign relations;
    (iv) preventing or investigating the commission of a serious crime;
    (v) responding to an apparent threat to the safety of a person; or
d. the information relates to an Australian person who is, or is likely to be:
    (i) acting for, or is suspected of acting for, or on behalf of a foreign power;
    (ii) involved in activities related to the proliferation of weapons of mass destruction or the movement of goods listed from time to time in the Defence and Strategic Goods List (within the meaning of regulation 13E of the *Customs (Prohibited Exports) Regulations 1958)*;
    (iii) involved in activities related to a contravention, or an alleged contravention, by a person of a UN sanction enforcement law; or
e. the information was, at the time of collection, collected in accordance with a Ministerial Privacy Approval granted under rule 2.4; or
f. the information relates, or appears to relate, to the performance of the functions of an intelligence agency or an agency with an intelligence role or function, and the information is provided by ONI to that agency; or
g. the information was provided to ONI by an intelligence agency or an agency with an intelligence role or function for the purposes of ONI's functions under paragraph 7(1)(d); or
h. the subject of the information has consented, either expressly or impliedly, to the communication of that information for use in accordance with ONI's functions.

RULE 5 – ACCURACY OF INFORMATION

5.1 ONI is to take reasonable steps to ensure that identifiable information that ONI retains or communicates is retained or communicated in a fair and reasonable manner.

RULE 6 – OVERSIGHT BY THE IGIS

6.1 To facilitate the oversight role of the IGIS, ONI is to take the following measures:
a. the IGIS is to have access to all identifiable information held by ONI;
b. the IGIS is to be consulted about the processes and procedures applied by ONI to the collection, communication, retention and handling of identifiable information;
c. where a presumption under rule 1 has been found to be incorrect, ONI is to advise the IGIS of the incident and measures taken by ONI to protect the privacy of the Australian person; and

d. in any case where a breach of these rules is identified, ONI is to advise the IGIS of the incident and the measures taken by ONI to protect the privacy of any affected Australian person or of Australian persons generally.

RULE 7 – PUBLIC ACCESS TO THE RULES

7.1 ONI is to ensure a copy of these rules is publicly available on the ONI website.