Australian Government

Attorney-General's Department

Deputy Secretary
National Security and Criminal Justice

14/9823

18 August 2014

Mr James Nelson
a/g Inquiry Secretary
Parliamentary Joint Committee on Intelligence and Security

Dear James

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

I refer to the appearance of witnesses from the Attorney-General's Department at the Committee's public hearing on the above Bill on 15 August 2014. I now provide the Department's responses to several matters taken on notice at the hearing.

These matters relate primarily to the Committee's questions on measures in Schedule 1 (ASIO employment), Schedule 2 (ASIO powers) and Schedule 3 (special intelligence operations) to the Bill. The enclosed responses further address a general invitation from the Committee to respond to various issues raised by the Inspector-General of Intelligence and Security in her oral evidence and written submission to the inquiry.

The Department also anticipates lodging a supplementary submission with the Committee late this week. This will address key matters raised by other submitters and witnesses appearing before the Committee at its public hearing on 18 August 2014.

Please contact Annette Willing, National Security Legal Adviser, should you wish to discuss the enclosed responses, or if the Department can be of any further assistance to the Committee in completing its inquiry.

Yours sincerely

Mike Rothery PSM
a/g Deputy Secretary
National Security and Criminal Justice Group

UNCLASSIFIED

Attorney-General's Department
Responses to matters taken on notice
Public hearing, 15 August 2014

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

Contents

Summary **2**
Outline of matters taken on notice 2
Supplementary Departmental submission (forthcoming) 3
Schedule 1 – 'ASIO affiliates' **3**
Meaning of, and policy justification for, the new term 'ASIO affiliate' (s 4) 3
Application of the term 'ASIO affiliate' to authorisations to exercise powers or undertake activities on behalf of ASIO 4
Application of the term 'ASIO affiliate' to ASIS cooperation measures 6
Alternative proposal 6
Schedule 2 – ASIO's computer access powers **7**
Permitted interference, etc with the lawful use of a computer – meaning of 'material' 7
Retention of data or other information obtained under a computer access warrant 9
Schedule 2 – use of reasonable force in the execution of ASIO warrants **10**
Justification for the limited power to use reasonable force against persons 10
Interpretation of existing use of reasonable force provisions in respect of persons 11
Safeguards, oversight and accountability – use of reasonable force against persons 12
Schedule 2 – evidentiary certificates in relation to ASIO warrants **13**
Schedule 3 – special intelligence operations – secrecy offences **14**
Justification 14
Elements of the offences 17
Further safeguards 22
Schedule 3 – special intelligence operations – differences to controlled operations **24**
Authorisation 25
Oversight 25
Judicial scrutiny 25
Other differences 26
Responses to other matters raised by the IGIS **26**

Summary

Representatives of the Attorney-General's Department took several matters on notice at the Committee's public hearing on 15 August 2014, in relation to the issues set out below.

To assist the Committee with timely information, the Department has prepared its responses in advance of receiving proof Hansard. As such, questions are paraphrased from notes made of the proceedings.

Outline of matters taken on notice

The new term 'ASIO affiliate' (Schedule 1)

- The application of this proposed new term in s 4 of the *Australian Security Intelligence Organisation Act 1979* (ASIO Act) to authorisations in relation to ASIO's special powers, and cooperative arrangements with the Australian Secret Intelligence Service (ASIS).

ASIO's special powers (Schedule 2)

- The justification for authorising the use of reasonable force against a person if necessary for the purpose of executing an ASIO warrant.
- The meaning of the term 'material' as used in proposed provisions conferring on ASIO a limited power to add, delete or alter data in a computer, in accordance with a warrant authorising computer access.
- Safeguards against the retention of data or information obtained under a warrant authorising computer access, where that data or information does not relate to persons relevant to security (particularly information or data relating to third parties, such as users of a target computer network or a computer on specified premises; or owners or users of a third party computer that is used to gain access to a target computer).
- Mechanisms for the oversight and scrutiny of evidentiary certificates issued in relation to activities authorised under certain types of ASIO warrants, which relate to details of technical capability (such as computer access or surveillance technologies or techniques).

Special intelligence operations (Schedule 3)

- The elements of, and justification for, the proposed offences applying to the communication of information relating to a special intelligence operation (particularly in their potential application to journalists reporting on national security matters).
- Differences between the proposed special intelligence operations scheme and that authorising controlled operations for law enforcement purposes under Part IAB of the *Crimes Act 1914*, particularly in relation to authorisation, oversight and judicial scrutiny.

Other matters

- A general invitation from Committee members to respond to any further issues raised by the IGIS and Deputy IGIS in their oral evidence on 15 August, or in the IGIS's written submission, noting that the submission was only released just prior to our hearing.

Supplementary Departmental submission (forthcoming)

As a further aid to the Committee's deliberations, the Department proposes to lodge a supplementary submission in the coming days, addressing further matters raised in other submissions, the evidence of witnesses appearing at the public hearing on 18 August, and the matters raised with the Department and ASIO at a private hearing on 18 August.

Schedule 1 – 'ASIO affiliates'

Meaning of, and policy justification for, the new term 'ASIO affiliate' (s 4)

Committee questions

Further to the submission and evidence of the IGIS about the scope of the new term 'ASIO affiliate' in amending item 1 of Schedule 1 to the Bill (which inserts a definition in s 4 of the ASIO Act), members of the Committee sought further information from Departmental and ASIO witnesses about the reasons for the proposed inclusion of this term, noting that it is an additional measure to the recommendations from its 2013 *Report on Potential Reforms to Australia's National Security Legislation* (2013 report).

Departmental response

The term 'ASIO affiliate' has been proposed to help streamline and harmonise across the Commonwealth statute book the terminology applied to persons who:

- are in a form of relationship with ASIO other than employment (such as under a contract, agreement or another form of arrangement) that involves the performance of functions or services for the Organisation (including, for example, contractors, consultants and secondees to the Organisation); and

- by reason of their relationship with the Organisation, are authorised, or able to be authorised, to undertake certain activities, or made subject to obligations, duties, liabilities and prohibitions as set out in the ASIO Act or in other Commonwealth legislation.

To this end, the term 'ASIO affiliate' is a new label or an 'umbrella term' to capture a range of different terminology presently used in the ASIO Act and other Commonwealth statutes (such as an "agent", "another person" to an employee, or an "officer" in some instances where that term is used). As such, the new term 'ASIO affiliate' ensures that there is clarity and certainty, on the face of individual provisions, about the classes of persons to whom

those substantive provisions apply, and thereby ensures that such persons are regulated in a consistent manner. The current 'patchwork' of terminology largely reflects the different points in time at which the ASIO Act has been amended, and the fact that the development of individual pieces of amending legislation did not involve a general review of terminology for internal consistency in the ASIO Act, or whole-of-statute book consistency.

The specific word 'affiliate' in the new term has been selected to help avoid the risk of misunderstanding or misrepresentation that ASIO affiliates are invested with a greater degree of 'status' or 'authority' in connection with the Organisation than they, in fact, possess. (Hence, a label along the lines of an 'ASIO official' was not preferred.) The term 'ASIO affiliate' is further intended to communicate that such persons have a different and separate status to an 'ASIO employee'. (The latter is a further new term proposed to be inserted in s 4 by amending item 1 of Schedule 1 to the Bill. It represents a similar harmonisation measure, in respect of persons who are in a relationship of employment with ASIO, and who are currently described, both in the ASIO Act and various other Commonwealth laws, by numerous different, undefined terms.)

An example of the different status of an ASIO affiliate, compared to an ASIO employee, is that there are some activities that only ASIO employees are authorised or able to be authorised to perform, such as applying for an authority to conduct a special intelligence operation under proposed s 35B in Schedule 3 to the Bill. In addition, the Bill contains proposed amendments to enable the Director-General of Security to make determinations excluding certain ASIO affiliates or classes of ASIO affiliates from being authorised, or able to be authorised, to undertake certain activities (namely, warrantless surveillance under proposed s 26F in Schedule 2).

Accordingly, the proposed new labels of 'ASIO affiliate' and 'ASIO employee' are not designed to expand, in any substantial way, the classes of persons who are presently authorised to exercise powers, or who are subject to obligations, duties, liabilities or prohibitions by reason of their relationship with the Organisation.

Application of the term 'ASIO affiliate' to authorisations to exercise powers or undertake activities on behalf of ASIO

Committee questions

Committee members sought further information from Departmental and ASIO witnesses about the specific way, or ways, in which the new term 'ASIO affiliate' would apply to persons who are authorised to exercise powers or undertake activities on behalf of the Organisation, including special powers under Division 2 of Part III of the ASIO Act in relation to the collection of intelligence relevant to security (such as under a warrant or a warrantless power).

In particular, some members questioned whether the proposed new term 'ASIO affiliate' may result in an overly broad category of persons being authorised, or being able to be authorised, to exercise powers or undertake activities on behalf of the Organisation.

Departmental response

As noted above, the proposed new term 'ASIO affiliate' does not expand, in any substantial way, the classes of persons who are presently authorised, or able to be authorised, to exercise powers or undertake activities on behalf of the Organisation. Rather, it harmonises presently inconsistent terminology both within the ASIO Act and across the Commonwealth statute book.

The Bill includes additional safeguards to ensure that, in relation to those provisions conferring powers or authorisations on all persons answering the description of an ASIO affiliate, further limitations can be imposed as considered appropriate in practice. In particular, some proposed amendments authorise the Director-General of Security to exclude or 'carve out' certain ASIO affiliates (by reference to either individuals or classes of persons) from general provisions authorising ASIO affiliates to undertake certain activities. (As noted above, the relevant 'carve out' provisions apply under proposed new s 26F of the ASIO Act in relation to ASIO affiliates who are authorised to exercise the new warrantless surveillance powers in proposed ss 26C, 26D and 26E.)

Another safeguard can be found in other powers relevant to ASIO affiliates, which require the Director-General of Security or another designated person to specifically authorise certain ASIO affiliates (whether individually or by class) to exercise a particular power.

This includes, for example, the power of the Director-General under proposed new s 24(3) of the ASIO Act to appoint persons to exercise the power under proposed new s 24(2) to approve persons who can exercise powers authorised under ASIO's special powers warrants (Division 2 of Part III), and questioning warrants and questioning and detention warrants in relation to the collection of intelligence that is important in relation to a terrorism offence (Division 3 of Part III) in accordance with proposed new s 24(1). Under proposed new s 24(3), the Director-General can appoint 'senior position holders' (either individually or by reference to classes of such persons) to exercise the relevant powers under s 24(2). A 'senior position holder' is proposed to be defined in s 4 (by amending item 3 of Schedule 1 to the Bill) as a person who is either an ASIO employee or an ASIO affiliate who holds a designated senior position in the Organisation.

In addition, not all authorisations or authorising provisions in relation to powers or activities are contingent on a person's status as an 'ASIO affiliate' or an 'ASIO employee'. For example, under proposed ss 24(1) and (2), "a person" or "a class of persons" can be authorised by the Director-General (or a senior position holder appointed by the Director-General) to exercise powers under an ASIO special powers warrant, or a questioning or questioning and detention warrant. This approach is appropriate having regard to the need for operational flexibility in the persons who are able to be authorised to assist the Organisation in undertaking activities under warrants. It is consistent with the coverage of the existing provision in s 24, which relevantly authorises "officers and employees of the Organisation, and other people".

Application of the term 'ASIO affiliate' to ASIS cooperation measures

Committee questions

Committee members sought further information from Departmental and ASIO witnesses about whether – and if so, why – ASIO affiliates would be able to be authorised to request ASIS to collect intelligence on an Australian person of security interest overseas, pursuant to the proposed measures for enhanced cooperation in Schedule 5 to the Bill. (These proposed measures would, if enacted, amend the *Intelligence Services Act 2001* (IS Act) in partial implementation of recommendation 39 of the Committee's 2013 report.)

Departmental response

The proposed amendments to the IS Act in Schedule 5 to the Bill would, if enacted, authorise either the Director-General of Security or a person authorised by the Director-General to notify ASIS that ASIO requires the production of intelligence on an Australian or a class of Australian persons outside Australia (proposed ss 13B(1)(d) and 13C).

The Director-General's power to authorise other persons to notify ASIS and ASIO is set out in proposed s 13C, and is limited to a 'senior position holder' or a class of such position holders. As noted above, the term 'senior position holder' is proposed to be inserted in s 4 of the ASIO Act by amending item 3 of Schedule 1 to the Bill. This term covers both ASIO employees and ASIO affiliates who hold a designated, senior position within the Organisation (being that of an SES or equivalent level employee, or a position designated as 'Coordinator').

Accordingly, to the extent that ASIO affiliates are authorised to make requests of ASIS under the proposed new cooperative arrangements, this ability is constrained to affiliates who hold senior positions within the Organisation, and who are appointed by the Director-General. These limitations are considered proportionate to the nature of the power.

Alternative proposal – persons authorised to exercise powers or undertake activities on behalf of the Organisation

Committee question

Senator Fawcett asked Departmental and ASIO witnesses to comment on a possible alternative proposal to the inclusion of any references to 'ASIO affiliates', for the purposes of identifying persons who are authorised (or potentially able to be authorised) to exercise powers or undertake activities on behalf of the Organisation.

This suggested approach would, as the Department understands it, establish a single type of of scheme for the authorisation of persons to exercise powers or undertake activities without any reference to a person's status as an ASIO employee or an ASIO affiliate. (For example, all relevant powers or activities in the ASIO Act could be expressed as being exercisable by "such persons who are duly authorised in accordance with this Act" with a separate provision

enabling the Director-General of Security or others to authorise persons, which does not include any reference to their status as an ASIO employee or an ASIO affiliate.)

Departmental response

As mentioned above, the Department notes that the status of a person as an 'ASIO affiliate' (or an 'ASIO employee') does not automatically authorise that person to exercise powers or undertake activities on behalf of the Organisation, or automatically make that person eligible to be authorised to do so. Rather, specific provision is made for a person's authorisation, or eligibility to be authorised, in relation to individual types of powers or activities. (For example, specific provision is made for authorisations to undertake activities in accordance with warrants; undertaking warrantless surveillance; or appointing others as persons who can authorise the exercise of powers under warrants.)

Authorisations to exercise some powers or undertake some activities will necessarily need to be more limited than others. In this regard, engaging the concept of an 'ASIO affiliate' can be a helpful device to limit the classes of persons authorised or eligible to be authorised, as compared to a general reference in the relevant authorising provision to 'any person'. Further limitations can then be applied to the class of 'ASIO affiliates' as necessary – for example, limiting some types of authorisations to ASIO affiliates who are also 'senior position holders' (as it the case for persons who are able to request ASIS to collect information on Australians of security interest overseas); or alternatively investing the Director-General with a power to 'exclude' as appropriate certain ASIO affiliates from authorising provisions applying to all ASIO affiliates (as is the case for the proposed warrantless surveillance powers). In addition, there are some authorisation requirements, such as those in relation to warrants under proposed new s 24(1) of the ASIO Act, in which there are no linkages to a person's status as an 'ASIO employee' or an 'ASIO affiliate'.

The Department submits that retaining this approach is preferable because it allows the approach taken to authorisation provisions to be tailored to the nature of individual powers and activities. The proposed use of the term 'ASIO affiliate' does not change the existing application of relevant authorisation provisions in this respect, but merely updates (by way of consolidating) the relevant terminology applied to these persons.

Schedule 2 – ASIO's computer access powers

Permitted interference, etc with the lawful use of a computer – meaning of 'material'

Committee members examined proposed amendments to ASIO's search warrants (s 25), computer access warrants (s 25A) and computer access under the new scheme of identified persons warrants (proposed ss 27D and 27E), which implement recommendation 21 of its 2013 report. (That recommendation was directed to the Government giving further consideration to amendments enabling the disruption of a target computer for the purposes of executing a computer access warrant, to the extent of demonstrated necessity.)

Background – relevant provisions

Proposed ss 25(6), 25A(5) qualify certain, existing limitations on the power to access data relevant to a security matter on a computer, other electronic equipment or data storage device under a warrant in s 25(5) (search warrants) and 25A(4) (computer access warrants).

Currently, ss 25(6) and 25A(5) impose a prohibition on the addition, deletion or alteration of data, or the doing of any thing that interferes with, interrupts or obstructs the lawful use of the relevant computer by other persons; or which causes any loss or damage to other persons lawfully using the computer.

In line with recommendation 21 of the Committee's 2013 report, the proposed amendments remove these absolute prohibitions and replace them with provisions to the following effect:

- A prohibition on actions that are likely to cause material interference with, interruption to, or obstruction of, lawful use of the relevant computer.
- An exception to the above prohibition on a likely material interference, interruption or obstruction where necessary to carry out one or more of the activities specified in the warrant in relation to data relevant to the security matter in respect of which the warrant is issued. (Such activities include accessing data, inspecting or copying it, or converting it to documentary form; or doing any thing reasonably necessary to conceal such activities, or any thing reasonably incidental to these activities.)
- A prohibition on actions which are likely to cause other material loss or material damage to a lawful user of the relevant computer. (There is no exception for activities that are necessary to carry out one or more of the activities specified in the warrant. As such, only those activities which are likely to cause other non-material loss or damage are able to be authorised under a warrant.)

As computer access is authorised under the proposed new scheme of identified persons warrants, the Bill further includes provisions corresponding to those outlined above in proposed ss 27D(2), 27D(7), 27E(2) and 27E(5).

Committee questions

Some members of the Committee sought clarification of the meaning of the term 'material' in the proposed amendments, for the purpose of assessing whether:

- a likely form of interference, interruption or obstruction of lawful computer use was of a material kind (and therefore only able to be authorised if necessary to carry out one or more of the activities specified in the warrant, such as accessing data relevant to security); and
- a likely form of other loss or damage to a lawful user of a computer would be of a material kind (and therefore not able to be authorised under a warrant).

Departmental response

In addition to the explanations provided by Departmental and ASIO witnesses at the public hearing (and further evidence given in private session) the Department confirms that the term 'material' is intended to take its ordinary meaning – being a likely interference with or interruption or obstruction of the lawful use of a computer that is of a 'substantial' or 'essential' consequence to a person's ability to use the relevant computer in the ordinary way in which that computer would be expected to be used.

The material (or otherwise) nature of any likely disruption, interference or obstruction of lawful use – or likely other loss or damage to lawful users of a computer – is intended to be a matter for determination in individual cases, so that the degree of likely impact can be assessed in the particular circumstances. Relevant considerations may include the duration and extent to which the relevant activity would compromise a person's ability to use a computer. As further noted in the Explanatory Memorandum to the Bill (at p. 67) the proposed amendments are designed to enable ASIO to undertake action under a warrant that is "likely to cause immaterial interference, interruption or obstruction … for example using a minor amount of storage space".

Assessments by the Organisation as to the 'material' (or otherwise) impact of such actions on lawful computer use, or on lawful users of computers, are subject to oversight of the IGIS, who may make an assessment of both the legality and propriety of the Organisation's activities and practices in this regard. The IGIS can also relevantly recommend the payment of compensation to persons who are adversely affected by the actions of an intelligence agency, if considered appropriate.

Retention of data or other information obtained under a computer access warrant

Committee questions

Committee members asked Departmental and ASIO witnesses to respond to the evidence and submissions of the IGIS that there is no obligation on ASIO to actively consider whether information obtained under a warrant is actually related to the individual who was the subject of a warrant, and to promptly delete information generated by or about individuals who are not relevant to security.

It is noted that the IGIS raised this issue in the context of the proposed amendments to the definition of the term 'computer' under s 22 of the ASIO Act (including to cover a computer network), and the proposed amendments to computer access warrants under s 25A to allow use of third party computers for the purpose of accessing data relevant to security held in a target computer. The IGIS suggested that these proposed amendments create "the potential for a significant amount of information to be retained by ASIO about persons not relevant to security, but who were the subject of, or created information on, a computer connected to a target network or system that was on targeted premises." (IGIS submission at p. 9.)

Departmental response

The Department notes the existing obligation in s 31 of the ASIO Act requires the destruction of records (or copies) obtained under a warrant, if the Director-General is satisfied that the record (or copy) is not required for the performance of functions or exercise of powers under the ASIO Act.

The IGIS has correctly observed that this falls short of a positive obligation on the Director-General to consider whether such records are in the possession, custody or control of the Organisation. The Department notes that the propriety of the Organisation's activities or practices in relation to the practical application of this provision would fall within the IGIS's statutory remit. The Department further submits that any consideration of the possible imposition of a positive legislative obligation on the Director-General to undertake continuous review would desirably be informed by a consideration of its anticipated operational impacts.

Schedule 2 – use of reasonable force in the execution of ASIO warrants

Justification for the limited power to use reasonable force against persons

Committee questions

Committee members sought further explanation from Departmental and ASIO witnesses about the need for the proposed provisions authorising the use of reasonable force against a person, if necessary to do the things specified in a search warrant, computer access warrant, foreign intelligence warrant or identified person warrant, or to recover a surveillance device installed or used under a surveillance device warrant. (These are proposed ss 25(7)(a), 25A(5A)(a), 27A(2)(a), 27J(3)(d) and 26B(5)(j).)

It was noted that these provisions departed from recommendation 36 of the Committee's 2013 report, which recommended that, while the use of reasonable force should be exercisable at any time during the execution of a warrant, such force should be limited to property.

In particular, members of the Committee asked:

- why it is considered necessary to authorise the use of reasonable force against persons for the purpose of executing an ASIO warrant;
- whether law enforcement agencies need specific authorisation under an ASIO warrant to assist in executing an ASIO warrant, if the use of reasonable force against a person is necessary to undertake an activity authorised under a warrant; and
- if the second question is answered in the affirmative, why the proposed amendments to the ASIO Act cannot be limited to law enforcement officers assisting ASIO in executing a warrant.

Departmental response

The Department notes the evidence of the Director-General of Security at the public hearing on 15 August 2014 that there are realistic and credible (although rare) circumstances in which it may be necessary to use reasonable force against a person in order to execute a warrant, and in which the attendance of law enforcement officials may not be possible. This may be due to the sensitivity of a particular operation, or unforeseen circumstances which may arise during the execution of a warrant (such as the unexpected entry of another person to premises during the execution of a warrant, and attempts by that person to prevent activities authorised under the warrant from being undertaken). (A classified briefing would be necessary if the Committee requires further operational information.)

It is, in the Department's view, desirable that the legislative framework governing the execution of warrants should accommodate this operational contingency. In particular, a limitation on the use of reasonable force to property would likely mean that warrants are unable to be executed in the circumstances described above, which may mean that the Organisation is unable to collect the relevant intelligence authorised to be obtained under the warrant. (This is so because any use of force against the person would have to be necessary for the purpose of executing the warrant, in the sense of being essential or integral rather than simply convenient or efficient.)

The Department further notes that, to the extent there is ambiguity as to the source of legal authority for law enforcement officials to exercise reasonable force in the execution of an ASIO warrant, an express authorisation in the ASIO Act would remove this risk in cases where law enforcement officials are present to assist in the execution of an ASIO warrant and general police powers are either not available, or there is some doubt as to their availability, in the particular circumstances.

The Department also notes that the proposed provisions are caveated by several safeguards, as identified in the Explanatory Memorandum to the Bill (especially pp. 12 and 68). In particular, the use of force must be reasonable and necessary to execute the warrant (in the sense of being both essential and proportionate). Any force which exceeds these limitations is not authorised and would be subject to the general criminal law. In addition, the provisions do not authorise the use of force which would cause death or grievous bodily harm.

Interpretation of existing use of reasonable force provisions in respect of persons

Committee questions

Committee members noted the evidence of the IGIS that, in her view, the proposed amendments are not merely declaratory of an existing power to use reasonable force against persons, but rather confer a new power in relation to such force. Departmental and ASIO witnesses were invited to respond to this suggestion.

Departmental response

The Department acknowledges that competing interpretations are reasonably open in relation to the existing provisions authorising the use of force in the execution of a warrant. In the Department's view, this lends further weight to the need for the proposed amendments, in order to provide certainty and transparency by placing beyond doubt the availability of the relevant power.

The Department will, however, assist the Government in giving consideration to whether the Explanatory Memorandum to the Bill should be amended to include an acknowledgement that there is ambiguity as to whether the relevant provisions are, in their present form, capable of authorising the use of reasonable force against a person, and that an amendment is needed to remove legal risk in this regard.

Safeguards, oversight and accountability in relation to the use of reasonable force against persons

Committee questions

Committee members noted the evidence of the IGIS in relation to the importance of providing adequate training in the use of force against persons; suggested additional reporting requirements in relation to the use of force; and observations on the specific procedural requirements applying to the use of force by law enforcement agencies, which include the conduct of routine reviews when force is used against a person. (See, for example, p. 13 of the IGIS's submission to the inquiry.)

Some members of the Committee sought Departmental and ASIO witnesses' views on whether the costs associated with the necessary investment in training, accountability and oversight in relation to the use of force by persons other than law enforcement officials would outweigh the perceived benefit or utility of such a power – particularly if it was intended only to be used sparingly.

Departmental response

The Department notes the evidence of the Director-General that there are credible circumstances in which it may be necessary to use reasonable force against a person in order to execute a warrant, where law enforcement officials are not present.

As noted above, in such circumstances, it may be impossible for the relevant warrant to be executed unless the persons doing so are authorised to use reasonable force against a person. In this event, the Organisation may be unable to collect the relevant intelligence.

Schedule 2 – evidentiary certificates in relation to ASIO warrants

Committee questions

The Committee asked Departmental and ASIO witnesses to provide further information about arrangements for the oversight of decisions of the Director-General or a Deputy Director-General of Security to issue evidentiary certificates under proposed s 34AA of the ASIO Act.

(These certificates may be issued in respect of certain activities undertaken in accordance with a 'relevant warrant' – being a surveillance device warrant; or a search, foreign intelligence or identified persons warrant authorising surveillance or computer access – or a 'relevant authorising provision', such as warrantless surveillance. Proposed s 34AA implements recommendation 37 of the Committee's 2013 report, which supported the introduction of an evidentiary certificate scheme in the ASIO Act to protect the identity of officers and sources.)

Departmental witnesses were also asked to provide further information about applicable safeguards to ensure that any information in respect of which a certificate is issued has been collected in a duly authorised manner, so that a court or tribunal may have confidence in relying on it.

Departmental response

Consistent with Commonwealth evidence law policy, evidentiary certificates under proposed s 34AA are of a 'prima facie' nature only, as distinct from a 'conclusive' nature. That is to say, such certificates do not bind a court or tribunal to accept them as evidence of the relevant matters to which they relate. Rather, these certificates are of persuasive value and allow an opportunity for evidence of contrary matters to be adduced.

As such, the key form of scrutiny in relation to the issuing of a certificate is the relevant court or the tribunal hearing the legal proceedings in which the certificate is adduced. If the relevant court or tribunal is satisfied that it is appropriate to place greater weight on contrary evidence (for example, if the certificate is challenged by another party to the proceedings), it will not be bound to accept the certificate as evidence of the matters to which it relates.

By way of further clarification, and as set out in the Explanatory Memorandum to the Bill (at p. 94) the Department notes that the matters to which a certificate issued under s 34AA are able to be issued are limited to technical details of the way in which intelligence was obtained under a warrant. (For example, details of particular surveillance or computer access technologies or methods, or the identity of ASIO officers or sources involved in activities under the warrant.) Evidentiary certificates cannot be issued in relation to the actual intelligence obtained under the warrant, in the event that it may be sought to be adduced in evidence in a proceeding.

In addition, questions in relation to whether or not particular activities authorised under a warrant were, in fact, capable of authorisation; whether or not any conditions or limitations

on authority under a warrant were complied with in practice; and whether or not the issuing process for a warrant was compliant with the applicable legislative requirements, are separate matters that are not addressed by proposed s 34AA.

Schedule 3 – special intelligence operations – secrecy offences

Justification for the offences in proposed s 35P

Committee questions

Committee members asked Departmental and ASIO witnesses to provide further information about the need for the proposed new offences in relation to the communication of information relating to a special intelligence operation. In particular, further information was sought about why existing non-disclosure offences were considered insufficient or inadequate to cover such actions.

Departmental response

Further to the evidence of Departmental witnesses at the public hearing on 15 August, the Department provides the following additional observations about limitations in other, existing criminal offences that could potentially apply to some instances of conduct that would constitute an offence against proposed s 35P.

These limitations arise principally because existing offences are directed to different forms of mischief to that which is targeted by proposed s 35P, with the result that their physical elements may not apply, or they would not adequately target and denounce the wrongdoing associated with compromising a covert intelligence operation that is of sufficient importance to have been designated as a special intelligence operation, in accordance with the authorisation process set out in Schedule 3 to the Bill.

<u>Offences under the ASIO Act</u>

In particular, the existing offence in s 18(2) of the ASIO Act concerning the unauthorised disclosure of intelligence-related information (including with the amendments proposed in Schedule 6 to the Bill) applies to persons who are in a specified form of relationship with ASIO (by way of employment, contract, agreement or some other form of arrangement).

While this may cover participants in special intelligence operations, and others within ASIO or other agencies who are legitimately privy to details of such operations, it may not cover persons to whom such information is disclosed on an unauthorised basis, and who engage in subsequent disclosures. This is a considerable limitation, given that the disclosure of the existence of a covert intelligence operation is, by its very nature, prejudicial to the effectiveness or viability of that operation. Such disclosure additionally carries a substantial risk of endangering the lives or safety of participants, who are likely to have close contact with persons of security concern as part of the operation.

The wrongdoing targeted by s 35P is the harm that is occasioned by the very fact of disclosure of information about a special intelligence operation. Therefore, the nature of a person's prior relationship (if any) with ASIO is not necessarily material to a person's culpability (although it may be a relevant consideration in sentencing a person convicted of an offence against s 35P). Relying on the existing offence in the ASIO Act would not, therefore, adequately target or contribute to deterring the wrongdoing to which proposed s 35P is directed.

A further offence under s 92 of the ASIO Act, concerning the publication of the identity of an ASIO officer (which is proposed to be amended by Schedule 1 to the Bill to adopt the terminology of an ASIO employee or an ASIO affiliate rather than an 'officer') could potentially apply to persons who communicate information relating to a special intelligence operation.

However, this offence will only be open if the relevant information communicated about the special intelligence operation would disclose the identity of an ASIO officer or an ASIO affiliate. This may not cover all participants in a special intelligence operation, and would not offer any protection against the disclosure of other information about the operation. In addition, the offence carries a maximum penalty of imprisonment for one year, which is disproportionate to the harm associated with conduct that – in addition to disclosing an ASIO officer or affiliate's identity – will prejudice a special intelligence operation by disclosing its existence, and may place at risk the lives or safety of participants, or persons connected to such participants.

Offences in the Criminal Code

Other criminal offences in the nature of espionage in Division 91 of the *Criminal Code 1995* (Cth) (Code) require proof of a person's intention to cause a specified form of serious harm, such as prejudice to the security or defence of the Commonwealth (or that this was the likely result of the person's conduct); or to give an advantage to another country's security or defence (or that this was the likely result of the person's conduct). The maximum penalties of 25 years' imprisonment applying to these offences reflect that that they are directed to conduct which causes, or is intended to cause, harm of the gravest possible nature to Australia's security interests. While a person who disclosed information about a special intelligence operation with the requisite intention to cause harm of one of these kinds could potentially be prosecuted under Division 91 of the Criminal Code, these offences are targeted to harm at the very uppermost end of the spectrum. They are not of application to the comparatively lesser, but still highly significant, degree of harm that may be occasioned by unauthorised disclosures of information relating to special intelligence operations in the absence of any malicious intention on the part of the discloser, or with an intention to prejudice a particular operation or the health or safety of an individual.

The Department is aware that some submitters to the inquiry have identified other offences in the Criminal Code as being potentially relevant to the communication of information about a special intelligence operation, including treason (s 80.1) and materially assisting enemies

(s 80.1AA). The prospects that these offences may have application in relation to the disclosure of information about special intelligence operations are, in the Department's view, remote other than in very exceptional cases. These offences require the causation of death or harm to the Sovereign, the Prime Minister or Governor-General, or the levying of war or an armed invasion (or preparatory conduct) against the Commonwealth, or the intentional engagement in conduct to assist an enemy engage in war against the Commonwealth. The penalties of life imprisonment applying to these offences reflect their exceptional nature.

Offences in the Crimes Act

The Department is further aware that some submissions to the inquiry have suggested that adequate coverage is provided by some offences in s 79 of the Crimes Act, which are directed to the disclosure of official secrets. They relevantly cover:

- the unauthorised communication or retention of certain information or records by a person to whom it is entrusted, with the intention of prejudicing the security or defence of the Commonwealth, under penalty of seven years' imprisonment: s 79(2);
- the unauthorised communication of certain information or records in the absence of any intention to cause harm, under penalty of two years' imprisonment: s 79(3);
- the unauthorised retention or failure to take reasonable care of certain information or records, in the absence of any intention to cause harm, under a penalty of six months' imprisonment: s 79(4);
- the receipt of certain information, where the recipient has reasonable grounds to believe the communication was made in contravention of s 91.1 of the Criminal Code (espionage) under penalty of seven years' imprisonment: s 79(5); and
- the receipt of certain information where the recipient has reasonable grounds to believe the communication was made in contravention of s 79(3) of the Crimes Act (see above), under penalty of two years' imprisonment.

The Department notes that these offences would not adequately target the wrongdoing inherent in conduct that would constitute an offence against proposed s 35P, particularly the basic offence in proposed s 35P(1). The only offence that would capture conduct targeted by proposed s 35P(1) is that in s 79(3) of the Crimes Act, which carries a maximum penalty of two years' imprisonment. This is disproportionately low to the disclosure of information that, by its very nature, will prejudice a covert intelligence operation and carries a risk of jeopardising the lives and safety of participants.

As noted above, such harm is inherent in a disclosure of information about a special intelligence operation, irrespective of a person's subjective intention (or otherwise) in making the disclosure. A maximum penalty of two years' would not provide a sentencing court with an adequate range within which to impose a sentence that reflects the gravity of the consequences of the conduct constituting the offence. As such, a two-year sentence applying to an offence of general application would be unlikely to serve as a significant deterrent to

persons who may be contemplating communicating information relating to a special intelligence operation.

The Department's supplementary submission will address similar contentions made in relation to the proposed offences in Schedule 6. (Namely, suggestions that s 79 of the Crimes Act, and various other offences, adequately cover the wrongdoing to which the proposed amendments are directed.)

Corresponding offences for controlled operations in Part IAB of the Crimes Act

The offences in proposed s 35P are identical in their elements to those in ss 15HK and 15HL of the Crimes Act, in relation to the unauthorised disclosure of information relating to a controlled operation. The Department re-iterates its oral evidence on 15 August that no issues have been identified in relation to the application of these offences to date – which have been in force since 2010 – to journalists or others reporting on, or seeking to discuss publicly, matters of law enforcement or national security.

In addition, advice from law enforcement agencies is that media professionals have engaged effectively with them in seeking guidance or clarification about reporting on such matters, in order to avoid the risk of unintentionally compromising sensitive operations. Media professionals can similarly contact the Organisation on a publicly listed telephone number on the Organisation's website. The media telephone line is staffed 24 hours.

Elements of the offences

Committee question

In the context of questioning about the potential application of the proposed offences to journalists, members of the Committee asked Departmental and ASIO witnesses to provide further information about the elements of the proposed offences.

Clarification was sought, in particular, about the application of the fault element of recklessness to the physical element of the offences that the information disclosed related to a special intelligence operation. (Proposed ss 35P(1)(b) and 35P(2)(b).)

Departmental response

As set out in the Explanatory Memorandum to the Bill (at pp. 111-112), proposed s 35P contains two offences in subsections (1) and (2) respectively. The offence in proposed subsection (1) is a 'basic offence, requiring a person to have intentionally communicated information, and to have been reckless, at the time of making the communication, to the circumstance that the information related to a special intelligence operation. The offence in proposed subsection (2) is an aggravated offence, which requires further proof that the person made the disclosure intending to cause a specified form of harm, or that the disclosure, in fact, had that effect. (The specified forms of harm relate to prejudicing the conduct of an operation, or endangering health or safety.)

The prosecution must prove each element of the relevant offence prosecuted beyond reasonable doubt. The applicable elements are discussed below, prefaced by a general explanation of the structure of Commonwealth criminal offences.

Structure of Commonwealth criminal offences

All criminal offences are comprised of physical elements and fault elements which apply to each physical element. (This is provided for in s 3.1 of the Criminal Code.)

In broad terms, physical elements relate to a person's actions (namely, conduct, an omission to act, a result of conduct, or a circumstance in which conduct occurs). Fault elements relate, in broad terms, to a person's state of mind in relation to the applicable physical element. (For example, a person's intention to engage in conduct, a person's knowledge that his or her conduct was likely to produce a certain result, or recklessness as to the existence of a particular circumstance). These elements are provided for in Part 2.2 of the Criminal Code.

Section 5.6 of the Criminal Code sets out a number of rules in relation to physical and fault elements, which apply to all Commonwealth offences, unless disapplied by an individual offence provision (noting that departures from standard fault elements applied by s 5.6 of the Criminal Code requires adequate justification in line with Commonwealth criminal law policy, and the expectations of relevant Parliamentary scrutiny committees).

Elements of the basic offence – unauthorised disclosure of information – s 35P(1)

(1) A person commits an offence if:

(a) the person discloses information; and

> Physical element: Conduct
> Reason: s 4.1(2) of the Criminal Code, which provides that conduct includes an action.
>
> Fault element: intention (that is, the person meant to engage in the conduct of disclosing information – as per the definition of intention in s 5.2(1) of the Criminal Code).
> Reason: s 5.6(1) of the Criminal Code, which provides that the fault element of intention applies to a physical element which consists of conduct.

(b) the information relates to a special intelligence operation.

> Physical element: circumstance
> Reason: s 4.1(c) of the Criminal Code, which provides that a circumstance is one in which conduct, or a result of conduct occurs.
>
> Fault element: recklessness. (That is, the person was aware of a substantial risk that the information disclosed relates to a special intelligence operation, and unjustifiably in the circumstances known to him or her took the risk of making the disclosure – as per the definition of recklessness in s 5.4(1) of the Criminal Code).
> Reason: s 5.6(2) of the Criminal Code, which provides that the fault element of recklessness applies to a physical element which consists of a circumstance.

Penalty: imprisonment for five years.

Elements of the aggravated offence – unauthorised disclosure of information – endangering safety, etc.

(2) A person commits an offence if:

(a) the person discloses information; and

Physical element: Conduct
Reason: s 4.1(2) of the Criminal Code, which provides that conduct includes an action.

Fault element: intention. (That is, the person meant to engage in the conduct of disclosing information – as per the definition of intention in s 5.2(1) of the Criminal Code.)
Reason: s 5.6(1) of the Criminal Code, which provides that the fault element of intention applies to a physical element which consists of conduct.

(b) the information relates to a special intelligence operation; and

Physical element: circumstance
Reason: s 4.1(c) of the Criminal Code, which provides that a circumstance is one in which conduct, or a result of conduct occurs.

Fault element: recklessness. (That is, the person was aware of a substantial risk that the information disclosed relate to a special intelligence operation, and unjustifiably in the circumstances known to him or her took the risk of making the disclosure – as per the definition of recklessness in s 5.4(1) of the Criminal Code.)
Reason: s 5.6(2) of the Criminal Code, which provides that the fault element of recklessness applies to a physical element which consists of a circumstance.

(c) either:

(i) the person intends to endanger the health or safety of any person or prejudice the effective conduct of a special intelligence operation; or

Fault element: intention
Reason: specified in the provision.

(ii) the disclosure of the information will endanger the health or safety of any person or prejudice the effective conduct of a special intelligence operation.

Fault element: recklessness
Reason: s 5.6(1) of the Criminal Code, which provides that the fault element of recklessness applies to a physical element comprising a circumstance.

Penalty: imprisonment for 10 years.

Explanation of the fault element of recklessness – ss 35P(1)(b) and (2)(b)

Members of the Committee sought more specific information from Departmental witnesses about the meaning of the fault element of recklessness, and how (if at all) it might apply to journalists who report on information, unaware that it related to a special intelligence operation.

As noted above, s 5.4(1) of the Criminal Code provides that a person is reckless with respect to a circumstance if:

(a) He or she is aware of a substantial risk that the circumstance existed. (For example, a person was aware of a substantial risk that the information related to a special intelligence operation); and

(b) Having regard to the circumstances known to the person, it was unjustifiable to take the risk. (For example, it was unjustifiable, in the circumstances known to the person at the time, to take the risk of disclosing the information.)

Hence, the two key concepts in relation to recklessness are awareness of a substantial risk that a circumstance existed, and the unjustifiable nature of the person's conduct in taking the risk.

Substantial risk

For the prosecution to prove that a person was aware of a substantial risk that the information disclosed related to a special intelligence operation under proposed s 35P, it would not be necessary to establish that a person had actual knowledge of that connection, in the sense of a conscious awareness of the existence of a special intelligence operation, and that the relevant information related to that operation.

However, the prosecution must establish, beyond reasonable doubt, that a person was aware of a real and not remote possibility that the information was so related. This will depend on the availability of evidence of the person's awareness of relevant information about an operation or suspected operation, which must suggest more than mere advertence to a nominal or speculative possibility that a special intelligence operation might have been declared, and that the information they proposed to communicate related to that operation. Importantly, the prosecution would need to prove, beyond reasonable doubt, that the person was aware of a real and not remote possibility that the information related not just to an intelligence or national security operation of some general kind, but specifically a special intelligence operation.

Contrary to the suggestions of some submitters and witnesses appearing before the inquiry that the fault element of recklessness is a low threshold, the Department notes that this element imposes a significant burden of proof on the prosecution in terms of proving, beyond reasonable doubt, a person's actual advertence to the existence of a risk that a very specific circumstance existed, and that this risk was substantial in nature. The assertions made by some submitters to this inquiry about the 'low' standard imposed by recklessness were recently made to, and rejected by, a recent review of Australia's counter-terrorism legislation, undertaken by a Committee chaired by the Hon Tony Whealy QC (a former judge of the New South Wales Supreme Court who presided over several major counter-terrorism trials). The Committee commented on the application of the fault element of recklessness, as it applies to various preparatory terrorism offences in Part 5.3 of the Criminal Code, in the following terms:

> It will be immediately apparent that this language [the definition of recklessness in s 5.4 of the Criminal Code] creates a high hurdle for the prosecution to clear where recklessness is alleged in a criminal trial. Indeed, it is a hurdle that is significantly higher than the ordinary usage or understanding of the term 'reckless' might suggest. A pedestrian who runs across a busy road might, in common parlance, be described as 'reckless'. But his behaviour, though probably negligent, would not ordinarily satisfy the statutory definition of the 'recklessness' fault element which requires actual advertence to the circumstance in question.
>
> A higher level of fault element in these preparatory offences is that of 'knowledge'. For example, Bilal Khazaal 'made' an e-book by compiling material on the internet and adding his own contribution. The book contained procedures and methods for assassinating world leaders. The prosecution had to prove that the defendant 'knew' that there was a connection between the book he had compiled and the fact it was connected with preparation for, or assistance in, a terrorist act. His conviction by the jury meant that the jury were satisfied that he had knowledge of that connection.
>
> By contrast, the element of 'recklessness' sets the bar below that of knowledge. If convicted, as might be expected, a person accused of a 'recklessness' offence will face a lower penalty than where 'knowledge' is alleged. Nevertheless, although the bar is set lower, it remains the task of the prosecution to prove that the defendant was aware of a substantial risk and that, having regard to the circumstances known to him or her, it was unjustifiable to take that risk. With these matters in mind, the Committee is not persuaded that the 'recklessness' element should be removed from the preparatory offences [in Part 5.3 of the Criminal Code].
>
> Source: Report of the Council of Australian Governments Review of Counter-Terrorism Laws, March 2014 at p. 17.

The application of the fault element of recklessness means that a successful prosecution could not be brought against a person who discloses information without any awareness that it could relate to a special intelligence operation, since there would be no evidence of an advertence to a risk of any kind. To the extent that a person is aware that information in his or her possession related to an investigation of some kind (but the precise nature of which was unknown), it would be a question of fact in individual cases as to whether that awareness amounted to advertence to a substantial risk that the information related specifically to a special intelligence operation. The Department does not accept suggestions that a mere awareness that ASIO is, or may be, involved in an activity of any kind must necessarily give rise to awareness of a substantial risk that there was a special intelligence operation on foot, particularly given the criminal standard of proof that would apply. Any awareness of substantial risk must also be considered alongside the second component of the fault element of recklessness, that taking that risk (making the disclosure) was unjustifiable in the circumstances known to the person at the time.

Unjustifiable taking of the risk

In addition to proving a person was aware of a substantial risk that the relevant circumstance existed, the prosecution must further prove that, having regard to the circumstances known to the person at the time of making the disclosure, it was unjustifiable to have taken the risk. The actions of a journalist in attempting to manage risk – such as by taking actions to independently check facts – would be relevant to an assessment of whether it was unjustifiable to have taken the risk by making the disclosure.

For example, a journalist who consulted with ASIO about any possible concerns in reporting on a matter, and acted in reliance on such consultation, would be unlikely to have been found to have acted unjustifiably in the circumstances known to him or her at the time. There is an established practice of consultation between journalists or media organisations and law enforcement agencies in relation to the publication of operational matters. Adherence to such a practice is directly relevant to the question of whether a communication was justified in the circumstances known to him or her at the time.

The policy justification for proposing the fault element of recklessness, rather than knowledge, as to the circumstance that information related to a special intelligence operation is, as noted above, that the wrongdoing targeted by proposed s 35P(1) is the disclosure of information about a covert operation that will, by its very disclosure, cause harm by jeopardising it covert nature. Proposed s 35P(1) gives effect to the imperative to deter such disclosures, and proposed s 35P(2) enables the imposition of a higher penalty in respect of persons who specifically intend to cause harm by the making of a disclosure. The fault element of recklessness clearly places an onus on persons contemplating making a disclosure of such information to consider whether or not their actions would be capable of justification.

Further safeguards

Committee questions

Members of the Committee asked Departmental and ASIO witnesses to provide further information about the way in which the ability to make public interest disclosures (whether by journalists or whistleblowers) about suspected wrongdoing is protected by the proposed offences.

Departmental response

Exceptions – s 35P(3)

In addition to the application of the fault element of recklessness to the circumstance that the information related to a special intelligence operation, a number of exceptions or 'offence-specific defences' apply in proposed s 35P(3). One such exception, in paragraph (b), applies to disclosures made for the purposes of any legal proceedings arising out of or otherwise related to the proposed new special intelligence operations scheme, or any report of any such proceedings. This means that a journalist who reported on any legal proceedings commenced in relation to a special intelligence operation would have a defence.

In these circumstances, it is unlikely a journalist would be subject to a prosecution given that the *Prosecution Policy of the Commonwealth* requires the Commonwealth Director of Public Prosecutions (CDPP) to assess the availability and strength of any potential defences as part of a decision to commence a prosecution.

Absence of a specific exception in favour of journalists

Some media organisations' submissions and public commentary have advocated for a specific exception to the offence in favour of journalists. It is contrary to the criminal law policy of the Commonwealth in relation to the design of secrecy offences to create special exceptions of this kind from the legal obligations of non-disclosure to which all other Australian citizens and bodies are subject. It is considered appropriate that all members of the community are expected to adhere to such non-disclosure obligations, which should apply equally to them – whether they are intelligence or law enforcement professionals engaged in a special intelligence operation, or journalists reporting on national security matters.

The absence of a specific exception in favour of journalists is also consistent with the fact that the wrongdoing to which the offences are directed is not the identity of the person making the disclosure, but the fact that operationally sensitive information has been disclosed. As Justice Hope observed in his 1984 report on ASIO, "the disclosure of secrets or the exposure of secure areas to risk through inadvertence or carelessness can result in just as much damage to the national interest as can result from espionage or sabotage". The offences in proposed s 35P are not directed to questioning the motives or legitimate interests of the media, or any other person, in seeking to ensure that matters relating to security threats can be reported. However, it needs to be recognised that the degree of damage to security caused by a disclosure of sensitive information does not depend on the motives of the discloser.

Application of the Public Interest Disclosure Act 2013

As some commentators have correctly identified, the offences in proposed s 35P do not contain an express defence for the good faith disclosure of information to an independent oversight body, in relation to suspected misconduct in relation to a special intelligence operation. This is in contrast to ss 15HK(3) and 15HL(3) of the Crimes Act, which create exemptions along these lines for reports made to the Ombudsman or the Law Enforcement Integrity Commissioner about suspected corruption or misconduct in relation to a controlled operation, provided that the disclosure is made in good faith and the discloser believes that the information may assist the relevant oversight body in performing its functions or duties.

This exemption has not been replicated in the provisions in Schedule 3 to the Bill because the relevant provisions in the Crimes Act were enacted in 2010, which pre-dated the *Public Interest Disclosure Act 2013* (PID Act). In broad terms, the PID Act provides avenues for the making of disclosures about suspected wrongdoing in relation to special intelligence operations to the Director-General of Security and the IGIS.

The Department is aware, however, that some submitters to the inquiry, including the IGIS, have made detailed comments about the application of the *Public Interest Disclosure Act 2013* to the proposed secrecy offences in the Bill (both proposed s 35P and the measures in Schedule 6). The Department intends to respond to these matters in a supplementary submission.

Prosecutorial discretion

Finally, the Department notes that, under the *Prosecution Policy of the Commonwealth*, the CDPP is required to consider whether a potential prosecution is in the public interest as part of making decisions about whether to commence a prosecution. The context in which a person's conduct occurred – potentially including the fact that it occurred in the course of his or her employment as a journalist – could potentially be taken into account in making this assessment. (However, the Department acknowledges that the CDPP is an independent agency which must make an assessment of all relevant matters in individual cases.)

Schedule 3 – special intelligence operations – differences to controlled operations

Committee questions

Committee members asked Departmental and ASIO witnesses to respond to the evidence of the IGIS in relation to differences between the proposed special intelligence operations regime in Schedule 3 to the Bill and the scheme of controlled operations in Part IAB of the *Crimes Act 1914* in relation to covert law enforcement operations. (Recognising that Schedule 3 implements the Government's response to recommendation 28 of the Committee's 2013 report, which suggested the establishment of a special intelligence operations regime, subject to similar safeguards and accountability arrangements as those applying to controlled operations.)

In particular, Departmental witnesses were invited to respond to differences identified by the IGIS in relation to authorisation, oversight and opportunities for judicial scrutiny.

Departmental response

As noted in the Explanatory Memorandum to the Bill (at p. 96), the provisions of Schedule 3 are based broadly on the controlled operations scheme in Part IAB of the Crimes Act, but appropriate modifications have been made to reflect the differences between a law enforcement operation to investigate a serious criminal offence, and a covert intelligence-gathering operation conducted for national security purposes.

As such, the schemes are similar at a broad level. (For example, the schemes are similar in terms of their general approaches in conferring limited protections from criminal and civil liability, provided that the relevant participants in an operation and the particular conduct are authorised in accordance with a prescribed statutory process and authorisation criteria, in advance of the operation commencing. The schemes are also similar in terms of the fact they incorporate reporting and oversight arrangements.) However, as is acknowledged in the Explanatory Memorandum (at p. 96), the precise content of each broad area has been adapted to suit the different purposes to which law enforcement and intelligence operations are directed. Further information about the key differences mentioned by the IGIS are set out below.

Authorisation

As the IGIS and other submitters to the inquiry have observed, under proposed s 35C, authorities to conduct special intelligence operations are made on a purely internal basis by an 'authorising officer' (defined in s 4 as the Director-General or a Deputy Director-General of Security). While controlled operations under Part 1AB of the Crimes Act are initially authorised internally by a senior law enforcement officer (such as the Australian Federal Police Commissioner or a Deputy Commissioner), any extensions beyond a period of three months must be authorised by a member of the Administrative Appeals Tribunal nominated by the Minister (s 15GT)

This has not been replicated in the proposed special intelligence operations provisions in Schedule 3 to reflect a necessary difference in the separate purposes to which each scheme is directed. Controlled operations for law enforcement purposes are generally shorter-term, with the primary objective of obtaining evidence for the prosecution of a serious offence. In contrast, intelligence operations are often longer term, and are aimed at obtaining intelligence over a period of time so as to understand the activities and plans of persons and groups of security concern.

Decisions about the commencement and conduct of a covert intelligence gathering operation are appropriately made by the Director-General of Security of a Deputy Director-General. These senior officers have the necessary visibility and detailed understanding of the security environment and the conduct of intelligence operations to make decisions about authorisations, including in time critical circumstances. In addition, these officers are invested with the power to cancel an authority at any time, and for any reason. The scheme further operates under the extensive oversight jurisdiction of the IGIS, to whom the Organisation must report every six months (as well as to the Attorney-General) on special intelligence operations that are in progress.

Oversight

Division 4 of Part 1AB of the Crimes Act establishes a specific compliance and monitoring regime in relation to controlled operations, which is overseen by the Ombudsman who must make a specific annual report. The Ombudsman is invested with specific information gathering and inspection powers.

A comparable regime is not considered necessary in relation to special intelligence operations, having regard to the extensive general oversight jurisdiction of the IGIS and the fact that special intelligence operations are conducted by ASIO alone (whereas controlled operations may involve participants from multiple agencies).

Judicial scrutiny

The IGIS noted in her submission (at p. 15) that special intelligence operations carry "less likelihood of judicial scrutiny". This is largely attributable to the focus of special intelligence

operations on the collection of intelligence relevant to security. This means that such operations are more likely to continue, on a covert basis, for a longer period of time than controlled operations.

However, it is relevant to note that neither the provisions in the proposed special intelligence operations scheme, nor those in the existing controlled operations regime purport to remove the jurisdiction of a court to hear matters relating to the conduct of either type of operation. (That is, the regimes do not contain such features beyond the conferral of limited immunities on participants, the availability of prima facie evidentiary certificates to protect sensitive information with respect to the granting of an authority to conduct an operation, and a modification of the general discretion of the court to exclude evidence merely on the basis it was obtained in the course of conduct that would otherwise have constituted an offence, but for the application of a limited immunity under the relevant scheme.)

Other differences

The Department is aware that some submitters to the inquiry have undertaken a detailed comparative analysis of the relevant provisions in relation to special intelligence operations and controlled operations. As such, the Department will provide a further response, addressing matters of detail, in its supplementary submission to the Committee. (Particular areas of focus include: notification requirements in the controlled operations provisions that do not have an equivalent in the special intelligence operations provisions; differences in maximum duration; differences in maximum penalties applying to non-disclosure offences; and differences in the protections afforded to participants in relation to civil liability, with the controlled operations provisions conferring an indemnity rather than an immunity from suit as is the case for special intelligence operations.

Responses to other matters raised by the Inspector-General of Intelligence and Security

Committee question

Committee members invited the Department and ASIO to provide responses to any further matters raised by the IGIS in her submission to the inquiry and evidence given in her appearance before the Committee on 15 August.

Departmental response

The Department's responses to several key matters in the IGIS's submission and evidence are set out under the subheadings below.

The Department acknowledges the contribution of the IGIS to the development and scrutiny of the measures in the Bill, and will provide a more comprehensive response to the balance of the issues she has identified as part of its forthcoming supplementary submission to the Committee. (This supplementary submission will address key issues arising from other submissions and oral evidence provided to the Committee.)

Schedule 1 – ASIO employment, etc

IGIS oversight of ASIO affiliates

The IGIS's submission to the inquiry commented (at pp. 6 and 7) that "it may not always be clear who falls within the class of an ASIO affiliate for the purpose of oversighting the numerous legislative powers and restrictions that are dependent on the term", and that assessments will need to be made on a case-by-case basis.

This is the intended manner in which oversight arrangements would apply to ASIO affiliates. (That is, the definition is readily capable of application to an individual or a class of persons in the context of a particular complaint or inquiry, having regard to the relevant contract, agreement or other arrangement for the performance of functions or services for the Organisation). It is not intended that a comprehensive list of all ASIO affiliates should be prepared, or necessarily able to be produced, at a given point in time.

Secondment of persons to and from ASIO

The IGIS's submission further commented that – notwithstanding the commentary in the Explanatory Memorandum to the Bill suggesting that ASIO employees who are seconded to another body or organisation will not retain their ASIO powers while on secondment – this result is not clear on the face of the relevant provision in proposed new s 86 of the ASIO Act.

The Department's view is that the intended result articulated at p. 43 of the Explanatory Memorandum is inherent in the nature of a 'secondment', in accordance with the ordinary meaning of that term. We would also expect that it would be made clear in arrangements made at the time of the secondment. If further clarification is thought desirable, it would be possible to have a qualification to this effect – in the nature of an 'avoidance of doubt' styled provision – in proposed new s 86.

Schedule 2 – Powers of the Organisation

Reporting in relation to activities impacting or potentially impacting on third parties

The IGIS's submission and evidence to the inquiry indicated that the inclusion of certain, additional matters in Ministerial reporting requirements on warrants could assist in her oversight role. (For example, requirements to report on any use of force against persons; the causation of any interference with or disruption to lawful use of a computer; any access to third party computers or communications in transit; and any entry to third party premises. It was suggested that reporting requirements on these matters could also explain the reasons for which these activities were carried out, and the result.)

The Department understands that the IGIS has not suggested the inclusion of a specific reporting requirement to her Office on these matters, having regard to her existing statutory powers of oversight in relation to ASIO warrants and existing practices in examining samples of warrants. The Department further acknowledges that the IGIS considers additional

reporting requirements to the Attorney-General would enhance her capacity to conduct effective oversight.

The Department notes, however, that the administrative burden associated with any legislatively mandated Ministerial reporting on some of the above measures could potentially be considerable. (For example, activities authorised under a computer access warrant that are likely to cause non-material interference with lawful use of a computer.) The Department considers that an alternative solution may be to distinguish between those matters considered to be sufficiently 'exceptional' to justify an indefinite, statutory reporting requirement to the Minister, and those which could be managed through practical measures (such as internal record keeping, and inspections by the IGIS).

Threshold for use of third party computers and communications in transit in order to gain access to data on a target computer

The IGIS's submission (at p. 10) and evidence to the inquiry commented on the relevant threshold for use of a third party computer or communication in transit under a computer access warrant in proposed s 25A(4)(ab), and an identical threshold for such use under an identified persons warrant in proposed s 27E(2)(d). (This threshold is that it was reasonable in all of the circumstances to use the third party computer or communication in transit, having regard to other methods – if any – that are likely to be as effective in gaining access to the relevant data in the target computer.)

The IGIS noted that this is different to the test applied to a 'B-Party warrant' under s 9(3) of the *Telecommunications (Interception and Access) Act 1979.* The test for a B-Party warrant is that the Attorney-General must be satisfied that ASIO has exhausted all other practicable methods, or the interception would not otherwise be possible.

The policy and operational justifications for this distinction are detailed in the Explanatory Memorandum to the Bill (at p. 71), which states that: "To clarify, this does not require ASIO to exhaust all other methods of accessing the target computer. In considering whether to use a third party computer or communication in transit, ASIO must have regard to all the circumstances, which could potentially include the intrusiveness of ASIO's actions, the risk of detection, complexity of implementation and risk of harm".

The Department further notes that a 'last resort' styled requirement was considered in the development of this provision, but determined to be unduly restrictive. For example, such a test may result in the Organisation needing to rely on another way of accessing the relevant data, even though it would be more complex and carry a greater risk of harm or detection. Instead, the proposed amendments require an assessment to be undertaken of the availability of other, comparably effective, methods. This is taken into account as a relevant consideration in assessing the reasonableness, in all of the circumstances, of using a third party computer or communication in transit.

This proposed amendment must also be considered alongside the Attorney-General's Guidelines to ASIO, issued under s 8A of the ASIO Act. Under the Guidelines, ASIO is

required to use as little intrusion into individual privacy as possible, consistent with the performance of its functions. They also require ASIO, wherever possible, to use the least intrusive method of gathering intelligence before using more intrusive techniques.

Identified persons warrants – authorisations issued by the Director-General

The IGIS's submission noted (at p. 14) that the new provisions will enable decision making about the authorisation of activities under warrants issued by the Attorney-General "to be devolved … to the Director-General, whose decisions will be subject to IGIS oversight". The submission further noted that "many of the tests in the proposed legislation will turn on whether the decision maker was satisfied on reasonable grounds that something will substantially assist in the collection of intelligence relevant to security. These decisions will be subject to IGIS oversight".

As the IGIS's comments indicate, the ability of the Director-General to authorise activities under an identified person warrant enhances, rather than diminishes, the scope for independent oversight by the IGIS, given that Ministerial decisions may not be amenable to oversight.

Administrative and resourcing impacts of Schedule 2 measures on the Office of the IGIS

The IGIS's submission and evidence to the inquiry noted that the proposed amendments to ASIO's special powers under Division 2 of Part III of the ASIO Act would, if enacted, impact on the resourcing requirements of her Office (including creating a need for greater access to technical expertise), and the way in which oversight is conducted (such as in relation to the use of warrantless surveillance powers, given an existing practice of inspecting a sample of warrants).

As the Prime Minister announced on 5 August 2014, the Government has committed to increasing the resources of the Office of the IGIS, to ensure it can perform its important oversight function in relation to the measures proposed in this Bill, if enacted. The IGIS has been consulted on the anticipated resource impacts of the proposals.

Schedule 3 – Special Intelligence Operations

Reporting

The IGIS's submission (at p. 15) and evidence to the inquiry commented that there are "no detailed reporting requirements" in the proposed scheme of special intelligence operations beyond six monthly reporting to the Attorney-General and the IGIS under proposed s 35Q, and that there will be a need for periodic review of such operations while they are on foot, not only at their conclusion.

The Department acknowledges the IGIS's suggestion that contemporaneous reporting (such as on the commencement of an operation) could assist in conducting oversight. Whether there should be an additional, statutory requirement that mandates such reporting (as distinct

from settling arrangements at a practical level, at least while the provisions are newly in force) would need to be weighed carefully against potential operational impacts.

Cancellation of authority

The IGIS's submission further noted (at p. 15) that there is no obligation on an authorising officer (the Director-General or a Deputy Director-General of Security) to cancel an operation if the grounds have ceased to exist, or if they are no longer satisfied of the relevant matters.

The Department notes that, while the provisions in Schedule 3 to the Bill do not impose an obligation on the authorising officer to cancel a special intelligence operation for these reasons, the authorising officer is invested with a broad discretion under proposed s 35G to cancel an authority at any time, and for any reason. This would include satisfaction that the relevant authorisation criteria are no longer satisfied. The IGIS's oversight jurisdiction would extend to decision-making in relation to the exercise of discretion under proposed s 35G.

Schedule 4 – ASIO cooperation with private sector bodies

Scope of proposed new s 19(1)(d) – cooperation with "any other body whether within or outside Australia"

The IGIS's submission (at p. 16) commented on the proposed amendment to s 19(1) of the ASIO Act, which would insert a new paragraph (d) allowing ASIO to cooperate with (so far as is necessary for, or conducive to the performance of its functions, and subject to any arrangements or directions given by the Attorney-General) "any other person or body whether within or outside Australia". The IGIS advanced an opinion that this provision may exceed the intended scope of recommendation 33 of the Committee's 2013 report, which suggested an amendment to formalise ASIO's capacity to cooperate with private sector entities.

The IGIS's concern is that the reference to "any … person or body whether within or outside Australia" in proposed s 19(1)(d) could be applied to foreign bodies or persons not approved by the Attorney-General in such a way as to impact on current arrangements for ensuring compliance with human rights obligations. Given that many corporate entities may have offices outside Australia, it is important that a geographical limitation is not applied to proposed paragraph (d). However, the persons or bodies ASIO is cooperating with under this provision would still be subject to any arrangements made or directions given by the Attorney-General, as provided in subsection 19(1).

Schedule 5 – activities and functions of Intelligence Services Act agencies

Training in use of weapons, etc for self-defence purposes

The Department acknowledges the suggestion in the IGIS's submission (at p. 19) that the proposed amendments to the Intelligence Services Act to authorise the use of weapons in a

'controlled environment' confer a power as distinct from a clarification of existing powers (as described in the Explanatory Memorandum to the Bill).

To the extent that there may be any doubt or competing views about the legality or otherwise of such activities under the present provisions, the Department submits that this heightens the need for amendments to be made, in order to ensure certainty and transparency as to the existence of such authorisation (including applicable limitations and conditions). The Department will, however, assist the Government in giving consideration to whether the Explanatory Memorandum to the Bill should be amended in light of the IGIS's comments.

Schedule 6 – protection of information

The Department notes the remarks of the IGIS in her written submission to the inquiry (at p. 20) concerning the potential impact of the proposed offences in Schedule 6 to the Bill on the following matters, and the need for clear advice to be provided about these.

- The making of complaints to the IGIS, or the pro-active disclosure of information outside the IGIS's formal statutory inquiries or the regime under the Public Interest Disclosure Act.

- The impact, if any, of agreements signed by IGIS staff in order to access information of, or relating to, certain agencies on the ability of these persons to convey such information to the IGIS and other staff in that Office.

As noted above, several submissions to the inquiry have commented on the interaction of the proposed new and amended offences with public interest disclosures. Accordingly, the Department will respond collectively to these comments in its supplementary submission to the Committee.