**Australian Government**

**Attorney-General's Department**

**National Security Law & Policy Division**

14/11411

9 September 2014

James Nelson
a/g Inquiry Secretary
Parliamentary Joint Committee on Intelligence and Security
pjcis@aph.gov.au

Dear James

**Inquiry into the National Security Legislation Amendment Bill (No 1) 2014**

The Department is aware that a number of late and supplementary submissions to the above inquiry were published on 28 August 2014 and 4-5 September, and that a Bills Digest was also published by the Parliamentary Library on 28 August.

To assist the Committee in its consideration of the issues raised in these materials, I enclose a further supplementary submission from the Department. This responds to commentary on some measures in Schedules 1-6 to the Bill. The balance of issues are addressed in the Department and ASIO's joint supplementary submission to the Committee (provided in a classified form on 26 August, and in unclassified form on 29 August) and the Department's responses to matters taken on notice at the public hearing on 15 August (provided on 18 August).

Please contact me on or if the Department may be of any further assistance to the Committee in completing its inquiry.

Yours sincerely

Annette Willing
National Security Legal Adviser

UNCLASSIFIED

**Attorney-General's Department**
**Supplementary submission**

**Parliamentary Joint Committee on Intelligence and Security**
**Inquiry into the National Security Legislation Amendment Bill (No 1)**
**8 September 2014**

**Contents**

## Introduction

The Attorney-General's Department (Department) is pleased to provide a second supplementary submission to the Parliamentary Joint Committee on Intelligence and Security (PJCIS) inquiry into the National Security Legislation Amendment Bill (No 1) 2014 (the Bill). This submission is provided in response to issues raised in a number of supplementary or late submissions to the Committee, which were published on 28 August 2014.

While most issues raised in these additional materials have already been the subject of commentary in the Department and ASIO's first joint supplementary submission to the Committee (provided on 26 August, and in unclassified form on 29 August), this second supplementary submission addresses a small number of new matters which have been raised in supplementary submission 2.1 (Gilbert + Tobin Centre of Public Law), submission 28 (Australian Human Rights Commission), and in the Bills Digest which was published by the Parliamentary Library on 28 August 2014. These matters relate to certain measures in Schedules 2-6 to the Bill.

## Schedule 2 – computer access warrants

### Definition of computer – coverage of multiple networks

The Bills Digest commented that "it is unclear why the definition of computer needs to refer to 'one or more' computer networks" and suggested that amending items 16[1] and 18[2] of Schedule 2 "would appear to cover the only circumstances in which it might be appropriate to authorise access to more than one computer network under a single warrant".[3]

The Department confirms that it is necessary to include one or more computer networks in the new definition of 'computer' in order to ensure that ASIO's computer access warrants keep pace with developments in computer networking technology and its contemporary usage. Individual devices can be readily connected to multiple computer networks, and individual computer networks can be related to each other. In all cases in which a warrant is sought in relation to a target computer that comprises one or more computer networks, the Attorney-General must be satisfied that there are reasonable grounds on which to believe that access to data held in that target computer will substantially assist in the collection of intelligence in respect of a security matter. The Attorney-General must further be satisfied that the activities authorised under the warrant are appropriate in the circumstances, and any access to data held in the target computer network by ASIO under the warrant must be for the purpose of accessing data relevant to the security matter.

---

1 Amending item 16 removes the word 'particular' from the issuing criteria in s 25A(2), so the Minister must be satisfied that there are reasonable grounds for believing that access by the Organisation to data held in a computer (the target computer) will substantially assist in the collection of intelligence in respect of a matter that is important to security (security matter).

2 Amending item 18 inserts a new s 25A(3) which specifies that a target computer may be any one or more of a particular computer, a computer on particular premises, or a computer associated with, used by or likely to be used by, a person (whose identity may or may not be known).

3 Bills Digest, National Security Legislation Amendment Bill (No 1) 2014, 28 August 2014, p. 13.

Contrary to the suggestion in the Bills Digest, amending items 16 and 18 do not adequately cover the situation in which a device may be used to access more than one computer network, and it is reasonably believed that access to data held in the computer networks will substantially assist the collection of intelligence relevant to a security matter. Amending item 16 removes the reference to a 'particular' target computer in s 25A(2), while amending item 18 inserts a new s 25A(3) which provides that a target computer in s 25A(2) may comprise a particular computer or computers; computers on particular premises; or computers associated with, used or likely to be used by a person specified in the warrant, whose identity may or may not be known.

As noted in the Explanatory Memorandum (EM), the amendments to the definition of a computer, together with those in amending items 16 and 18, are necessary to address the following circumstances (it is noted that, although the example given in the EM pertains to a computer system, it could feasibly apply to a computer network):

> Currently, computer access warrants under section 25A of the ASIO Act authorise access to data that is held in a 'particular computer'. If an individual has more than one computer which is not part of the same computer system, more than one warrant will be necessary (for example, if there are multiple computers on a premises and it is only discovered upon entering the premises for the purpose of executing a warrant that a particular computer is not connected to the computer system specified in the warrant, ASIO would be required to seek another warrant and enter the premises a second time, in order to access the data on that particular computer). Also, with the variety of computers and electronic devices now commonly used by individuals, it is highly probable that a person may store data on a number of computers (for example, a laptop, a phone and a tablet PC).
>
> These amendments update the warrants process under the ASIO Act to better reflect the way people use computer technology in the modern world, by allowing ASIO to seek computer access warrants to identify the computers, computer systems or computer networks to which access is authorised by reference to a specified person or premises. In combination with the updated definition of computer in section 22, this amendment will enable a computer access warrant to authorise ASIO to use computers, computer systems and computer networks located at a particular premises or associated with a nominated person in order to obtain intelligence relevant to a matter that is important in relation to security and held in the relevant computers, computer systems or computer networks.[4]

## Thresholds for accessing computer networks

The Gilbert + Tobin Centre of Public Law suggested, in its supplementary submission to the Committee, that an additional test should apply to decisions by the Attorney-General to issue computer access warrants. The Department understands that this test is intended to limit the number of computers that could be accessed on a network (where the target computer is a network) to those which are reasonably necessary to collect the intelligence in respect of the security matter for which the warrant was sought.

4 Explanatory Memorandum, National Security Legislation Amendment Bill (No 1) 2014, p. 69 at [288]-[269].

The Centre provided the following illustrative provision:[5]

> **Section 25A Computer Access Warrant**
>
> (2A) The warrant may only authorise access to those parts of the target computer that are reasonably necessary for the collection of intelligence in respect of the security matter.

As noted in the Department and ASIO's first joint supplementary submission to the Committee, an additional issuing test to that in s 25A(2) is not considered necessary or appropriate. It may not be possible to identify, in advance of access to a target computer, which parts of a target computer are 'reasonably necessary' to access for the purpose of collecting intelligence in respect of the security matter. Where that is known in advance, ASIO may limit its warrant application to part of a computer, or the Attorney-General may issue the warrant subject to a restriction or condition that it is limited to part of a computer, in accordance with new s 25A(3A) (currently s 25A(3)). In obtaining intelligence by warrant, ASIO is required to adhere to the Attorney-General's Guidelines issued under s 8A of the ASIO Act. The Guidelines specifically require ASIO to use as little intrusion into individual privacy as possible, consistent with the performance of ASIO's functions, and wherever possible use the least intrusive techniques of information collection before more intrusive techniques.

For the reasons set out in the first joint supplementary submission, the Department is of the view that an adequate and appropriate limitation on the power to access computers is found in the existing linkage of issuing and authorisation decisions in ss 25A(2) and 25A(4) to a 'security matter' – being a matter that is important in relation to 'security' (as that term is defined in s 4).

As noted in the first joint supplementary submission, the Department and ASIO will assist the Government in giving consideration to amending the EM to the Bill to explain what is meant by a 'security matter'. Alternatively, clarification could be inserted in the Attorney-General's Guidelines to ASIO.[6]

### Third party computer use

The Australian Human Rights Commission (AHRC) recommended amendments to the test for authorising the use of a third party computer or a communication in transit to gain access to relevant data in a target computer in proposed s 25A(4)(ab). The AHRC recommended that the test should be, "if, having regard to other methods (if any) of obtaining access to the relevant data which are likely to be as effective, it is *necessary* [replacing 'reasonable'] in all the circumstances to do so *and having regard to the rights of individuals to privacy*". This was said to "better protect against arbitrary interferences of privacy" in recognition that "accessing third party computers where the individuals are not a direct threat to security in order to gain access to the target computer is a potentially broad power".[7]

---

5 Gilbert + Tobin Centre of Public Law, *Submission 2.2*, p. 2.

6 AGD and ASIO, *Joint Supplementary Submission (unclassified)*, 29 August 2014, pp. 15-21.

7 Australian Human Rights Commission, *Submission 28*, p. 10 (recommendation 1).

As noted in the Department and ASIO's first joint supplementary submission, replacing the current standard of 'appropriate' with that of 'necessary' would significantly and inappropriately limit the utility of ASIO's computer access warrants. It would implement a *de facto* 'last resort' requirement, in that it would be necessary to show that the use of a third party computer is essential or critical to achieving the purpose of gaining access to the relevant data on the target computer. It would mean that ASIO may be unable to access relevant data on a target computer because methods other than the use of a third party computer exist, even though they may be less effective and carry a higher operational risk.[8]

As further noted in the Department and ASIO's first joint supplementary submission, a specific statutory privacy test is not considered necessary in s 25A, or any other provision in Division 2, because the objective of such a suggestion is already addressed through a range of existing mechanisms, including the issuing thresholds, the Attorney-General's Guidelines to ASIO and the oversight role of the Inspector-General of Intelligence and Security (IGIS).[9]

**Material interference**

The AHRC also recommended amendments to the proposed limitations in ss 25(6) and 25A(5) of the ASIO Act "so that only minor or inconsequential (or immaterial) interference with computers is permitted in all the circumstances". The AHRC "considers that allowing material interference that is necessary to execute the warrant is not proportionate to the legitimate aim of gathering security intelligence".[10]

The proposed limitations in ss 25(6) and 25A(5) generally prohibit ASIO doing anything under a computer access warrant or a search warrant (to the extent it is authorised under s 25(5)) that is likely to materially interfere with, interrupt or obstruct the lawful use of a computer. There is a limited exception where the action is necessary to do the relevant things authorised by the warrant.

ASIO needs to be able to undertake such action that is necessary to execute its warrants to assist in the legitimate aim of collecting of intelligence relevant to security. Otherwise the utility of ASIO's computer access warrants is significantly compromised.

As identified above, the Department and ASIO consider a "necessary" test to be a significant limitation, placing in effect a *de facto* 'last resort' requirement on an action that is likely to materially interfere with the lawful use of a computer. For ASIO to be able to rely on the limited exception, it would be necessary to show that the action likely to cause the material interference is essential or critical to doing the relevant things authorised by the warrant.

As identified in the Department and ASIO's first joint supplementary submission, there is a strong operational need to ensure minimal interruption or interference is caused given the

8 AGD and ASIO, *Joint Supplementary Submission (unclassified)*, 29 August 2014, pp. 22-23.

9 AGD and ASIO, *Joint Supplementary Submission (unclassified)*, 29 August 2014, pp. 59-60.

10 AHRC, *Submission 28*, p. 11 (recommendation 2).

covert nature of ASIO's computer access operation. As such, a material interference would be extremely rare.[11]

## Schedule 2 – entry to third party premises

The AHRC commented on the ability to authorise entry to third party premises for the purpose of gaining entry to, or exiting, the subject premises of a search warrant, or for the purpose of executing a computer access or surveillance warrant. The AHRC submitted that, "in order to restrict this power to that which is justified and proportionate, entering third party premises should be limited to cases where it is necessary to execute the warrant, having regard to other means of executing the warrant".[12]

Consistent with the above comments in relation to a test of 'necessity', the Department does not support such an amendment to the provisions authorising entry to third party premises for the limited purposes of executing a warrant in proposed ss 25(4)(aa) (search warrants), 25A(4)(aaa) (computer access warrants) and 26B(1)(g) (surveillance device warrants).

As noted in the EM to the Bill, the limited power of entry to third party premises will cover those circumstances in which there is no other way to gain access to the subject premises or to execute the warrant (for example, in an apartment complex where it is necessary to enter the premises through shared or common property). However, as further noted in the EM it is important that the power is not limited to these circumstances alone. The amendment is intended to make clear that ASIO can enter third party premises where, for operational reasons, the best means of entry might be through adjacent premises, having regard to the risk to the operation and safety of participants that is presented by other means of entry (such as through the main entrance to the subject premises). The amendment is also intended to make clear that ASIO can enter third party premises in emergency and unforeseen circumstances (for example, where a person arrives at the subject premises unexpectedly during a search and exit through third party premises is the best way of avoiding detection).[13] A 'necessity' test would have the effect of removing or severely constraining ASIO's ability to access third party premises in these legitimate circumstances.

## Schedule 3 – special intelligence operations

### Limited immunity from legal liability – proposed s 35K

The AHRC suggested that the limited immunity from criminal and civil liability conferred by proposed s 35K should be subject to an additional condition, that the special intelligence conduct engaged in was "necessary and there were no other means of obtaining the security information".[14]

---

11 AGD and ASIO, *Joint Supplementary Submission (unclassified)*, 29 August 2014, p. 18.

12 Australian Human Rights Commission, *Submission 28*, p. 11 (recommendation 3).

13 Explanatory Memorandum, National Security Legislation Amendment Bill (No 1) 2014, pp. 69-70 at [272]-[273].

14 Australian Human Rights Commission, *Submission 28*, p. 13 (recommendation 5).

The Department does not support this additional condition, which does not have an equivalent in the regime of controlled operations in Part 1AB of the Crimes Act. Applying such a condition would remove the utility of the proposed scheme of special intelligence operations, which is to provide certainty to participants in relation to their legal liability, provided that they act for the purposes of the operation and in accordance with a prior authorisation to engage in specific conduct.

An assessment of whether conduct is 'necessary' in relation to a particular purpose, as distinct from a lesser concept such as 'effective', is a question of fact in the circumstances of an individual case. The same view applies to any assessment of the existence or otherwise of other possible means of obtaining relevant intelligence in the circumstances. As such, there is considerable scope for differences of opinion to arise in the assessment of these matters. This leaves open an unacceptable risk that participants in special intelligence operations may be reluctant to engage in authorised conduct due to the risk that, for example, a jury might view a particular action as merely 'effective' as distinct from 'necessary', notwithstanding that it has been authorised in accordance with proposed s 35C. There is similarly a risk that some duly authorised operations may not commence or may be ceased for this reason.

Accordingly, the Department submits that the appropriate test for the existence of an immunity is that found in proposed s 35C(2), under which the Director-General or a Deputy Director-General must be satisfied of the relevant matters, which include: that the circumstances are such as to justify the conduct of a special intelligence operation; that any unlawful conduct will be limited to the maximum extent consistent with conducting an effective special intelligence operation; and that the conduct will not involve the causation of death or serious injury to any person, the commission of a sexual offence, or the causation of serious loss of or damage to property, or conduct in the nature of entrapment. Proposed s 35K provides an appropriate level of certainty that, if the conditions of an authority are complied with, the immunity from civil and criminal liability applies as a matter of law.

**Disclosure offence – proposed s 35P(1)**

The AHRC suggested that the 'basic offence' in proposed s 35P(1) for the disclosure of information relating to a special intelligence operation, where a person is reckless as to that circumstance, should be amended "so that it is an offence for a person to disclose information where the information relates to an SIO and disclosure of the information is likely to endanger the health or safety of any person or prejudice the effective conduct of an SIO". This was said to be appropriate because the offence as drafted does not, in the AHRC's view, contain "a sufficient, direct and immediate connection between the limitation on [the right to freedom of expression] and the threat". In particular, it was noted that the offence will apply to journalists and others who "may not even know that an SIO has been authorised".[15]

15 Australian Human Rights Commission, *Submission 28*, p. 14 (recommendation 7). The Bills Digest (at pp. 29-30) also commented that "an exception or defence to the proposed offence – at least to the basic offence, which does not require any intended harm – would provide much clearer protection for public interest disclosures".

In the first joint supplementary submission to the Committee, the Department and ASIO strongly opposed a suggestion that any of the disclosure offences in the Bill should require the prosecution to prove that the person intended to cause harm, or that the unauthorised conduct was likely to cause harm. It was noted that the wrongdoing to which the offences, including s 35P, is directed is the harm inherent in the disclosure of information that is, by its very nature, highly sensitive. In essence, significant damage to people and the integrity of an operation can be caused by a disclosure of information relating to special intelligence operation, and often the implications may not be fully understood by a discloser. The proposed offences in s 35P are required to deter those considering such a disclosure, and encourage them to do so through the IGIS or under the Public Interest Disclosure Act where applicable, rather than other means that will necessarily create, at the very least, a significant risk of prejudice to a special intelligence operation and the safety of its participants.

In the case of s 35P(1), it is considered that the disclosure of the existence of a special intelligence operation – which is intended to remain covert – is, by its very nature, likely to cause harm to security interests. This includes both the risk of prejudicing the effective conduct of the operation, and the risk of jeopardising the safety of its participants or persons associated with those participants such as family members. The corresponding offences in ss 15HK and 15HL of the Crimes Act, concerning unauthorised disclosures of information relating to controlled operations, have been enacted on this basis and were found acceptable to the Parliament in 2010.

In addition, the AHRC has, in its media release[16] and other media comments[17] on its submission to the inquiry, described these offences as applying strict liability. This is not accurate. The offences apply the standard fault elements in Chapter 2 of the Criminal Code. These are that:

- the person intended to disclose the information: ss 35P(1)(a) and 35P(2)(a);
- the person was reckless as to the circumstance that the information related to a special intelligence operation in proposed ss 35P(1)(b) and 35P(2)(b); and
- in the case of the aggravated offence in proposed s 35P(2)(c), the person intended to endanger the health or safety or prejudice the effective conduct of a special intelligence operation; or the person was reckless that the disclosure of the information will do so.

16 Australian Human Rights Commission, 'Commission responds to National Security Legislation Amendment Bill (No 1) 2014', media release, 1 September 2014. (https://www humanrights.gov.au/news/media-releases/commission-responds-national-security-legislation-amendment-bill-no1-2014).

17 Commissioner Tim Wilson, interview with Fran Kelly, ABC Radio National, 1 September 2014, (http://www.abc.net.au/radionational/programs/breakfast/anti-terror-laws-must-not-restrict-rights-human-rights-commn/5709522).

**Duration of authorisations and authorising officers**

The AHRC has suggested that the duration and authorisation framework for special intelligence operations should align with that in the Crimes Act for controlled operations. (Namely, the maximum duration should be three months, renewable in three-month increments up to a total duration of 24 months, and a nominated member of the Administrative Appeals Tribunal should be the authorising officer in relation to extensions beyond the initial period of three months.)

The Department and ASIO refer to the first joint supplementary submission at pp. 25-30 (authorising officer) and 36-37 (duration of authority).

## Schedule 4 – ASIO cooperation with the private sector

**Limitations on the purpose of disclosure and misuse of information by third parties**

The AHRC commented that proposed s 19(1)(d) "would potentially allow ASIO to cooperate with private entities, including foreign ones, with fewer restrictions that apply to it when cooperating with foreign governments". The AHRC stated that it was concerned the provision "would allow ASIO to share sensitive personal information with a person or organisation it chooses, with very little recourse in the event that person or organisation subsequently misused or released the information".

The AHRC noted that, while the Attorney-General may make directions under s 19(1) and issue Guidelines under s 8A in respect of private sector cooperation, there is no obligation on him or her to do so. The AHRC further commented that the offence in s 18(2) for the unauthorised communication of information may not apply because the information may not be disclosed by ASIO under a contract, agreement or other arrangement. On this basis, it recommended that s 19(1)(d) be amended to limit the purposes for which personal information may be divulged to private sector entities, and restrict any misuse or release of such information by those entities.[18]

The AHRC and other submitters to the inquiry have correctly observed that there is no formal legal obligation on the Attorney-General to make directions under s 19(1) of the ASIO Act in relation to proposed s 19(1)(d) or any other ground in paragraphs (a)-(c). The Department will assist the Government in giving consideration to making a commitment to issuing such directions, or to the possible inclusion of a legislative requirement that the issuing of directions by the Attorney-General is a condition precedent to ASIO's ability to engage in activities under proposed s 19(1)(d).

The Department further notes that the privacy requirements in the Attorney-General's Guidelines to ASIO will apply to activities undertaken under proposed s 19(1)(d), including a

18 Australian Human Rights Commission, *Submission 28*, pp. 15-16 (recommendation 8). The Bills Digest also commented (at p. 32) that "consideration should be given to how cooperation under the proposed provision might be more narrowly circumscribed without unduly limiting necessary cooperation, by requiring some form of Ministerial approval, direction or guidelines".

requirement that the Director-General must take all reasonable steps to ensure that personal information shall not be collected, used, handled or disclosed by ASIO unless that collection, use, handling or disclosure is reasonably necessary for the performance of its statutory functions (or as otherwise authorised or required by law). In addition, ASIO is required under the Guidelines to keep appropriate records of all of its communications of personal information for purposes relevant to security, or as otherwise authorised. Such records are open to inspection by the IGIS. The Director-General is further required to ensure that all such personal information collected or held by ASIO is protected by reasonable security measures against loss and unauthorised access, use or modification.

As previously noted, ASIO's activities under proposed s 19(1)(d) would be subject to oversight by the IGIS, which can include an assessment of ASIO's compliance with the Attorney-General's Guidelines in undertaking such cooperation. The Department and ASIO will also assist the Government in considering whether the Guidelines could be reviewed to take specific account of the proposed measures in the Bill, as suggested by other participants in the inquiry, including the Office of the Australian Information Commissioner.

Further, the Department notes that the potential for the misuse of personal information by any private sector entities to whom such information may be disclosed is likely to be caught by the unauthorised communication offence in s 18(2) of the ASIO Act. This is on the basis that these recipients are likely to be in a type of 'arrangement' with ASIO – being a relationship for the sharing of information. It would be possible for ASIO to place conditions or limitations on the use of that information by the recipient entities, with the result that the offence will apply to disclosures in contravention of those conditions or limitations. It is further noted that the amendments in Schedule 6 to the Bill will provide that the broadest category of extended geographical jurisdiction under s 15.4 of the Criminal Code will apply to the relevant offences, including that in s 18(2). This means that a person or body corporate is liable to prosecution, whether or not it has a connection to Australia, and whether or not the conduct occurred wholly outside of Australia.

## Schedule 5 – new Ministerial authorisation ground

### Meaning of 'operational security'

The AHRC commented that "it is not entirely clear what kinds of conduct or potential conduct would satisfy the requirements of the new definition of 'operational security'." It commented that "if the intention is to allow ASIS to be authorised to produce intelligence about Australians in all circumstances where to do so would reduce the risk that ASIS would rely on inaccurate information, the provision might well be seen to allow authorisation of the production of intelligence in *any* circumstances, as further intelligence will presumably *always* reduce the risk of false information being relied upon". It was suggested that consideration could be given to limiting the scope of the ground to persons engaged in

activities designed to deliberately induce ASIS to rely on false information.[19] It was recommended that the definition should be clarified to reflect any such intention.

While recognising that this is a matter on which the Foreign Affairs portfolio may wish to comment, the Department is of the view that the scenario raised in the AHRC's submission will not eventuate. The proposed new ground will not allow authorisation of the production of intelligence on the basis that further intelligence would reduce the risk of false information being relied upon. The new ground only applies to the production of intelligence on an Australian person who is, or who is likely to be involved in, activities that pose a risk, or which are likely to pose a risk, to the operational security of ASIS. Paragraph 9(1A)(a) and proposed subparagraph (iiia) make clear that there must be a more significant connection between the specific activities of the Australian person and a risk to the operational security of ASIS.

In addition, s 9(1) requires the Minister to be satisfied of a range of matters before giving an authorisation. These include satisfaction that any activities which may be done in reliance on the authorisation will be necessary for the proper performance of a function of the agency concerned; there are satisfactory arrangements in place to ensure that nothing will be done in reliance on the authorisation beyond what is necessary for the proper performance of a function of the agency; and that there are satisfactory arrangements in place to ensure that the nature and the consequences of acts done in reliance on the authorisation will be reasonable, having regard to the purposes for which they are carried out.

Importantly, the concept of 'necessary' goes beyond that which is merely convenient, useful or relevant to a particular purpose. It requires that the activities must be reasonably appropriate and adapted to the purpose. In addition, the explicit requirement that the Minister must consider the reasonableness of the proposed actions also tends strongly against the risk suggested by the AHRC that the proposed ground may be relied upon indiscriminately. A further, significant safeguard is that any intelligence produced may only be retained and communicated in accordance with the rules to protect the privacy of Australians made by the Minister under s 15 of the Intelligence Services Act.

The Department is further of the view that there is no utility in limiting the proposed operational security ground to authorise only the production of intelligence on persons engaged in activities designed to deliberately induce ASIS to rely on false information. The adverse consequences of reliance on false or inaccurate information – whether it is provided with a malicious intent or otherwise – are potentially significant. Basing the ground on an assessment of the subjective intent of the relevant person would impose an arbitrary distinction between those activities capable of being authorised and those which are not.

**Proposed limitation of the ground to national security functions**

The AHRC further commented that the justification for proposed s 9(1A)(a)(iiia) in the Human Rights Statement of Compatibility in the Explanatory Memorandum to the Bill did

[19] Australian Human Rights Commission, *Submission 28,* p. 17.

not disclose a legitimate objective to limit the right to privacy in Article 17 of the International Covenant on Civil and Political Rights (ICCPR).

The AHRC noted that the Statement of Compatibility identified the conducting of counter-intelligence as a legitimate objective. However this was said to be overly broad because the purpose of such counter-intelligence is not limited to the protection of national security, and extends to the other functions in s 11 of the Intelligence Services Act, which include Australia's foreign relations and national economic wellbeing. The AHRC suggested that "these matters appear likely to go beyond factors that could justify the serious restriction on the right to privacy entailed by producing intelligence on the individual". The AHRC further expressed the view that "the government has not provided an adequate justification for these proposed amendments". It also recommended that the ground should be limited to the production of intelligence on Australian persons only for the purpose of protecting national security.[20]

The AHRC appear to be operating under some misconception regarding important concepts in the Act. Section 11 establishes boundaries to ASIS's functions which are set out in s 6 of the Act. The functions can only be performed in the interests of Australia's national security, Australia's foreign relations or Australia's national economic wellbeing and only to the extent that these matters are affected by the capabilities, intentions or activities of persons or organisations outside Australia. Counter-intelligence is not just about the protection of national security. ASIS's counter-intelligence function is intrinsic to ASIS's risk management regime to ensure the safety of ASIS operations and personnel in the performance of all of ASIS's statutory functions under s 6(1).

While recognising that this is a matter on which the Foreign Affairs portfolio may also wish to comment, in light of the above the Department is of the view that conducting counter-intelligence, in relation to all of ASIS's functions is a legitimate objective, and is proportionate to the limitations on the right to privacy under Article 17 that would arise as a result of the proposed amendment. As noted in the Statement of Compatibility, permissible limitations on Article 17 are not solely restricted to those which are directed to the protection of national security. (As noted in the Statement, the objectives of the ICCPR include State sovereignty and the protection of the nation state, which includes, but is not limited to, national security.)

Additionally, there are significant and appropriate statutory limitations on the scope of agencies' functions under the Intelligence Services Act. Activities in the nature of policing or law enforcement functions are also specifically excluded by s 11, as are activities for the purpose of furthering the interests of an Australian political party or political organisation. Further, section 12 requires that the activity must be necessary for the proper performance of ASIS's functions or authorised or required by or under another Act.

As also mentioned above, s 9(1) requires the relevant Minister, in giving an authorisation for an activity or activities, to be satisfied that the relevant activity or activities are necessary for the proper performance of the agency's functions, there are satisfactory arrangements in place

[20] Australian Human Rights Commission, *Submission 28,* p. 18 (recommendation 8(b)).

to ensure that nothing will be done that exceeds this, and that there are satisfactory arrangements in place to ensure that the nature and consequences of acts done are reasonable, having regard to the purposes for which they are carried out. Additionally, in accordance with s 9(1A)(b), where the Australian person is also, or is also likely to be, involved in a threat to security (within the meaning of that term in s 4 of the ASIO Act), the responsible Minister will still be required to obtain the agreement of the Attorney-General before issuing an authorisation.

The application for, and execution of, a Ministerial authorisation is also the subject of oversight by the IGIS, who may examine both the legality and propriety of an agency's actions. Further, any intelligence produced may only be retained and communicated in accordance with the Ministerial privacy rules made under s 15.

The Department will, however, assist the Government in considering whether the EM to the Bill should be updated to provide further clarification regarding the matters addressed above.

## Schedule 6 – protection of intelligence-related information

### Proposed public interest defence

The AHRC recommended that the proposed offences in Schedule 6 should be subject to a public interest exception, which would operate as an offence-specific defence where the public interest in a disclosure, dealing or recording is demonstrated to outweigh the harm that results from that action. It was said that such an exception is necessary due to the combination of the following factors, which the AHRC identified as the basis for its view that the "increases in penalties and the creation of new offences … have not been demonstrated to be necessary and proportionate to the Government's objective of protecting national security":

- The elements of the offences do not require a person to intend to cause harm to Australia's interests, or that their conduct in fact caused such harm.
- The offences are not limited to national security information, noting that several intelligence agencies have functions that go beyond the protection of national security, and all will necessarily generate some information the release of which could not jeopardise national security.
- The unauthorised dealing and recording offences do not require any information or records to be communicated outside the relevant agency.
- The Bill increases penalties or creates new offences.[21]

As noted in the Department and ASIO's first joint supplementary submission to the Committee, a specific public interest defence is not supported. A public interest defence would inappropriately make a jury or a trial judge the final arbiter of whether or not a disclosure caused harm to the public interest. There is a risk that such individuals may not

21 Australian Human Rights Commission, *Submission 28*, pp. 20-21 (recommendation 10(a)).

have an appropriate understanding or appreciation of the possible impact of releasing that information or placing it at risk, and may not have an opportunity to adequately assess how the disclosure of a particular piece of information may, when taken together with other information, cause prejudice to national security or other important national interests.

Instead, appropriate provision is made under the *Public Interest Disclosure Act 2013* (PID Act) for the reporting of suspected wrongdoing, in addition to the ability of individuals to make pro-active disclosures to the IGIS. In addition to providing an independent means to report concerns about an intelligence agency, the PID Act also allows a person to take such concerns to the Federal Court where the person claims there have been reprisals, or threats of reprisals, taken against them because he or she made a public interest disclosure.

As indicated in the first joint supplementary submission, the Department and ASIO will assist the Government in giving consideration to whether the Bill could include an express statement that the offences do not apply to persons making pro-active disclosures to the IGIS to ensure that the offences do not operate as a perceived deterrent to engaging with the IGIS (as proposed by the IGIS in her submission).

**Proposed expansion of the 'prior disclosure' defence**

For the reasons listed above, the AHRC further submitted that the existing exceptions for information or records previously made public under the authority of the Commonwealth should be expanded to include the public release of information or records without the authority of the Commonwealth.[22]

The Department strongly disagree with the proposal to extend the exemptions to the offences in Schedule 6 in the manner proposed by the AHRC. As noted in the EM to the Bill, the existing exceptions are deliberately designed to exclude the subsequent communication by entrusted persons of 'leaked' information. The risk to national security occasioned by a subsequent communication of intelligence-related information by an entrusted person is just as grave as the original unauthorised communication by an entrusted person. (The same can be said of the actions of an entrusted person that place sensitive information or records at risk of compromise, such as unauthorised dealings with records or recording of information.)

In addition, it is appropriate that persons to whom intelligence-related information is entrusted are held to a high standard in relation to their dealings with it. The fact of prior unauthorised disclosure by one entrusted person is not material to the application of this general expectation to all entrusted persons. An expanded exception along the lines of that proposed by the AHRC would produce the undesirable result that, if one entrusted person chose to 'leak' a piece of information by communicating it without authorisation (or chose to deal with a record, or make a record of information, without authority) all entrusted persons would, in effect, be free to similarly flout the limits of their authorisation without any prospect of being exposed to criminal penalty. Such an exemption would therefore achieve the opposite result to the deterrent effect contemplated by the proposed offences in Schedule 6.

22 Australian Human Rights Commission, *Submission 28*, p. 21 (recommendation 10(b)).

In practice, entrusted persons receive specific training to make clear their significant responsibilities in the communication, storage and handling of extremely sensitive information. A number of Commonwealth guidelines set out strict rules and procedures for dealing with sensitive business or national security information in both physical and electronic form. These are available publicly at www.protectivesecurity.gov.au.

For example, the *Physical Security Management Protocol* provides that information bearing a security classification carries with it a risk to business impact or national security that has been assessed by the originator or creator of the document when applying the classification. A document bearing the classification 'CONFIDENTIAL' therefore has been assessed, at the time of its creation, to have the capacity to cause a very high level of damage if released inappropriately. It is necessary and proportionate that persons working for or with intelligence agencies and dealing with national security classified information be subject to a higher penalty for release of information that could, in the case of information classified TOP SECRET, cause catastrophic damage to Australia, its political independence or territorial integrity.

It is important to bear in mind that the proposed offences in Schedule 6 apply only to entrusted persons – that is, those who are in a relationship of employment with the relevant intelligence agency, or who have a relationship with the agency under a contract, agreement or arrangement with the agency. These offences do not have any application to a non-entrusted person who might receive information from an entrusted person in contravention of the entrusted person's authority to deal with that information.

**Proposed exception – information or records unrelated to national security**

The AHRC further submitted that the offences should be amended to "exclude disclosures, dealings and recordings of information that do not relate to national security".[23]

The Department does not support the limitation of the proposed offences to 'national security'. The disclosure by an entrusted person of information that relates to the performance by an agency of its security intelligence related functions is inherently harmful and meritorious of criminal sanction. However, the disclosure by an entrusted person of information that relates to the performance by an agency of other intelligence-related functions can be equally harmful to Australia's national interests, including its international relations and relationships with foreign intelligence agencies, as well as the lives and safety of the persons responsible for collecting or providing advice about such intelligence.

These factors led the Australian Law Reform Commission (ALRC), in its 2009 *Report on Secrecy Laws and Open Government in Australia*, to conclude that:

> [A] prohibition on the disclosure of information obtained or generated by intelligence agencies is justified by the sensitive nature of the information and the special duties and responsibilities of officers and others who work in and with such agencies. The existing [Australian Intelligence Community] secrecy offences cover a limited range of people who handle intelligence information, namely officers and employees, and people with whom the agency has an agreement or an arrangement. The ALRC

23 Australian Human Rights Commission, *Submission 28*, p. 21 (recommendation 10(c)).

> considers that it is appropriate for people in this position to be subject to higher responsibilities to protect inherently sensitive information.[24]

The ALRC rejected suggestions that specific secrecy offences, such as those under intelligence legislation, should be limited to "national security information". Rather, the ALRC preferred offences that apply to "particular government agencies that obtain and generate sensitive information".[25] The ALRC included all agencies within the Australian Intelligence Community in this category. The Department concurs with the findings of the ALRC in this respect.

Safeguards applying to the offences have been set out extensively in supporting material already provided to the PJCIS, however in answer to the AHRC concerns, it is worth repeating that significant safeguards are already contained in the Bill and in the Prosecution Policy of the Commonwealth. The Bill provides that offences cannot be prosecuted without the consent of the Attorney-General, and includes a number of elements which the prosecution must prove. For example, these elements require evidence of a person's intention, or recklessness with information, knowing that the information was related to an intelligence agency, as well as a lack of authority to undertake a specific action with the information. In addition, before a prosecution is commenced the Prosecution Policy of the Commonwealth requires the CDPP to be satisfied that there is sufficient evidence to prosecute the offence and that it is evident in light of the provable facts and the whole of the surrounding circumstances that the public interest requires a prosecution to be pursued.

In recognition of the concerns raised by the AHRC, however, the Department will support the Government in considering whether it would be appropriate to amend the EM to the Bill to include a justification for the application of the proposed new or amended offences in Schedule 6 to the non-national security intelligence functions of those agencies governed by the Intelligence Services Act.

**Proposed gradation of offences**

Finally, the AHRC submitted that the offences in Schedule 6 should be re-structured to "provide for a series of gradated offences" in which the proposed maximum penalties would be available only where:

- the information or record disclosed or dealt with or recorded relates to national security; and
- the disclosure, dealing or recording is done with the intention of causing serious harm to national security, and does cause such harm.

The Department consider the gradated continuum of offences created by the Bill to be sufficient. (That is, the amendments in the Bill reflect an appropriate gradation with the penalties applicable to persons who engage in activities that place at risk intelligence related information, and who communicate that information without authorisation, as well as persons

24 Australian Law Reform Commission, Report 112 (December 2009), p. 289.

25 Australian Law Reform Commission, Report 112 (December 2009), p. 288.

who communicate that information with the intention of causing grave harm to Australia's national interests contrary to the espionage offences in Division 91 of the Criminal Code.) As such, the adoption of the gradated continuum of offences in the manner proposed by the AHRC is not supported. To the extent that a person intended to cause harm by a disclosure – or if their disclosure, in fact, caused harm – these circumstances are appropriately taken into account in determining sentence within the specified maximum penalties. Such factors would be aggravating circumstances upon the sentencing of persons who are convicted of the proposed new or amended offences in Schedule 6 to the Bill, if enacted. The Department is of the view that these circumstances are appropriately taken into account as sentencing factors, rather than as elements of the offences (and thus determinants of a person's guilt). This is consistent with the position set out in the first joint supplementary submission that the wrongdoing to which the proposed offences in Schedule 6 to the Bill are directed to the wrongdoing inherent in the conduct of an entrusted person who acts in excess of his or her authority to communicate or deal with information or records. As the numerous independent reviews of intelligence-specific secrecy laws cited in the first joint supplementary submission concluded, the harm occasioned by such conduct is implicit in the nature of the information to which it relates.[26]

Accordingly, if such factors are to be taken into account in determining criminal guilt, the Department submits that existing, serious criminal offences in the Criminal Code – such as those of espionage or treason – are the appropriate offences to be charged and prosecuted where there is adequate, admissible evidence suggesting that a person acted with the requisite, malicious intention.

26 AGD and ASIO, *Joint Supplementary Submission (unclassified)*, 29 August 2014, pp 78-80. These reviews include: the Hope Royal Commission on Intelligence and Security (Fourth Report) (1976), the Gibbs Review of Commonwealth Criminal Law (1991), and the ALRC Review of Secrecy Laws and Open Government in Australia (2009).