Summary of AGD and ASIO responses to key issues raised by the Committee

Computer access warrants (Schedule 2)

***Issue*:** In light of amendments to the definition of a 'computer' to include a computer network, the Committee has asked the Department and ASIO to consider linking access under a computer access warrant to a person, entity or event .

***Summary of response*:** the Department and ASIO note that the computer access provisions are limited by the concept of a 'security matter' (being a matter that is important in relation to security, as 'security' is defined in s 4 of the ASIO Act). As the term 'security matter' is not defined in the ASIO Act beyond 'a matter that is important in relation to security', the Department and ASIO acknowledge that there is scope to clarify its meaning. Any clarification of the 'security matter' needs to provide sufficient flexibility to enable ASIO to effectively utilise computer access warrants to perform its functions and should therefore be inclusive rather than exhaustive and broad enough to capture one or more of the following:

- a person or persons, including individuals, groups, bodies corporate or bodies politic, whether the person's identity is known or unknown; or
- an entity or entities, including bodies corporate or bodies politic, countries, and organisations or groups, whether known or unknown; or
- an activity.

The preference is that this is done via the Explanatory Memorandum to the Bill, or in the Attorney-General's Guidelines to ASIO issued under s 8A of the ASIO Act. This is because the word 'matter' for the purposes of the term 'security matter' is intended to take its ordinary meaning (covering persons, entities and activities), and because it is desirable to ensure that sufficient flexibility is retained to enable ASIO to effectively utilise computer warrants to perform its work.

Special intelligence operations – authorisation model (Schedule 3)

Issue: the Committee has sought responses from the Department and ASIO to a suggestion that authorisation decisions could be made on an external basis – for example, by an issuing authority who is a judicial officer or a tribunal member appointed in a personal capacity.

***Summary of response*:** the Department and ASIO are of the view that an internal authorisation model is necessary and appropriate, given the intrinsically operational nature of such decisions. Decisions about the commencement, continuation and conduct of covert intelligence operations are highly sensitive and specialised matters. They require an extensive awareness and understanding of the security environment and the way in which intelligence operations are conducted. Such expertise is essential in making decisions, particularly in time critical and rapidly developing circumstances. Internal decision-making is also consistent with the statutory role of the Director-General of Security, under whose control the Organisation is placed by s 8(1) of the ASIO Act. In addition, it is noted that a

special intelligence operation is materially different to a warrant under Divisions 2 and 3 of Part III of the ASIO Act. Warrants pertain to a specific activity or a technique, whereas a special intelligence operation is an entire operation, which involves multiple activities and techniques. An external authorisation model may also reduce the opportunity for the IGIS to conduct oversight of authorisation decisions because decisions made by persons who are independent of the Organisation would not fall within the statutory remit under the IGIS Act.

The Department and ASIO acknowledge the importance of subjecting authorisation decisions to the independent oversight of the IGIS, in addition to the general oversight of the Attorney-General. Accordingly, some additional notification requirements have been suggested for inclusion in the Bill, to ensure that the IGIS's statutory powers of oversight can be exercised in a timely manner in relation to special intelligence operations.

Special intelligence operations – differences to controlled operations (Schedule 3)

Issue: the Committee asked the Department and ASIO to provide a detailed itemisation and explanation of differences between the proposed special intelligence operations scheme and the controlled operations scheme in Part 1AB of the Crimes Act.

Summary of response: While the special intelligence operations scheme is modelled on that of the controlled operations scheme, some necessary adjustments have been made to reflect the purpose of the special intelligence operations scheme to collect security intelligence as distinct from the collection of evidence relevant to serious criminal offences. Key areas of difference concern: authorising officers; authorisation criteria; duration of operations; requirements for variation of authorities; penalties and exceptions applying to disclosure offences; protection of participants from civil liability; notification requirements if personal injury, or serious loss or damage is caused; and protections from civil liability. A table of the key differences is at Attachment 1 to the Submission.

Non-disclosure provisions – interaction with IGIS complaints and inspections (s 35P, Schedule 3 and Schedule 6)

Issue: the Committee asked the Department and ASIO to consider the submissions and evidence of the IGIS, which suggested it would be desirable to include additional legislative protections for persons making legitimate disclosures to the IGIS and for the IGIS and her staff in performing statutory functions under the IGIS Act.

Summary of response: the Department and ASIO consider that there would be benefit in giving express effect to the intention that the offence provisions should not apply to the making of complaints to the IGIS outside the regime in the *Public Interest Disclosure Act 2013*, or the conduct of the IGIS and her staff in undertaking inspections outside formal inquiries. The Department and ASIO will support the Government in considering this matter, including with the benefit of any views the Committee may wish to provide.

ASIO employment amendments – 'ASIO affiliate' (Schedule 1)

Issue: the Committee asked the Department and ASIO to respond to some stakeholder concerns that the proposed new term 'ASIO affiliate' might be applied to legal persons, with the result that entities such as foreign intelligence agencies could be subject to the provisions in the Bill authorising, or enabling the authorisation of, ASIO affiliates to perform certain activities and functions.

Summary of response: the Department and ASIO confirm that the definition of 'ASIO affiliate' is intended to be limited to natural persons, and will assist the Government in considering whether an explanation should be included in the Explanatory Memorandum.

Safeguards referenced in the Explanatory Memorandum

Issue: the Committee asked the Department and ASIO to address the comments of some submitters and witnesses that various safeguards referred to in the Explanatory Memorandum are not, in their view, readily identifiable in the corresponding provisions of the Bill.

Summary of response: In light of these and other comments about the Explanatory Memorandum, the Department and ASIO are assessing whether further material could be included in relevant places to assist the understanding of the legislative package. Some potential improvements have been identified, explaining the legislative safeguards which apply to specific provisions in the Bill, together with the broader safeguards that apply to intelligence agencies' conduct. The Department and ASIO will assist the Government in considering possible revisions to the Explanatory Memorandum, including with the benefit of any comments the Committee may wish to provide.

UNCLASSIFIED

Joint supplementary submission

Attorney-General's Department and Australian Security Intelligence Organisation

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

August 2014

Contents

Introduction

The Attorney-General's Department (Department) and the Australian Security Intelligence Organisation (ASIO) are pleased to provide this joint submission to the Committee, as a further aid to its consideration of the provisions of the National Security Legislation Amendment Bill (No 1) 2014 (the Bill).

This submission is intended to supplement the submissions of the Department (No 1) and ASIO (No 16) to the Committee, the evidence of Departmental and ASIO witnesses at hearings of the Committee on 15 August (in public session) and 18 August (in private session), and the Department's written responses to matters taken on notice at the public hearing of 15 August and provided to the Committee on 18 August.

In particular, this submission provides a combined Departmental and ASIO response to key issues raised by members of the Committee at the private hearing on 18 August, to which Departmental and ASIO witnesses were invited to respond in writing. This submission further addresses a number of other issues raised by submitters to, and witnesses appearing before, the inquiry.

Outline of submission

This submission is organised into two parts. Part 1 addresses the key issues raised by the Committee at its private hearing with the Department and ASIO on 18 August. These issues concern proposed amendments to the *Australian Security Intelligence Organisation Act 1979* (ASIO Act) in Schedules 2, 3 and 6 to the Bill. (Part 1 also includes a classified attachment, marked Attachment 1, which provides further examples of matters related to computer access).

Part 2 addresses the balance of major issues identified by submitters and witnesses to the Committee, which were not previously addressed in the Department's responses to matters taken on notice at the hearing of 15 August. These issues are summarised below.

Issues addressed in Part 1 (key issues raised by the Committee)

- ***Computer access warrants (Schedule 2)*** – a response to the Committee's invitation to consider possible ways in which the Bill could explicitly or more clearly prescribe the requisite connection between a target computer (particularly a computer network) or a third party computer and the relevant 'security matter' in respect of which a computer access warrant is issued. (This invitation was issued further to concerns identified by some submitters and witnesses to the inquiry about possible 'overbreadth' in the proposed

new definition of a computer, and provisions authorising the use of third party computers to access data in a target computer.)[1]

- ***Authorisation of special intelligence operations (Schedule 3)*** – a response to the Committee's invitation to consider a suggestion for an independent authorisation process for such operations, perhaps analogous to that applied to ASIO questioning warrants and questioning and detention warrants issued under Division 3 of Part III of the ASIO Act. (This invitation was issued further to expressions of support for such a model by various submitters and witnesses to the inquiry.)[2]

- ***Comparison of proposed special intelligence operations and controlled operations provisions (Schedule 3)*** – a response to the Committee's request for an itemisation and explanation of the key differences between the respective schemes. (This invitation was issued further to the evidence of some submitters and witnesses that there should be either uniformity of, or a closer degree of alignment between, the particular provisions applying to each scheme, notwithstanding the discrete purposes to which they are directed.)[3]

- ***Non-disclosure provisions in the Bill (s 35P in Schedule 3, and Schedule 6)*** – a response to the Committee's invitation to consider whether it may be desirable to include additional legislative protections for persons making legitimate disclosures to the Inspector-General of Intelligence and Security (IGIS), and for the IGIS and her staff in performing statutory functions under the *Inspector-General of Intelligence and Security Act 1986* (IGIS Act). (This invitation was made further to the submission and evidence of the IGIS that such express protections would be desirable, and suggestions of other submitters and witnesses that the general protections available under the *Public Interest Disclosure Act 2013* are too limited in their application to some or all of the proposed new and amended offences in the Bill, or that additional offence-specific defences are required.)[4]

---

1 Gilbert + Tobin Centre of Public Law, *Submission 2*, pp. 2-5; Associate Professor Greg Carne, *Submission 5*, p. 7; Media Entertainment and Arts Alliance, *Submission 6*, p. 8; Law Council of Australia, *Submission 13*, pp. 15-16; Electronic Frontiers Australia, *Submission 9*, p. 4; Senator David Leyonhjelm, *Submission 15*, pp. 3-4; Joint Media Organisations, *Submission 17*, pp. 4-5; Pirate Party Australia, *Submission 18*, pp. 5-7; Civil Liberties Councils, *Submission 20*, pp. 3-7; Blueprint for Free Speech, *Submission 22*, pp. 10-13; Muslim Legal Network, *Submission 21*, pp. 3-4. See also Proof Committee Hansard, 18 August 2014, p. 10 (Electronic Frontiers Australia), pp. 23, 25, 26-27 (Gilbert + Tobin Centre of Public Law); pp. 36-37 (Coalition of Media Organisations).

2 Gilbert + Tobin Centre of Public Law, *Submission 2*, pp. 7-8; Guardian Australia, *Submission 12*, p. 6; Law Council of Australia, *Submission 13*, pp. 8, 39. See also Proof Committee Hansard, 18 August 2014, p. 7 (Law Council of Australia), p. 22 (Civil Liberties Councils), pp. 24-25 (Gilbert + Tobin Centre of Public Law), p. 38 (Australian Lawyer's Alliance).

3 Gilbert + Tobin Centre of Public Law, *Submission 2*, pp. 6-7; Law Council of Australia, *Submission 13*, pp. 7, 29-45; Blueprint for Free Speech, *Submission 22*, pp. 4-7. See also Proof Committee Hansard, 18 August 2014, pp. 6-7 (Law Council of Australia), p. 24 (Gilbert + Tobin Centre of Public Law).

4 Inspector-General of Intelligence and Security, *Submission 4*, p. 20; Proof Committee Hansard, 15 August 2014, pp. 5-6. See also: Gilbert + Tobin Centre of Public Law, *Submission 2*, pp. 8-9; Law Council of Australia, *Submission 13*, pp. 8, 40-45; Media, Entertainment and Arts Alliance,

- ***ASIO employment amendments (Schedule 1)*** – a response to the Committee's invitation to consider whether an amendment of the proposed definition of an 'ASIO affiliate' is necessary to ensure, or to communicate clearly, that this term is limited to natural persons, consistent with the policy intention. (This invitation was extended further to concerns identified by some submitters and witnesses to the inquiry that the new term may be capable of application to legal persons, such as foreign intelligence agencies.)[5]

- ***Safeguards referenced in the Explanatory Memorandum*** – a response to the Committee's invitation to address the comments of some submitters and witnesses that various safeguards described in the Explanatory Memorandum were not, on their reading of the Bill, readily identifiable in the corresponding provisions.[6]

Issues addressed in Part 2 (additional issues raised by submitters and witnesses)

Part 2 provides Departmental and ASIO comments in response to major issues raised by submitters and witnesses in the course of the inquiry. These issues are listed below under relevant Schedules to the Bill.

Schedule 1 – ASIO employment

Secondment

- Suggestions that additional conditions or limitations are included in proposed new s 86, in relation to the secondment of ASIO employees to other bodies or organisations.[7]

ASIO affiliates

- Suggestions that the proposed new term 'ASIO affiliate' cannot be described as a minor or technical amendment because it is said to have been applied, in some of the consequential amendments in Schedule 1, to increase the number of persons able to perform certain functions or duties under certain legislation.[8]

Submission 6, pp, 6-7; Australian Lawyers' Alliance, *Submission 7*, pp. 3-5; Electronic Frontiers Australia, *Submission 9*, pp. 7-8; Guardian Australia, *Submission 12*, pp. 8-10; Law Council of Australia, *Submission 13*, pp. 40-45; Mr Bruce Baer Arnold, *Submission 14*, p. 5; Senator David Leyonhjelm, *Submission 15*, p. 3; Joint Media Organisations, *Submission 17*, pp. 2-4; Professor AJ Brown, *Submission 19*, pp. 1-4; Civil Liberties Councils, *Submission 20*, pp. 10-12; Blueprint for Free Speech, *Submission 22*, pp. 8-10; Alison Bevege, *Submission 23*, pp. 7, 12-13. See also, Proof Committee Hansard, 18 August 2014, pp. 8-9 (Law Council of Australia), p. 13 (Electronic Frontiers Australia), p. 26 (Gilbert + Tobin Centre of Public Law); pp. 33-35 (Media Entertainment and Arts Alliance).

5 See, for example, Electronic Frontiers Australia, Proof Committee Hansard, 18 August 2014, p. 10.

6 See, for example, Electronic Frontiers Australia, Proof Committee Hansard, 18 August 2014, p. 12; Civil Liberties Councils, Proof Committee Hansard, 18 August 2014, pp. 10-11, 21-22.

7 Law Council of Australia, *Submission 13*, pp. 12-13; Muslim Legal Network, *Submission 21*, p. 1.

8 Law Council of Australia, *Submission 13*, pp. 13-15.

Schedule 2 – powers of the Organisation

Reporting and oversight

- Suggestions that ASIO's reports to the Attorney-General in relation to warrants could address some additional matters, particularly relating to activities which impact on third party privacy or other interests (such as use of force, and third party computer use).[9]

Additional privacy related requirements

- Suggestions that the Attorney-General's Guidelines to ASIO under s 8A of the ASIO Act be reviewed, particularly in light of privacy impacts of the proposed amendments.[10]
- Suggestions that the issuing criteria for all ASIO warrants under Division 2 of Part III include a specific privacy impact test.[11]

Entry to third party premises

- Suggestions that authority under a warrant to enter third party premises is made subject to additional thresholds, in the nature of a last resort requirement, or a requirement that there is a substantial risk of detection unless third party premises are accessed.[12]
- Suggestions that entry to third party premises be accompanied by a requirement to notify the owner or occupant, and to rectify any interferences made to the third party premises.[13]

Use of force against persons

- Suggestions that the power is unnecessary, or that it should expressly exclude the use of lethal force or force which is likely to cause grievous bodily harm.[14]

Evidentiary certificates

- A suggestion that proposed s 34AA should expressly exclude material that may address or prove the substantive elements of a criminal offence.[15]

---

9 Inspector-General of Intelligence and Security, *Submission 4*, pp. 10, 11, 12, 14.

10 Office of the Australian Information Commissioner, *Submission 11*, pp. 2-3 and Proof Committee Hansard 18 August 2014, pp. 29-30. See also Law Council of Australia, *Submission 13*, pp. 11-12.

11 Law Council of Australia, *Submission 13*, pp. 8, pp. 17-18.

12 Law Council of Australia, *Submission 13*, p. 26.

13 Civil Liberties Councils, *Submission 20*, p. 8.

14 Law Council of Australia, *Submission 13*, pp. 8-9; 28-29; Muslim Legal Network, *Submission 21*, p. 11.

15 Law Council of Australia, *Submission 13*, pp. 26-27. See also Muslim Legal Network, *Submission 21*, p. 14 (opposed the inclusion of s 29 emergency warrants in s 34AA).

- An unintended omission of search warrants from the scheme of evidentiary certificates, to the extent that computer access is authorised under the proposed amendments to s 25(5).

Classes of persons authorised to exercise powers under warrants

- A suggestion that there is not a demonstrated need for the proposed amendments to s 24 of the ASIO Act, to enable the authorisation of classes of persons rather than individuals.[16] (It was further suggested that that the maintenance of lists of individuals authorised to exercise powers under warrants is a valuable accountability measure, and should be retained.)[17]

Variation of warrants

- A suggestion that the power to vary warrants should be limited to variations of a minor and technical nature.[18]

Identified persons warrants

- Suggestions that investing the Director-General of Security with the power to authorise the exercise of powers under an identified person warrant issued by the Attorney-General, together with the threshold for authorisation, represents a lowering of the threshold and the dilution of accountability.[19]

Surveillance devices

- Suggestions that the requirements in s 16(2) of the *Surveillance Devices Act 2004* (SDA) are replicated in proposed s 26 of the ASIO Act.[20] (Subsection 16(2) of the SDA prescribes matters to which the issuing authority must have regard, including the likely effect on a person's privacy, the existence of any alternative means to obtain the evidence or information, the extent to which the information sought would assist the investigation, its evidentiary value, and any previous warrants sought or issued.)

- Suggestions that the single authorisation provision in proposed s 26 may dilute the degree of specificity currently required under the existing, device-specific provisions (particularly in the assessment of how each device is necessary if multiple devices are specified in a single warrant application).[21] (A related suggestion was that the new

16 Law Council of Australia, *Submission 13*, p. 28. See also Joint Media Organisations, *Submission 17*, p. 5.

17 Muslim Legal Network, *Submission 21*, p. 10.

18 Law Council of Australia, *Submission 13*, pp. 9, 29.

19 Associate Professor Greg Carne, *Submission 5*, pp. 5-6. See also Muslim Legal Network, *Submission 21*, pp. 9-10. But cf Law Council of Australia, *Submission 13*, pp. 19-20.

20 Law Council of Australia, *Submission 13*, pp. 8, 22-23. (The Law Council also suggested that the judicial authorisation model in the SDA be adopted in relation to ASIO's surveillance warrants: at p. 23).

21 Law Council of Australia, *Submission 13*, p, 23.

structure is likely to "produced maximised applications for the use of multiple devices, in relation to multiple targets".)[22]

- Suggestions that it is unclear how, in practice, an issuing authority will be able to ensure that the relevant thresholds are met in relation to persons whose identity may not be known.[23]

- Suggestions that the warrantless surveillance powers in proposed ss 26C and 26D may have the potential to enable a broader category of people (ASIO employees and ASIO affiliates) to utilise highly intrusive devices without a warrant.[24]

- Suggestions that the reporting requirements applying under the SDA should be replicated in the ASIO Act.[25]

Computer access warrants

- Suggestions that the limited ability to add, copy, delete or alter data on a computer under s 25A may limit any evidential value of intelligence obtained under a computer access warrant, or may impact on the ability of a person to receive a fair trial in prosecutions in which intelligence is adduced as evidence.[26]

Schedule 3 – special intelligence operations

- Suggestions that there is an inadequate policy or operational justification for the enactment of a new scheme of special intelligence operations (including insufficient evidence of need, and suggestions that immunity from legal liability should not apply to intelligence operations because they are distinguishable from law enforcement operations).[27]

- Suggestions that a sunset clause should be applied to the proposed scheme, with a further requirement that an independent review be carried out prior to sunsetting.[28]

---

22 Associate Professor Greg Carne, *Submission 5*, pp. 4-5.

23 Law Council of Australia, *Submission 13*, p. 23.

24 Law Council of Australia, *Submission 13*, p. 24.

25 Law Council of Australia, *Submission 13*, pp. 22-23.

26 Electronic Frontiers Australia, *Submission 9*, p. 4.

27 Gilbert + Tobin Centre of Public Law, *Submission 2*, pp. 6-7; Guardian Australia, *Submission 12*, p. 6; Law Council of Australia, *Submission 13*, pp. 7, pp. 30-31; Civil Liberties Councils, *Submission 20*, pp. 8-10; Muslim Legal Network, *Submission 21*, pp. 17-19; Blueprint for Free Speech, *Submission 22*, p. 4. See also Proof Committee Hansard, 18 August 2014, pp. 17, 21-22 (Civil Liberties Councils).

28 Gilbert + Tobin Centre of Public Law, *Submission 2*, p. 8; Law Council of Australia, *Submission 13*, pp. 39-40; Civil Liberties Councils, *Submission 20*, p. 10. See also Blueprint for Free Speech, *Submission 22*, pp. 13-14 (suggested 'periodic sunsetting' of all measures in the Bill every two years).

Schedule 4 – ASIO cooperation and information-sharing

Private sector cooperation

- Suggestions that the Attorney-General's Guidelines to ASIO (issued under s 8A of the ASIO Act) should be revised to specifically address the types of activities envisaged will be carried out under the new private sector cooperation ground in s 19(1)(d) of the ASIO Act.[29]

Ability to refer breaches of s 92 of the ASIO Act to law enforcement

- Objections to the current form of the offence in s 92 of the ASIO Act (concerning the publication of the identity of an ASIO employee or an ASIO affiliate), on the basis that it should be subject to various exceptions, generally in connection with criminal proceedings initiated against an ASIO employee or affiliate, or other forms of alleged misconduct or maladministration by such a person.[30]

Schedule 5 – activities and functions of Intelligence Services Act 2001 agencies

Operational security ground of Ministerial authorisation

- Suggestions that the new ground in proposed s 9(1A)(a)(iiia) of the *Intelligence Services Act 2001* may be unnecessary. Some submitters suggested that the definition of 'operational security' proposed to be included in s 3 of that Act is already covered (in full or in part) by the existing security ground in s 9(1A)(a)(iii).[31] Another submitter argued that the ground is unnecessary because the matters it purports to cover are properly the functions of ASIO.[32]

- Suggestions that paragraph (b) of the proposed definition of operational security (prevention of the integrity of ASIS operations from reliance on inaccurate or false information) is unduly vague and should either be removed or limited to the precise language in recommendation 38 of the Committee's 2013 report (being protection from "intelligence or counter-intelligence activities"), or otherwise limited to exclude matters of lawful advocacy, protest or dissent.[33]

- Suggestions that a new privacy impact test should be applied to Ministerial authorisations by the Defence Minister for defence intelligence agencies to undertake activities in

29 Office of the Australian Information Commissioner, *Submission 11*, p. 3; Proof Committee Hansard, 18 August 2014, p. 30.

30 Law Council of Australia, *Submission 13*, p. 46; Muslim Legal Network, *Submission 21*, p. 6.

31 Law Council of Australia, *Submission 13*, pp. 7, 50-51. See also Inspector-General of Intelligence and Security, *Submission 4*, p. 17. (The IGIS noted the existence of "significant overlap" but indicated that this is not, of itself, a problem from an oversight perspective).

32 Associate Professor Greg Carne, *Submission 5*, p. 9.

33 Associate Professor Greg Carne, *Submission 5*, pp. 9-10.

relation to the operational security of ASIS under the proposed new ground in s 9(1A)(a)(iiia).[34]

ASIO cooperation with ASIS

- Suggestions that the removal of the requirement for Ministerial authorisation in the circumstances covered by proposed s 13B of the Intelligence Services Act may undermine existing standards of accountability, and that the need for the amendments has not been demonstrated.[35]

- Possible record-keeping requirements or practices, particularly a register of requests made and actioned by ASIS.[36]

- Suggestions that the Bill should prescribe the kinds of activities that may be undertaken in accordance with proposed s 13B, a maximum duration, and specific requirements for internal approvals and proposed renewals.[37]

Amendments to the statutory functions of the Australian Geospatial-Intelligence Organisation

- Suggestions that the proposed amendments to the statutory functions of the Defence Imagery and Geospatial Organisation (formally renamed the Australian Geospatial-Intelligence Organisation by Schedule 7 to the Bill) are of potentially significant effect in substantive terms, contrary to the suggestion in the Explanatory Memorandum that these measures are clarifications or incremental extensions of this organisation's functions.[38]

Schedule 6 – protection of information

Coverage of existing offences

- Comments that the proposed new offences in the ASIO Act and Intelligence Services Act (concerning unauthorised dealings with intelligence-related records and the unauthorised recording of intelligence-related information) are unnecessary, on the basis that the wrongdoing sought to be targeted is already addressed by existing offences, including those in the Crimes Act in respect of official secrets.[39]

---

34 Law Council of Australia, *Submission 13*, p. 51.

35 Gilbert + Tobin Centre of Public Law, *Submission 2*, pp. 10-11; Proof Committee Hansard, 18 August 2014, p. 24.

36 Inspector-General of Intelligence and Security, *Submission 4*, p. 19 (noted that there is no requirement that would require ASIS to keep a register of Australian persons that are the subject of activity in response to an ASIO request under the new scheme.)

37 Law Council of Australia, *Submission 13*, pp. 9, 50.

38 Muslim Legal Network, *Submission 21*, pp. 15-17.

39 Gilbert + Tobin Centre of Public Law, *Submission 2* (see also Attachment 1 to that submission) and Proof Committee Hansard, 18 August 2014, p. 28.

Penalties

- Comments that the proposed increase in penalties applying to existing offences in the ASIO Act and Intelligence Services Act for the unauthorised communication of intelligence-related information are too high, including because they are inconsistent with other Commonwealth secrecy offences. (The relevant penalties are proposed to be increased from two years' imprisonment to 10 years' imprisonment);[40]

Elements of the offences

- Suggestions that the proposed amended and new offences should include an element that the person intended to cause harm by engaging in the unauthorised conduct, particularly in relation to the unauthorised communication offences in light of the proposed increase in penalty.[41]
- Suggestions that the offences should only apply to persons who are in a contractual relationship or a relationship of employment with the relevant intelligence agency, and not those who are in an 'arrangement'.[42]

Suggestions for a further review of the Bill

- A suggestion that the Bill should be referred to the Independent National Security Legislation Monitor for inquiry and report, in advance of the Parliament determining whether the Bill should be passed.[43]

Part 1 – Key issues raised by the Committee

Computer access warrants

Outline of issues

The measures in Schedule 2 to the Bill include amendments implementing the Government's responses to recommendations 20, 21 and 22 of the Committee's 2013 *Report on the Inquiry into Potential Reforms to Australia's National Security Legislation* (2013 report).

These recommendations are directed to modernising ASIO's warrant based powers to access computers, where there are reasonable grounds for believing that access to data held in a particular computer will substantially assist in the collection of intelligence in respect of a matter that is important to security. These recommendations are, in summary, that:

40 Gilbert + Tobin Centre of Public Law, Submission 2, p. 12; Media, Entertainment and Arts Alliance, *Submission 6*, p. 7; Law Council of Australia, *Submission 13*, p. 52.

41 Law Council of Australia, *Submission 13*, p. 53. See also Gilbert + Tobin Centre of Public Law, Proof Committee Hansard 18 August 2014, p. 28.

42 Gilbert + Tobin Centre of Public Law, *Submission 2*, pp. 12-13.

43 Law Council of Australia, *Submission 13*, pp. 7, 56; Proof Committee Hansard, 18 August 2014, p. 2.

- The definition of computer in s 22 of the ASIO Act be amended to include multiple computers operating in a network (recommendation 20).
- The computer access provisions be amended to stipulate that access may be authorised to all computers at a nominated location and all computers directly associated with a nominated person (recommendation 20).
- Further consideration be given to amending the computer access provisions to enable the disruption of a target computer for the purpose of executing a computer access warrant (recommendation 21).
- The computer access provisions be amended to authorise the use of third party computers and communications in transit to access a target computer (recommendation 22).

The Committee has invited the Department and ASIO to suggest options to address concerns identified by some submitters and witnesses to the inquiry about perceived 'overbreadth' in:

- the proposed new definition of a computer in s 22 of the ASIO Act (particularly in the coverage of computer networks); and
- provisions authorising the use of third party computers to access data in a target computer that is relevant to a matter that is important in relation to security.

Amending the definition of a 'computer' to include computer networks

Proposed amendments

The current definition of a 'computer' in s 22 of the ASIO Act – which includes a computer system or part of a computer system – allows ASIO to access data held within a number of computers and connected devices if they are part of the same computer system.

However, it may not always be clear, in advance, whether particular computers are part of the same system, and this may rapidly change as computer connectivity is reconfigured. As a consequence, the present definition of a 'computer' means that multiple computer access warrants across multiple appointments with the Attorney-General may be required in respect of the same security matter. This can present challenges and inefficiencies where data relevant to a security matter is stored on multiple computers. As the operation of multiple computers in varying degrees of network connectivity (whether physical or virtual) is now commonplace, it is highly probable that relevant data will be stored in multiple computers. As the Committee recognised in its 2013 report, it is therefore necessary in the modern technological and security environment, that ASIO be able to use and access data held in a computer network under a computer access warrant.

Accordingly, amending item 4 of Schedule 2 inserts a new definition of 'computer' in s 22, which means all or part of:

- one or more computers;
- one or more computer systems;
- one or more computer networks; or
- any combination of the above.

The new definition will apply to the test for issuing computer access warrants in s 25A(2), which in its present form provides the Minister is only to issue a warrant if satisfied that there are reasonable grounds for believing that access by the Organisation to data held in a particular computer ('the target computer') will substantially assist the collection of intelligence in accordance with the ASIO Act in respect of a matter ('the security matter') that is important in relation to security.

Consistent with the intention of recommendation 20 that ASIO can apply for a single computer access warrant to obtain intelligence relating to a security matter from multiple computers, amending item 16 removes the reference to a "particular" computer from s 25A(2).

Proposed new s 25A(3) further inserts a new definition of a 'target computer' for the purpose of s 25A(2), which implements the second part of recommendation 20 in the Committee's 2013 report, that computer access warrants should authorise access to all computers at a nominated location, and all computers directly associated with a nominated person. Proposed new s 25A(3) defines a target computer as 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)".

Submissions and evidence

Some submitters and witnesses to the inquiry have argued that the proposed definitional amendment unreasonably broadens the application of ASIO's computer access warrants.[44] It has been said, for example, that a 'target computer' for the purpose of a computer access warrant could now include all computers connected to the internet, or all computers connected to a large local network such as the intranet or shared storage drives of a large organisation or an institution like a university, company or government department.[45]

Some stakeholders have expressed concern that the definitional amendments, in combination with the amendments to s 25A, are overly broad in two key respects. First, it was said that "large numbers of innocent persons could … be exposed to potentially severe invasions of

44 See footnote 1 above.

45 See, for example, Gilbert + Tobin Centre of Public Law, *Submission 2*, p. 3 and Proof Committee Hansard, 18 August, p. 5. See also Law Council of Australia, *Submission 13*, p. 16.

their privacy",[46] on the basis that all parts of a computer network could be accessed on the strength of the Minister's satisfaction under s 25A(2) that there are reasonable grounds for believing that such access will substantially assist in the collection of intelligence in respect of a security matter.[47] It was suggested that this issuing threshold was too low in its application to warrants covering multiple computers like those on a network. For example, it was said that:

> ASIO will be able to access entire computer networks (such as those of a workplace where a person of security interest is employed or a university where the person is studying) in the same way as they are currently able to access a single target computer. This means that ASIO could access and copy the files of other users on a network, such as those of colleagues or other university students, where this would 'substantially assist' in the collection of intelligence in relation to that person.[48]

Secondly, it was suggested that the limited ability under ss 25A(4) and (5) to undertake activities likely to cause material interference with, or interruption or obstruction of, the lawful use of a computer by a third party, where necessary to access relevant data, was too low a threshold in its application to computer access warrants covering multiple computers (particularly those on a network).[49] It was suggested that the absence of a definition of 'material' for the purpose of s 25A(5) "means that it is not clear that they would be sufficient to protect against significant delays or interruptions to the use of computer networks by third parties".[50]

Stakeholder proposals

Submitters and witnesses to the inquiry made proposals directed to four key areas, as summarised below.

Key area 1: Linkages between a computer network and the 'subject' of a warrant operation

A number of submitters and witnesses suggested that s 25A should expressly prescribe the requisite form of connection between the target computer (including systems or networks)

---

46 Gilbert + Tobin Centre of Public Law, *Submission 2*, p. 3.

47 Gilbert + Tobin Centre of Public Law, *Submission 2*, p. 3. It is noted, however, that this submission did not appear to address the authorisation requirements in s 25A(4) for the specific activities to be undertaken under a warrant. In addition to the threshold for authorising a warrant, the Minister must be satisfied under s 25A(4)(a), as it is proposed to be amended by this Bill, that it is appropriate in the circumstances to authorise the use of a target computer for the purpose of obtaining access to data held in the target computer that is relevant to the security matter in respect of which the warrant is issued. As is noted subsequently in this submission, if sensible analysis is to be undertaken of the scope of, and limitations on, the proposed amendments to ASIO's computer access warrants, ss 25A(2) and 25A(4) must be examined cumulatively, together with s 25A(5) which operates as a qualification on activities able to be authorised under s 25A(4).

48 Gilbert + Tobin Centre of Public Law, *Submission 2*, p. 4.

49 For example, Gilbert + Tobin Centre of Public Law, *Submission 2*, pp. 4-5; Law Council of Australia, *Submission 13*, p. 19.

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

sought to be accessed under a warrant, and the relevant person, entity or event that is the focus of the warrant operation.[51] Some key proposals included:

- ***Define the term 'computer network'*** in order to limit it to "computers that are linked in some substantive way, such as by having shared storage drives, and not merely by virtue of being connected to the internet or by some other telecommunications technology".[52]

- ***Re-cast the definition to apply to "multiple computers operating on a network"*** rather than providing that a 'computer' for the purpose of s 22 includes a 'network'. This would adopt the exact language of recommendation 20 in the Committee's 2013 report. It would mean that that a network is not, itself, recognised as a computer under s 22.[53]

Key area 2: An additional issuing test in s 25A(2) where the target computer is a network

Another possible limitation identified by submitters and witnesses was a 'necessity' or 'reasonable necessity' test for the issuing of warrants authorising access to a computer network as a target computer.[54] Such a test could operate to require the Attorney-General to be satisfied that access to a computer network would be necessary to access the relevant data, as well as being satisfied that access to such data would substantially assist in the collection of intelligence relevant to security.

Key area 3: Separate or additional authorisation requirements in s 25A(4) for using computer networks to access relevant data

It was further suggested by some submitters and witnesses that separate or additional authorisation requirements should apply in s 25A(4) in relation to a target computer that is a network, and it is proposed to use that network (for example, by using a computer connected to it) to gain access to relevant data on it. Proposals included:

- ***A 'last resort' requirement***, which would require all other methods of gaining access to the relevant data (that is, all methods other than accessing the network) must have been exhausted or are impracticable in the circumstances.[55]

- ***A 'minimal intrusion'[56] or proportionality[57] test***, which might operate to require that any use of a computer network to gain access to relevant data must be done with as little

51 See, for example, Gilbert + Tobin Centre of Public Law, *Submission 2*, pp. 3-4. See also Proof Committee Hansard, 18 August 2014, p. 25.

52 Gilbert + Tobin Centre of Public Law, *Submission 2*, p. 3. See also: Law Council of Australia, *Submission 13*, p. 16; Senator David Leyonhjelm, *Submission 15*, p. 3 (suggested that the definition should only cover 'local networks').

53 Gilbert + Tobin Centre of Public Law, Proof Committee Hansard, 18 August 2014, p. 25.

54 Gilbert + Tobin Centre of Public Law, *Submission 2*, p. 4; Proof Committee Hansard, 18 August 2014, p. 27.

55 ibid.

56 Gilbert + Tobin Centre of Public Law, Proof Committee Hansard, 18 August 2014, p. 27.

57 Law Council of Australia, *Submission 13*, p. 16.

impact as possible on the privacy of persons using that network, or that use of the network must be established to be the least intrusive way of accessing the relevant data, or that the likely benefit to an investigation should substantially outweigh the extent to which access is likely to interfere with the privacy of any person or persons.

- ***A 'reasonable grounds' requirement***, under which there must exist 'reasonable grounds' on which to believe that a person of security concern had access to a computer on a network.[58]

Key area 4: Further limitations on the ability to undertake an activity likely to cause material interference, interruption or obstruction to lawful users of a computer network under s 25A(5)

- ***Define the term 'material' for the purpose of s 25A(5).*** Some members of the Committee also questioned whether the terms 'material interference', 'material obstruction, and 'material interruption' should be defined for the purpose of s 25A(5) to make clear the scope of the limited ability to engage in conduct likely to cause such outcomes, where necessary to gain access to the relevant data.

Departmental and ASIO comments on stakeholder proposals

The Department and ASIO acknowledge the objective of Committee members and stakeholders to ensure that the ability to access networked computers is duly limited. The below comments examine – but do not support – the above proposals outlined by submitters and witnesses participating in the inquiry.[59] The Department and ASIO have identified a possible alternative proposal to give effect to the Committee's objective, which is also detailed below.

Comments on stakeholder proposals

The Department and ASIO have significant concerns about, and do not support the adoption of, any of the above amendments proposed by submitters and witnesses participating in the inquiry. Comments on specific proposals are set out below.

In general, the Department and ASIO are concerned that these proposals place inadequate weight on existing limitations in s 25A(4)(a) on the purpose for which computer access is permitted. (That is, to obtain data relevant to the particular security matter in respect of which a warrant is issued under s 25A(2), if the Attorney-General is satisfied that the specific activity through which that data is to be obtained is appropriate in the circumstances.)

Several of these proposals may also unduly limit the ability of the provisions to apply to new computer technologies, because they would entrench an approach that is limited to current

58 Gilbert + Tobin Centre of Public Law, *Submission 2,* p, 4; Law Council of Australia, *Submission 13,* p. 16.

59 The Department and ASIO note that the Gilbert + Tobin Centre of Public Law has undertaken to provide a supplementary submission containing further proposed amendments: Proof Committee Hansard, 18 August, p. 27. The Department and ASIO would be pleased to assist the Committee with comments on any further proposals it may receive in the course of its inquiry.

technology, contrary to the intention of the reforms to modernise outdated provisions. Some proposals would further unduly limit the ability to assess the circumstances of individual cases.

Proposal to define a 'computer network' or to adopt the exact wording of recommendation 20 in s 22

The Department and ASIO do not support a definition of a computer network in s 22. The concept of a computer network is constantly evolving. Defining this term, rather than relying on its ordinary meaning, risks having a quickly dated and inadequate definition.

Rapid advances in technology and changes to the way technology is commonly used in society make it desirable to adopt 'technology-neutral' language in legislation. It is for this reason that 'computer network' and 'computer' are not exhaustively defined in the ASIO Act or in the *Criminal Code Act 1995* (which contains the offences that would otherwise make computer access by ASIO unlawful if it is not authorised under a computer access warrant).

In addition, amending the definition to 'multiple computers operating on a network' would not appear to address the underlying concern about the breadth of a computer network.

Proposal for an additional issuing test in s 25A(2) in relation to computer networks

It would not be feasible to require the Attorney-General to be satisfied of an additional requirement under s 25A(2), that access to a computer network is necessary to access data relevant to a security matter (in addition to being satisfied that there are reasonable grounds for believing that access to the relevant data will substantially assist in the collection of intelligence in respect of a security matter). The issuing test in s 25A(2) reflects that a warrant is granted in advance of any access, with the result that it is not possible to conclusively determine, at the time of issuing, that access to a computer network is necessary. (For these reasons, it would be similarly problematic to include a 'necessity' test in s 25A(4)(a), in relation to the use of a computer connected to a target network to access relevant data on that network.)

Proposals for separate or additional requirements for using computer networks to access relevant data under s 25A(4)

The Department and ASIO do not support proposals for separate or additional requirements to be included in s 25A(4) in relation to the use of a computer network to access data on that network that is relevant to the security matter specified in the warrant. This is on the basis ss 25A(2) and (4) contain appropriate limiting mechanisms.

In combination, ss 25A(2) and (4) require approval of both the need to access data on a network, and the specific way in which that data is to be accessed. In both cases, approval must be made by reference to an assessment of the connection between the relevant decision (access and a specific activity) and the purpose of collecting intelligence that is relevant to a specified security matter. In particular:

- The threshold requirement for the issuing of a warrant in s 25A(2) is that the Attorney-General must believe that access by the Organisation to data held in the computer network (specified as the target computer) will substantially assist the collection of intelligence in respect of a specified security matter.

- The authorisation requirement in s 25A(4)(a) is that the Attorney-General must consider it appropriate in the circumstances to authorise the use of the target computer network (or any other electronic equipment or a data storage device) for the purpose of obtaining access to data that is relevant to the security matter specified in the warrant and is held in the network specified as the target computer.

'Reasonable grounds' proposal

In addition to the above reasons, an additional requirement in the form of a 'reasonable grounds' test would not be appropriate because it assumes that a 'security matter' for the purpose of ss 25A(2) and (4) must be a person. Consistent with evidence provided to the Committee in private session, a security matter is not so limited. It may also not be possible to determine in advance whether there are reasonable grounds to believe that a person of security concern had access to a particular computer on a network.

'Minimal intrusion' or 'last resort' proposals

The proposals for 'minimal intrusion' or 'last resort' requirements in s 25A(4), in relation to the use of a computer connected to a target network in order to access data on that target network, are not supported because they are unduly restrictive. For example, a 'last resort' test may result in ASIO being unable to access relevant data on the network, because it may require ASIO to rely on another way that is more complex and would carry a greater risk of detection.

The entrenchment of a 'minimal intrusion' requirement in s 25A(4) may also require priority to be given automatically to the least intrusive method of accessing data, and may not allow for appropriate weight to other considerations like effectiveness and risk. It is preferable that the Attorney-General makes an assessment of whether the proposed use of a computer on a target network to access relevant data is "appropriate in the circumstances", within the limitations set out in s 25A(5) in relation to activities likely to cause material interference, interruption or obstruction, or likely to cause other material loss or damage to users of the network.

Decisions about the appropriateness of an activity in all of the circumstances can be informed by all relevant considerations arising in a particular case. This can include an assessment of the impacts on third party users of a network, relative to the effectiveness and necessity of the proposed activity in accessing data relevant to the security matter in respect of which the warrant is issued. In addition, ASIO must, in making warrant applications and undertaking activities under warrants, act in accordance with the relevant privacy requirements in the Attorney-General's Guidelines to ASIO. These relevantly require ASIO to conduct its

activities with as little intrusion into privacy as possible, consistent with the performance of its functions.

Consistent with these requirements, ASIO may, in appropriate cases, limit its applications to parts of a network. Under proposed s 25(3A)(b) the Attorney-General may also issue a warrant subject to such restrictions or conditions as he or she sees fit to impose. This may include limiting access to part of a network.

Proposal to define 'material' interference, obstruction or interruption in s 25A(5)

As explained in the Department's responses to the matters taken on notice at the public hearing of 15 August and evidence given by Departmental and ASIO witnesses at that hearing, the inclusion of a definition of the term 'material' in s 25A(5) is not supported. 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. It is important that the material (or otherwise) nature of any likely disruption, interference or obstruction – or likely other loss or damage to lawful users of a computer – is able to be determined in individual cases.

Given the covert nature of computer access under ASIO's special powers in Division 2 of Part III, there is a strong operational need to ensure that, in all computer access operations, the absolute minimum interruption or interference to the subject's computer or service is caused. Accordingly, it is not in ASIO's intelligence collection objectives to interfere or interrupt a computer in a way which is material and draws the attention of the target or any other person to that interference or interruption.

Alternative proposals

Some Committee members suggested that it might allay concerns raised by some submitters and witnesses if s 25A were to include an express link between the access to a target computer (particularly a network) and the person or entity that is the focus of the warrant operation. As noted above, the computer access provisions are limited by the concept of a 'security matter'. The Department and ASIO have given consideration to three proposals, for providing further guidance on what is meant by the term 'security matter'. These are:

(1) ***Preferred option*** – include an explanation of the intended meaning of the term 'security matter' as it applies to s 25A in the Explanatory Memorandum to the Bill.

(2) ***Second preferred option*** – include a clarification in the Attorney-General's Guidelines to ASIO about the meaning of a 'security matter' for the purpose of s 25A.

(3) ***Non-preferred option*** – include a non-exhaustive definition of the term 'matter' in the ASIO Act, for the purpose of the term 'security matter'.

These proposals and supporting justification, together with further background on the term, are outlined below.

Meaning of a 'security matter'

The term 'security matter' is not defined in the ASIO Act, beyond the statement that it is **a matter that is important in relation to 'security'**. In this context 'security' is defined in s 4 of the Act to include:

(a) the protection of, and of the people of, the Commonwealth and the States and Territories from:
   i. espionage;
   ii. sabotage;
   iii. politically motivated violence;
   iv. promotion of communal violence;
   v. attacks on Australia's defence system; or
   vi. acts of foreign interference;
   vii. whether direct from, or committed within, Australia or not; and

(b) the protection of Australia's territorial and border integrity; and

(c) the carrying out of Australia's responsibilities to any foreign country in relation to the matters mentioned above.

The term 'matter' is intended to take its ordinary meaning. It is defined in the Macquarie Dictionary, for example, as a "thing, affair or business". As such, it is apparent that the term is capable of covering persons, entities or other things such as activities, and does not require the relevant matter to be known, in the sense that a particular person or entity, or a specific activity, must be identified. This is important because a requirement that ASIO's ability to access a computer under warrant must be linked to a known person or a known entity would significantly limit its ability to investigate serious security threats. Such investigation may be necessary to identify a person or an entity. Accordingly, relying on the ordinary meaning of the term 'matter' for the purpose of interpreting the term 'security matter' strikes a balance between certainty and flexibility.

Justification for an amendment – legal necessity v 'reassurance'

The Department and ASIO acknowledge and agree with the Committee's desire to provide reassurance to the wider community in relation to what is meant by a 'security matter', and therefore how the thresholds for computer access would remain appropriately limited by ss 25A(2), (4) and (5) (together with the wider oversight and accountability framework within which ASIO operates) if the proposed amendment to s 25A were enacted.

The Department and ASIO do not consider there to be a strict legal need to define the term 'matter' for the purpose of the definition of the term 'security matter' in Division 2 of Part III of the ASIO Act. As mentioned above, the ordinary meaning of the term 'matter' is sufficiently clear, and its practical application is well established in relation to the tests for computer access warrants as well as search warrants.

The Department and ASIO emphasise that significant care must be taken in framing any proposed clarifications for inclusion in either primary legislation or in guidelines, to ensure that capability is not unintentionally limited. Sufficient flexibility is required in the interpretation of the term 'security matter' to enable ASIO to effectively utilise computer access warrants to perform ASIO's functions.

Any such requirements should be inclusive rather than exhaustive and broad enough to capture one or more of the following:

- a person or persons, including individuals, groups, bodies corporate or bodies politic, whether the person's identity is known or unknown; or
- an entity or entities, including bodies corporate or bodies politic, countries, and organisations or groups, whether known or unknown; or
- an activity.

The Department and ASIO further emphasise that care would need to be taken in the selection of specific terms within any inclusive definition of a 'matter' for the purpose of the definition of a 'security matter'. (For example, the inclusion of an 'event' in preference to an 'activity' may be open to a narrow interpretation as a significant or scheduled occurrence with particular dates, such as the G20 or another major sporting or political event.)

Form of amendment – legislation v guidelines

Taking into account the above considerations, it is suggested that the best way of balancing the interests in 'reassurance' with those in maintaining flexibility and drafting integrity is to include some commentary in the Explanatory Memorandum to the Bill on the meaning of the term 'security matter', and outline how it will apply to the proposed amendments to s 25A. The Department and ASIO will assist the Government in considering possible amendments to the Explanatory Memorandum.

It is acknowledged, however, that the Committee may prefer any clarification to be made legislatively rather than in the extrinsic materials to the Bill. The Department and ASIO consider that any clarification of the meaning of the word 'matter' for the purposes of the term 'security matter' should be incorporated in the Attorney-General's Guidelines to ASIO rather than the ASIO Act itself.

It is important that the regulatory framework within which ASIO operates is capable of keeping pace with, and accommodating rapid changes to, the security environment, including developments in the technology used by people ASIO investigates. A major risk associated with a statutory definition is that it may entrench in legislation provisions that become outdated, or require amendment if unintended consequences arise.

Guidelines issued by the Attorney-General provide greater flexibility to respond to such changes, but have the same mandatory status by reason of s 8A(1)(a) of the ASIO Act. (This provision states that "the Minister may, from time to time, by written notice given to

the Director-General, give to the Director-General guidelines to be observed: (a) in the performance of its functions or the exercise of its powers".) In addition to the phrase "to be observed" in the above provision operating to impose an obligation on ASIO to comply with the Guidelines, ASIO's compliance is also subject to oversight by the IGIS.

The Guidelines are also subject to considerable scrutiny. In accordance with ss 8A(3)-(6) of the ASIO Act, the Attorney-General is required to cause a copy of any guidelines issued to be laid before each House of Parliament and is required to give a copy to the Leader of the Opposition, Inspector-General of Intelligence and Security and the PJCIS.

Use of third party computers and communications in transit to access target computers

Proposed amendments

Schedule 2 to the Bill amends ss 25A(4) to implement the Government's response to recommendation 22 of the Committee's 2013 report, to authorise the use of third party computers and communications in transit to access a target computer.

As the Committee recognised in its 2013 report, technological advancements have created challenges in the execution of computer access warrants, especially when a person of security interest is security conscious. In some circumstances, use of a third party computer is necessary to obtain access to data in a target computer, which is relevant to the security matter in respect of which a warrant is issued.

In line with recommendation 22, proposed new s 25A(4)(ab) enables the Minister, where considered appropriate in the circumstances, to authorise the use of any other computer (or a communication in transit) to access the relevant data in a target computer. This is provided that use of the third party computer or communication in transit is reasonable in all of the circumstances, having regard to other methods (if any) of obtaining access to the relevant data which are likely to be as effective. The authorisation to use a third party computer or communication in transit includes the ability to add, copy, delete or alter other data in the computer or communication in transit, if necessary to achieve the purpose of obtaining access to the relevant data in the target computer.

As acknowledged in the Department and ASIO's evidence to the inquiry, this test is different to that applied to 'B-Party' warrants under s 9(3) of the *Telecommunications (Interception and Access) Act 1979* (TIA Act) (which applies a 'last resort' requirement in that the Attorney-General must be satisfied that ASIO has exhausted all other practicable methods, and access to the relevant intelligence would not otherwise be possible).

Submissions and evidence

Some submitters and witnesses participating in the inquiry argued that the threshold in proposed s 25A(4)(ab) is too low, "given the severe implications for privacy that access to a

person's computer entails".[60] A number of submitters argued in favour of a 'last resort' styled test, such as:

- an identical formulation to that applying to B-Party warrants under s 9(3) of the TIA Act (detailed above);[61] or
- a more stringent test again, being that access is necessary to obtain access to the relevant data, and that all other methods of obtaining access have been exhausted (as distinct from all other practicable methods).[62]

These suggestions appear to be additional to proposals summarised above to strengthen statutory requirements as to the requisite 'linkage' between access to a target computer and the security matter in respect of which a warrant is issued.

Departmental and ASIO comments

The Department and ASIO support the retention of s 25A(4)(ab) as drafted. As noted in the Department's responses to matters taken on notice at the Committee's hearing of 15 August, a 'last resort' requirement was considered in the development of s 25A(4)(ab), but was determined to be unduly restrictive. This is for largely the same reasons as those set out above in relation to the possible 'last resort' test proposed by some stakeholders in relation to the use of computer networks as target computers.

For example, applying a last resort test to the use of a third party computer or a communication in transit to access relevant data on a target computer may result in ASIO 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 to access relevant data on the target computer.

The requirement that the use of a third party computer must be "reasonable in all of the circumstances" is an additional safeguard to those which currently apply under the ASIO Act for use of a third party computer. Under the existing computer access warrant provisions, ASIO already has the authority to use a third party computer to access data on a target computer that is relevant to the security matter in respect of which the warrant is issued. This authority does not require ASIO to determine whether the use is reasonable in all of the circumstances.[63] As such, the proposed test represents a strengthening of existing safeguards, in a way that accommodates necessary operational considerations.

---

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

61 Law Council of Australia, *Submission 13*, p. 17.

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

63 It is noted, however, that amendments are required to this existing power of access because the ability to add, delete or alter data under s 25A(4)(a) is presently limited to data in the target computer. It is

The test applied by s 25A(4)(ab) must be also considered in the context of the broader safeguards and oversight applicable to the issuing and execution of computer access warrants, and to ASIO's activities more generally. These include the statutory tests for issuing computer access warrants and the authorisation of activities under those warrants, the Attorney-General's Guidelines to ASIO, and independent oversight by the IGIS.

Tests for issuing warrants and authorising activities under warrants

In particular, under s 25A(4)(ab), ASIO may only use a third party computer or a communication in transit to access the relevant data. 'Relevant data' is defined in s 25A(4)(a) as data on a target computer that is relevant to 'the security matter' – that is, the matter that is important in relation to security in respect of which the warrant was issued under s 25A(2).

This is a significant limitation on the purpose for which a third party computer may be used. It means that if ASIO is to use a third party computer, it must be for the purpose of accessing data on the target computer. (For example, the third party computer cannot be used only as if it were a target computer, in order to obtain data relevant to security, irrespective of whether that data is relevant to the specific security matter in relation to which the warrant was issued).

This limitation means that a third party computer cannot be used to:

- Gain access to a target computer to access data solely because it is considered relevant to security. Rather, the third party computer must be used to access data in the target computer that is relevant to the particular security matter in respect of which the warrant was issued under s 25A(2).

- Add, copy, modify or delete or alter data in the third party computer except where there is a purpose of gaining access to data in the target computer that is relevant to the security matter in respect of which the warrant was issued under s 25A(2). (For example, data in the third party computer cannot be copied or altered only because it would be a convenient or desirable way of gaining access to data in the third party computer. Similarly, data in the third party computer cannot be copied or altered only because it may assist in collecting intelligence relevant to a security matter, irrespective of whether or not it is relevant to the specific security matter in respect of which the warrant was issued.)

Similarly, if ASIO is to use a communication in transit, it must be for the purpose of gaining access to relevant data (being that which is on a target computer, and is related to the security matter in respect of which the warrant was issued). The contents of a communication in transit cannot, themselves, be accessed or used solely because they are considered relevant to

---

also necessary to have this power in relation to data in the third party computer, for the purpose of gaining access to data in the target computer. This amendment (inserted by amending item 23 of Schedule 2) is consistent with what ASIO can do now under a computer access warrant in relation to a target computer.

security in some way (irrespective of whether that is the specific security matter in relation to which the warrant was issued, or some other security matter). Interception of a communication in transit will continue to be subject to the requirements of the TIA Act.

In addition, any interference with the lawful use of a third party computer in executing a computer access warrant will be limited in accordance with proposed new s 25A(5) (as discussed above). As such, ASIO will not be able to do anything under a computer access warrant that is likely to materially interfere with, interrupt or obstruct the lawful use of a third party computer unless necessary to execute the warrant (noting that 'necessary' means essential rather than convenient). ASIO will not, in any circumstances, be permitted to do any thing that is likely to cause other material loss or damage to persons lawfully using a third party computer.

Further, under s 25A(4), the Attorney-General will need to be satisfied that the use of a third party computer or a communication in transit is appropriate in the circumstances before specifying that authority in the warrant. The Attorney-General may, under proposed s 25A(3A)(b), also specify any conditions or restrictions in the warrant.

Other safeguards

In addition to the limited purposes for which use of a third party computer is permitted, ASIO's use of third party computers under warrant will also be subject to the following, significant safeguards:

- The Attorney-General's Guidelines to ASIO, which require ASIO to use as little intrusion into individual privacy as is possible, consistent with the performance of its functions; and wherever possible to use the least intrusive techniques of collecting information before using more intrusive techniques.

- Oversight by the IGIS, who has access to every warrant, and may conduct inspections or inquiries in accordance with the IGIS Act.

Subject to further consideration of the suggestions made by the Office of the Australian Information Commissioner (concerning a review of the Guidelines)[64] and the IGIS (concerning reporting in relation to warrants),[65] the Department and ASIO consider that the above matters are adequate and appropriate safeguards for the use of third party computers as authorised under warrant, including where the target computer specified in a warrant is a network.

64 Office of the Australian Information Commissioner, *Submission 11*, p. 2; Proof Committee Hansard, 18 August 2014, p. 29.

65 Inspector-General of Intelligence and Security, *Submission 4*, pp, 10, 11, 12, 13-14.

Special intelligence operations – authorisation

Outline of issue

Schedule 3 to the Bill sets out the proposed scheme of special intelligence operations, implementing the Government's response to recommendation 28 of the Committee's 2013 report that such a scheme be established (subject to the inclusion of similar safeguards and accountability requirements as those applicable to controlled operations under Part IAB of the Crimes Act in relation to covert law enforcement operations).[66]

Proposed s 35C sets out a model of internal authorisation for special intelligence operations, under which an authorising officer (being the Director-General of Security or a Deputy Director-General of Security) may, on the application of an ASIO employee, grant an authority to conduct a special intelligence operation. An authority may only be granted if the relevant statutory criteria in s 35C are satisfied. These criteria require the authorising officer to be satisfied, on reasonable grounds, that:

- the operation will assist the Organisation in the performance of one or more special intelligence functions (defined by reference to the matters set out in ss 17(1)(a), (b), (e) and (f) of the ASIO Act);
- the circumstances are such as to justify the conduct of an operation;
- any unlawful conduct will be limited to the maximum extent consistent with an effective operation; and
- the operation will not involve conduct in the nature of entrapment; or conduct which will cause death, serious injury, or serious loss of or damage to property; or conduct which will involve the commission of a sexual offence.

The Committee has sought responses from the Department and ASIO to a suggestion that authorisation decisions should be made on an external basis. That is, a suggestion that special intelligence operations must be authorised by a person who is independent to ASIO, such as an issuing authority who may be a judicial officer or tribunal member appointed in a personal capacity. An alternative was identified as appointing the Attorney-General as an issuing authority.

66 Notwithstanding the Committee's 2013 recommendation to implement a scheme of special intelligence operations, some submitters and witnesses to the inquiry continued to argue that there is an insufficient policy or operational justification for doing so. The Department and ASIO have provided further comments in response to these remarks in Part 2 of this submission.

Submissions and evidence

Several submitters and witnesses who participated in the inquiry expressed support for an external authorisation model.[67] Proponents of this model appeared to be motivated primarily by a desire to increase confidence that the scheme will not be abused, by ensuring impartiality and accountability in the authorisation process. These submissions appeared to suggest – or in some instance presume – that internal authorisation is incompatible with this objective.

Some submitters and witnesses also pointed to the existence of Subdivision C of Part 1AB of the Crimes Act, which was said to lend support to an external authorisation model for special intelligence operations. Subdivision C provides for a 'nominated tribunal member' to determine applications to extend the duration of a controlled operation authority for a period beyond three months.

Departmental and ASIO comments

Preferred option –internal authorisation model

Consistent with the evidence of the Director-General of Security to the Committee on 15 August,[68] ASIO is of the view that the authorisation of special intelligence operations is necessarily, and exclusively, an internal function given the intrinsically operational nature of such decisions.

Decisions about the commencement, continuation and conduct of covert intelligence operations are highly sensitive and specialised matters. They require an extensive awareness and sophisticated understanding of the security environment, and a strong practical understanding of the way in which intelligence operations are conducted, in order to review and assess operational aspects of a proposed special intelligence operation, and ensure that any otherwise unlawful conduct would be limited to the maximum extent consistent with an effective operation. Such expertise is essential in making decisions about the commencement, continuation and conduct of operations in time critical and rapidly developing circumstances.

Internal decision-making on such matters is consistent with the statutory role of the Director-General of Security, under whose control the Organisation is placed by s 8(1) of the ASIO Act. The Director-General has an obligation to ensure that the work of ASIO is limited to what is necessary for the purpose of discharging its functions, and that ASIO is kept free from any influences or considerations that are not relevant to its functions. An external authorisation model would transfer primary decision making on a core operational matter to a person who is not responsible for the Organisation's performance of its functions, and who lacks the requisite understanding of the security environment and operational expertise to make informed and effective decisions on highly significant operations.

67 See footnote 2 above.

68 Proof Committee Hansard, 15 August 2014, p. 22.

For these reasons, authorisation decisions are unsuitable to be made on an external basis. It is noted that a comparable scheme in the US, under the *Attorney-General's Guidelines to the FBI on Undercover Operations*, also adopts an internal authorisation model, with a requirement that comparable operations are approved by designated senior officials within the FBI.

ASIO and the Department acknowledge, however, the importance of subjecting authorisation decisions to the independent oversight of the IGIS, in addition to the general oversight of the Attorney-General. Accordingly, some additional notification requirements could be included in the Bill, to ensure that the IGIS's statutory powers of oversight can be exercised in a timely manner in relation to special intelligence operations. These suggestions are detailed below.

The Department and ASIO also acknowledge that members of the Committee are interested in exploring alternative options to internal authorisation. To assist the Committee in undertaking this task, comments are provided on the options raised by some submitters to the inquiry, and explored with witnesses appearing at the Committee's public hearing on 18 August.

Comments on alternative models under consideration by the Committee

Alternative model (1): authorisation by an independent issuing authority

As mentioned above, several witnesses appearing before the Committee on 18 August were asked to comment on a possible external authorisation process involving an independently appointed issuing authority, similar to issuing authorities appointed for the purpose of Division 3 of Part III of the ASIO Act (questioning warrants and questioning and detention warrants).

ASIO does not support this option, for the reasons set out above in relation to the necessarily internal nature of decisions to authorise special intelligence operations. In addition, the appointment of multiple, external issuing authorities also creates a significant risk of inconsistency in decision making. Individual issuing authorities could conceivably place different degrees of weight on identical or substantially similar considerations relevant to the authorisation criteria, with the result that vastly different, and potentially inconsistent, authorisation decisions are made. In contrast, an internal authorisation model would facilitate consistency of decision-making in relation to the commencement, continuation and conduct of operations, since decisions would be made by the Director-General and Deputy Directors-General of Security, who would have visibility of all previous applications and decisions, and would further be informed by their awareness of the conduct of operations, and the broader activities being undertaken by the Organisation in the performance of its statutory functions, as a result of their office.

Another important consideration is that a special intelligence operation is a materially different undertaking to the coercive questioning of an individual under a questioning or questioning warrant, or a questioning and detention warrant, issued under Division 3 of Part III. It is appropriate that such differences are reflected in the respective authorisation

models applying to each scheme. Key distinguishing features of the questioning and questioning and detention warrant scheme include:

- Questioning under a Division 3 warrant is a specific activity or technique, as distinct from a special intelligence operation, which may comprise multiple activities or techniques. As such, issuing decisions in relation to Division 3 warrants are more focussed and contained.

- Questioning under a Division 3 warrant must be authorised for a specific purpose (being the collection of intelligence that is important to a terrorism offence) as distinct from the much broader purpose of the performance of one or more of the Organisation's statutory functions under s s17(a), (b), (e) or (f), pursuant to the proposed definition of a 'special intelligence function' for the purpose of the special intelligence operations scheme.

- Questioning warrants and questioning and detention warrants involve the exercise of highly intrusive powers, including the ability to compel responses to questions, and to deprive a person of liberty by detaining him or her. This is in contrast to special intelligence operations, which cannot be authorised in relation to conduct that would require ASIO to obtain a warrant, and which cannot authorise conduct that would cause death, serious injury, serious loss of or damage to property, the commission of a sexual offence, or the inducement of another person to commit an offence which that person would not otherwise have intended to commit.

It is similarly important to acknowledge that the adoption of external authorisation for the extension of controlled operations under Part IAB of the Crimes Act reflects the specific, law enforcement purpose to which controlled operations are directed. These operations are concerned with the investigation of serious criminal offences, including the collection of admissible evidence which may be used in a prosecution. As such, they are necessarily of a short-term nature. An extension of time beyond three months is therefore exceptional in this context, and this circumstance is duly reflected in the external authorisation model for extensions of time in Subdivision C of Part IAB. In contrast, special intelligence operations are concerned with the collection of security intelligence, including building an understanding of persons and organisations of security concern – including an understanding of changes or developments over time. To achieve this purpose, such operations must necessarily run for a sustained period of time.

Additionally, an external authorisation model may reduce the opportunity for the IGIS to conduct oversight of authorisation decisions, given that the oversight mandate conferred under the IGIS Act relates to relevant intelligence agencies. An external authorising officer, such as a judicial officer or tribunal member appointed in a personal capacity, would not be part of ASIO for the purposes of being subject to oversight in accordance with the IGIS Act.

Accordingly, the Department and ASIO submit that it is important, in assessing the appropriateness of any authorisation model, to distinguish between the general policy objective of accountability and the means by which this objective is given effect. It should

not be assumed that external authorisation is the sole means of doing so, or necessarily the best means.

Alternative model (2): authorisation by the Attorney-General

Some members of the Committee identified a possible alternative option to an authorisation model involving the appointment of independent issuing authorities. This was in the form of a Ministerial authorisation model analogous to the special powers warrants under Part 2 of Division III of the ASIO Act. Such a model would involve the designation of the Attorney-General as an issuing authority, who would determine applications made by the Director-General of Security.

Given the Attorney-General's overall responsibility for security matters, and consequent broad awareness of the security environment, this alternative may have fewer adverse operational impacts than decision making by an external issuing authority. However, the comments made above about the necessary degree of operational background and expertise to make authorisation decisions also apply to this proposal, although to a lesser extent than an independent issuing authority.

In addition, while the Attorney-General is an issuing authority for ASIO warrants (including special powers warrants under Division 2 of Part 3) there are inherent differences in what is being approved. Authorising an ASIO warrant requires the approval of a particular technique (which would otherwise be unlawful) such as a search to be used as part of an intelligence collection operation. In contrast, authorising an SIO will require a detailed appreciation of the broad and dynamic operational context in which a range of activities envisaged by the authority will be allowable. Such detailed appreciation is held within ASIO and it is the mandated responsibility of the Director-General of Security to consider in all his or her decisions on operational matters. This goes to the heart of operational judgment and, in the SIO context, will require the decision-maker to find (among other things) that in all the circumstances the SIO is justified, that unlawful conduct is limited to the maximum extent possible and it will assist the Organisation in the performance of the SIO functions. These are functions that should be the domain of the Director-General rather than a person external to ASIO.

Further, a Ministerial authorisation model would limit the opportunity for IGIS oversight of authorisation decisions, given that Ministerial decision making is not generally within the statutory oversight remit conferred by the IGIS Act.

Departmental and ASIO proposal

As noted above, the Department and ASIO support the inclusion of additional notification requirements in relation to the granting of a special intelligence operation authority, and the commission of certain conduct as part of a special intelligence operation.

Proposed s 35Q requires ASIO to provide six-monthly reports on special intelligence operations to the Attorney-General and the IGIS. These reports must address how the operation has assisted the Organisation in the performance of one or more special intelligence

functions. Proposed s 94(2A) will also require details to be included in ASIO's annual reports on the total numbers of applications made and authorisations provided in each reporting year.

The following additional notification requirements to the IGIS could be included in the Bill to enhance the IGIS's ability to undertake timely oversight of relevant activities:

- A new requirement to notify the IGIS when a special intelligence operation authority is granted, to provide the IGIS with the opportunity to conduct effective oversight from the commencement of an operation.

- A new requirement that ASIO advise the Attorney-General and the IGIS of any special intelligence operation where there is an intention for that operation to continue beyond six months. This would enable both the Attorney-General and the IGIS to raise any concerns, and to make decisions about the level of scrutiny to which it will be subject.

- An additional notification requirement in proposed s 35Q, requiring the Director-General to inform the Attorney-General and the IGIS, as part of six monthly reporting on operations, if any injury, loss or damage was caused to a person or property in the course of, or as a result of, the operation. This would enable the IGIS to undertake any relevant inquiries, and to consider making recommendations as to the payment of compensation as appropriate.

- If the Committee requires statutory assurance that oversight powers will be exercised in relation to special intelligence operations (in addition to the general oversight powers of the IGIS) a similar provision to s 15HS of the Crimes Act could potentially be included (relating to inspection of controlled operations records) requiring the IGIS to periodically inspect records relating to current special intelligence operations (for example, annually).

In addition, to provide further assurance of accountability and oversight, the power to approve a special intelligence operation could potentially be limited to the Director-General alone (including a person acting as Director-General), and not also invested in the Deputy Directors-General. (It is noted, however, that Deputy Directors-General are directly accountable to the Director-General.)

Special intelligence operations – other differences to controlled operations

Outline of issue

As noted in the Explanatory Memorandum to the Bill,[69] and in the Department and ASIO's evidence to the Committee, the proposed special intelligence operations regime is modelled on the provisions of Part IAB of the Crimes Act, which authorise and govern the conduct of controlled operations for law enforcement purposes.

The proposed regime of special intelligence operations is analogous to that of controlled operations in terms of its broad elements, including the adoption of an application-based authorisation process; the conferral of limited protections from legal liability on authorised participants; and the imposition of reporting and oversight arrangements in relation to authorised operations. However, it is important that these elements are implemented in a way that is adapted to the purpose of the relevant covert scheme (being intelligence collection in the case of special intelligence operations, and law enforcement investigations into serious criminal offences in the case of controlled operations). Accordingly, there are some necessary differences in the content and form of the individual provisions that give effect to the common, core components of each scheme.

The Committee has asked the Department and ASIO for further information about, and explanation of, the key differences between the respective schemes. This request was made further to the evidence of some submitters and witnesses that there should be either uniformity of, or a closer degree of alignment between, the particular provisions applying to each scheme, notwithstanding the discrete purposes to which they are directed.

Submissions and evidence

Several submitters and witnesses commented on differences between the proposed provisions in Schedule 3 to the Bill and those authorising and regulating controlled operations under Part 1AB of the Crimes Act. Some suggested that amendments should be made to the provisions of Schedule 3 to increase their degree of alignment, or in some instances uniformity, with corresponding provisions in Part 1AB. Some submissions appeared to be motivated by a preference that the respective schemes ought to be uniform or nearly uniform in their particular provisions, in addition to being consistent in their broad elements.

Areas of departure identified by external entities providing submissions or evidence to the Committee as: the definition of a 'special intelligence operation' compared to the definition of a 'controlled operation'; the duration of authorisations; the relevant authorising officers; the authorisation criteria; the nature of limited protections from civil liability; compensation and notification requirements in relation to the causation of property damage or personal injury; reporting, record keeping and oversight requirements; penalties and exemptions

69 Explanatory Memorandum, p. 976 at [463].

applied to disclosure offences; the express exclusion of certain types of activities; requirements for the variation of authorities; and the appointment of a principal officer with overall responsibility for an authorised operation.

Some submitters also suggested that the proposed special intelligence operations scheme should be subject to additional limitations, which do not have an equivalent in the controlled operations provisions in the Crimes Act. These included suggestions for:

- a prohibition on operations that do not include any ASIO employees as participants;[70]
- further restrictions to the authorisation criteria, to exclude activities that would cause injury of any kind, whether minor or serious;[71]
- a 'last resort' styled requirement in the authorisation criteria, which would require the authorising officer to be satisfied, on reasonable grounds, that all other methods of collecting the relevant intelligence have been exhausted;[72] and
- limitations on the matters which may be covered by evidentiary certificates in relation to the granting of special intelligence operation authorities in proposed s 35R.[73]

Departmental and ASIO comments

The provisions of Part 1AB of the Crimes Act were given careful consideration in the design of the proposed special intelligence operations scheme in Schedule 3 to the Bill. All proposed instances of departure are directed to accommodating the different purposes to which special intelligence operations and controlled operations are directed, and ensuring that the requirements applied to each regime are adapted to achieving its particular purpose.

A summary table of key similarities and differences between controlled operations and special intelligence operations is provided at **Attachment 2** Commentary on the major areas of difference is provided below (other than in relation to authorising officers, which has been addressed above). This analysis is prefaced by some general remarks on the guiding principles taken to the design of the proposed special intelligence operations scheme.

Guiding principle in the design of the special intelligence operation scheme

The proposed special intelligence operations scheme is directed to covert operation for the purpose of collecting intelligence relevant to security, consistent with ASIO's statutory functions. As such, special intelligence operations will be directed to obtaining intelligence, typically over a period of time, so as to understand the activities and plans of persons or groups of security concern by means of obtaining close access to them in a way that is not presently possible due to the potential for criminal or civil liability to attach to such activities.

70 Law Council of Australia, *Submission 13*, pp. 7, 33.

71 Blueprint for Free Speech, *Submission 22*, p. 7.

72 ibid, p. 6.

73 Law Council of Australia, *Submission 13*, p, 40.

In contrast, controlled operations are directed to law enforcement purposes – namely, the investigation of serious criminal offences – with a focus on obtaining admissible evidence able to be used in prosecutions for such offences.

Accordingly, the Department and ASIO are concerned to ensure that the guiding principle in designing the special intelligence operations scheme – and in assessing the appropriateness of its individual provisions – is that of its suitability for its specific purpose of collecting security intelligence, which seeks to predict future security relevant activity, in accordance with ASIO's statutory functions.

While consistency with the broad structure and particular provisions of Part 1AB of the Crimes Act is a relevant consideration, it is important that this assessment is not reduced to a perfunctory exercise in identifying differences between the provisions in the Bill and those in Part 1AB of the Crimes Act in isolation of meaningful regard to the purpose to which each scheme is directed. It is important that uniformity is not perceived to be an end in itself.

Definition of 'special intelligence operation' and 'special intelligence function'

A special intelligence operation is proposed to be defined in s 4 of the ASIO Act as an operation:

(a) in relation to which a special intelligence operation authority has been granted (under proposed s 35C); and

(b) that is carried out for a purpose relevant to the performance of one or more special intelligence functions (defined as a function of the Organisation under paragraph 17(a), (b), (e) or (f) of the ASIO Act); and

(c) that may involve an ASIO employee or an ASIO affiliate in special intelligence conduct (defined as that which would, but for the limited immunity in proposed s 35K, be subject to criminal or civil liability).

A special intelligence function for the purpose of paragraph (b) is proposed to be defined in s 4 of the ASIO Act as a function of the Organisation under paragraph 17(a), (b), (e) or (f) of the ASIO Act.

This is analogous to the formulation in the definition of a controlled operation in s 15GD(1) of the Crimes Act, to the extent that paragraphs (a)-(c) apply to conduct engaged in for specified purposes, which may otherwise constitute an offence under a law of the Commonwealth or a State or Territory. Subsection 15GD(1) defines a controlled operation as an operation that:

(a) involves the participation of law enforcement officers; and

(b) is carried out for the purpose of obtaining evidence that may lead to the prosecution of a person for a serious Commonwealth offence, or a serious State offence that has a federal aspect; and

(c) may involve a law enforcement officer or other person in conduct that would, apart from s 15HA (limited immunity from criminal liability), constitute a Commonwealth office or an offence under a law of a State or Territory.

However, some submitters and witnesses have commented on three differences between these definitions, and have suggested a closer degree of alignment with the Crimes Act in these areas. These differences are discussed below.

Difference 1: the participation of ASIO employees is not mandated

First, s 15GD(1)(a) requires the participation of law enforcement officers in a controlled operation, whereas the proposed definition of a special intelligence operation does not mandate the participation of ASIO employees, with the result that an operation could be comprised entirely of ASIO affiliates (being a person performing functions or services for the Organisation under a contract, agreement or arrangement). It was suggested that the definition should mandate the participation of ASIO employees in all operations.[74]

It would not be appropriate to mandate the participation of ASIO employees in all special intelligence operations. The inclusion of s 15GD(1)(a) in the Crimes Act reflects the law enforcement purpose to which the controlled operations regime is directed – as set out in s 15GD(1)(b) (evidence collection in connection with a prosecution for a serious offence). The mandatory involvement of law enforcement officers reflects their responsibility for investigating criminal offences and their expertise in the collection of admissible evidence.

In contrast, special intelligence operations are for the purpose of obtaining, correlating, evaluating and communicating intelligence relevant to security, and for cooperating and assisting other bodies in s 19A in the performance of their functions (being ASIS, ASD, AGO and a law enforcement agency), consistent with the proposed definition of special intelligence function, incorporating ss 17(a), (b), (e) and (f) of the ASIO Act. It is appropriate that special intelligence operations are flexible and adaptable, and there is the ability to utilise those persons who are best placed to gather intelligence to perform these functions, irrespective of the technical nature of their relationship with ASIO (for example, as an ASIO employee or an ASIO affiliate).

The selection of participants in special intelligence operations will therefore depend on all of the circumstances of individual operations. There may be circumstances in which it is appropriate that the participants in a special intelligence operation are only ASIO affiliates or other persons, just as there may be circumstances in which participants are exclusively ASIO employees, or a combination of ASIO employees, ASIO affiliates and other persons.

There are a number of safeguards to the participation of persons other than ASIO employees in special intelligence operations. Proposed s 35B requires that an application for an authority (which will set out the proposed participants and conduct to be authorised) must be made by an ASIO employee.

Proposed s 35C provides that the authorising officer must be satisfied, on reasonable grounds, that the statutory authorisation criteria are satisfied, including satisfaction that the operation would assist in the performance of the Organisation's functions, and that the circumstances

74 Law Council of Australia, *Submission 13*, p. 33; Proof Committee Hansard, 18 August 2014, p. 5.

are such as to justify the conduct of the operation. This includes consideration of proposed participants and the particular conduct in which they are authorised to engage, which is to be recorded in an authority under proposed s 35D.

The authorising officer may impose such conditions on an authority as he or she considers appropriate (which can include limitations on certain conduct by certain participants such as non-ASIO employees). The authorising officer also has discretion to cancel an authority at any time, for any reason (proposed s 35G) and to vary an authority at any time, on application of an ASIO employee or on his or her own initiative (proposed s 35F), which could include amending an authority in relation to certain participants, such as to add or remove them or vary the conduct in which they are authorised to engage.

Difference 2: no limitation to 'serious' security matters

Some submitters and witnesses suggested that, as s 15GD(1)(b) of the Crimes Act limits controlled operations to the purpose of investigating a 'serious offence', consideration should be given to limiting special intelligence operations to security matters of a 'serious' kind, or circumstances which are "sufficiently serious" as to justify the conduct of a special intelligence operation.[75] (Paragraph (b) of the proposed definition of a 'special intelligence operation' refers to a purpose relevant to the performance of one or more 'special intelligence functions', defined by reference to some, but not all, of the statutory functions of the Organisation under s 17 of the ASIO Act).

The express confinement of the special intelligence operations scheme to matters or circumstances designated as 'serious' is not necessary, because the definition of security in s 4 of the ASIO Act already performs this limiting function. The matters within this term are inherently serious – concerning the protection of Australians from espionage, sabotage, politically motivated violence, promotion of communal violence, attacks on Australia's defence system, acts of foreign interference, the protection of Australia's territorial and border integrity from serious threats, and the carrying out of Australia's responsibility to foreign countries in relation to such matters.

In contrast, the criminal law covers a broad spectrum of wrongdoing, with the result that it is necessary to limit controlled operations to those offences which are considered to be sufficiently serious in terms of their subject matter and penalties to justify undertaking covert law enforcement activities (consistent with the definition of 'serious offence' in s 15GE).

Difference 3: no sub-category of 'major' special intelligence operations

Subsection 15GD(2) of the Crimes Act makes further provision for a sub-category of 'major controlled operations' (being those which are likely to involve the infiltration of a criminal group by one or more undercover law enforcement officers for more than seven days, or continue for more than three months, or be directed to suspected criminal activity that includes a threat to human life). This distinction is material to the levels of authorisation

75 Law Council of Australia, *Submission 13*, p. 33.

required for controlled operations under s 15GF of the Crimes Act. 'Major controlled operations' may only be authorised by the most senior law enforcement officials (such as the Commissioner of Police or a Deputy Commissioner) whereas 'ordinary' controlled operations can be authorised by other senior executive level employees within the relevant law enforcement agency who have been authorised in writing by their agency head.

Consideration was given to creating a special category of 'major' special intelligence operations, but it is considered preferable to require all authorisations to be given by the Director-General of Security or a Deputy Director-General. This applies the higher of the two thresholds in the Crimes Act. Reserving the power to grant authorisations to the most senior officers within ASIO is consistent with the need to ensure that the authorising officer possesses a detailed understanding and awareness of the security environment, and that appropriate rigour is applied to decision-making, including within time critical and dynamic operational circumstances.

Duration of authorisations

A controlled operation may run for a maximum period of 24 months, which must be approved in three-month increments. Authorisations for up to three months may be granted on an internal basis by a designated senior official within a law enforcement agency. (This includes extensions of an initial authority, where the total duration of the operation would be no longer than three months.) Extensions that would result in a total duration of more than three months must be authorised independently by a nominated member of the Administrative Appeals Tribunal (under Subdivision C of Part IAB).

In contrast, special intelligence operations are proposed to have a maximum duration of 12 months under proposed s 35D(1)(d). If an authority is granted for an operation with a duration of less than 12 months, proposed s 35F(5) provides that an authorising officer can vary the duration of the operation, provided that the operation does not exceed 12 months in total. Some submitters and witnesses to the inquiry have questioned the need for a 12 month period, and have suggested that a shorter duration such as six months would improve accountability.

A total duration of 12 months is appropriate for special intelligence operations. This reflects the longer-term nature of intelligence operations compared to law enforcement operations. As reflected in the operational examples provided to the Committee in private session, intelligence operations are aimed at obtaining information over a period of time, so as to build an understanding of the activities and plans of persons or groups of security concern. As such activities may change or develop over time, the capacity to collect intelligence over a sustained period is essential to ASIO's ability to perform its statutory functions.

A 12-month maximum duration therefore represents a balance between the operational need for covert operations to be conducted over a longer period of time, and ensuring appropriate accountability and oversight, as a new authority must be sought and obtained if an operation is to continue beyond 12 months. An authorising officer may also cancel an authority at any time and for any reason. In contrast to covert intelligence operations, covert law enforcement

operations are generally of a shorter duration given their focus on the investigation of suspected serious criminal offences, including the collection of admissible evidence for the prosecution of such offences.

Authorisation criteria

The authorisation criteria for special intelligence operations in proposed s 35C(2) are largely the same as those for controlled operations in s 15GI of the Crimes Act. The criteria for both schemes require the authorising officer to be satisfied, on reasonable grounds, of the following matters:

- The relevant circumstances exist. (In the case of special intelligence operations, this is that the proposed operation will assist the Organisation in the performance of one or more special intelligence functions. In the case of controlled operations, this is relevantly that a serious offence has been, is being, or is likely to be committed.)
- The relevant circumstances are such as to justify the conduct of the proposed operation.
- Any unlawful conduct will be limited to the maximum extent possible, consistent with conducting an effective operation.
- The operation will not be conducted in such a way that a person is likely to be induced to commit an offence that the person would not otherwise have intended to commit.
- The conduct involved in the operation will not cause the death of or serious injury to another person, involve the commission of a sexual offence, or result in significant loss of, or serious damage to, property.

The authorisation criteria for controlled operations contain two additional matters, which some submitters and witnesses to the inquiry suggested should be applied to the proposed special intelligence operation scheme.[76] These are:

- a requirement that the proposed conduct will be capable of being accounted for in a way that will satisfy the relevant reporting requirements under Division 4 of Part IAB to be complied with: s 15GI(2)(e); and
- a requirement that any conduct involved in the operation will not seriously endanger the health or safety of any person: s 15(2)(g)(i).

The first of these requirements has not been included in proposed s 35C because the special intelligence operations scheme does not include a dedicated independent oversight and reporting role, or obligations to maintain a central register of authorisations, as prescribed by

76 For completeness, it is noted that three other authorisation criteria in s 15GI(2) of the Crimes Act have not been reproduced in Schedule 3 to the Bill because they are specific to law enforcement operations. These relate to: controlled operations in connection with law enforcement integrity testing; the distinction between roles of law enforcement and civilian participants in operations; and the control of illicit goods involved in an operation: ss 15GI(2)(a)(ii), (d) and (h).

Division 4 of Part 1AB of the Crimes Act. (As noted below, this reflects that controlled operations are undertaken by participants from multiple law enforcement agencies, and that the Ombudsman's general jurisdiction and powers required supplementation to accommodate this. In contrast, the IGIS's general statutory powers are adequate to enable the oversight of special intelligence operations.)

In contrast, the reporting requirements applicable to special intelligence operations in proposed s 35Q are capable of being satisfied in all cases, given that they involve reporting to the Attorney-General and the IGIS on a six-monthly basis about operations that are in progress. (These observations would apply equally to the proposed additional notification requirements detailed above.) Accordingly, there is no benefit apparent in specifically requiring the authorising officer to be satisfied that these requirements can be met in individual applications.

The second of the suggested additional requirements listed above (concerning the exclusion of conduct that will not seriously endanger health or safety) is not considered appropriate for inclusion in proposed s 35C because it is inconsistent with the nature and purpose of intelligence operations. It may be necessary, in order to collect vital security intelligence, for authorised participants to engage in activities that place themselves at risk, mitigated by planning, training and preparation. Replicating s 15(2)(g)(i) of the Crimes Act in Schedule 3 to the Bill may therefore significantly limit the effectiveness of any special intelligence operations scheme in obtaining critical intelligence which can only be gained from close access to persons or organisations of security concern – for example, the collection of intelligence on terrorist organisations.

Protection from liability

Both proposed s 35K of the ASIO Act and Division 3 of Part IAB of the Crimes Act provide limited protection from legal liability to participants in special intelligence operations and controlled operations. Both sets of provisions expressly require that the conduct must have been undertaken in accordance with an authority; and that it did not involve the causation of death or serious injury, the commission of a sexual offence, serious loss of, or damage to, property, or conduct in the nature of 'entrapment'. However, there are two main differences in these protections, outlined below.

Civil liability

Proposed s 35K provides participants in a special intelligence operation with a limited immunity from criminal and civil liability in relation to special intelligence conduct undertaken in accordance with an authorisation. In contrast, while s 15HA of the Crimes Act confers an immunity from criminal liability, s 15HB only imposes an obligation on the Commonwealth to indemnify participants in controlled operations from civil liability, with the result that civil proceedings can still be commenced in relation to conduct authorised under a controlled operation.

Immunity from civil liability is necessary to achieve the purpose of the special intelligence operations scheme to provide participants with appropriate legal protections in a manner that does not expose a covert intelligence operation to detection. This includes preventing the exposure of methodologies and capabilities being employed, and the identities of authorised participants. A limited immunity from civil liability is the best way of managing these issues. Were civil matters brought before the courts for consideration, it would necessarily risk the disclosure of highly sensitive information, or result in the Commonwealth being unable to bring relevant information to the court's attention without prejudicing national security interests.

The approach of conferring an immunity, rather than an indemnity, is consistent with the immunity applied to staff members and agents of Intelligence Services Act agencies, in accordance with s 14 of that Act, which was found acceptable to the Parliament in 2001.

Conditions of protection from liability

Sections 15HA and 15HB additionally require 'civilian participants' in operations to have acted in accordance with the instructions of a law enforcement officer. Some submitters suggested that an equivalent condition should be inserted for ASIO affiliates or other persons who are not ASIO employees, which would require these persons to have acted in accordance with the instructions of an ASIO employee.[77]

An additional condition of protection, requiring non-ASIO employees to have acted in accordance with the instructions of an ASIO employee, is not considered to be necessary or appropriate. The involvement of non-ASIO employees in special intelligence operations is not sufficiently analogous to the involvement of civilian participants in controlled operations who are obtaining admissible evidence of serious criminal offences, including for the purposes of prosecution in open court, to justify such a condition. As noted above, there may be circumstances in which an operation does not involve any ASIO employees as participants.

In addition, appropriate safeguards on the scope of the immunity are found in the requirements in proposed s 35D, that the authority must particularise individual participants and the conduct in which they are authorised to engage, and any such additional conditions the authorising officer has decided to impose on an operation under proposed s 35C. Any person who acts outside the limits of their authority will not be subject to the immunity in proposed s 35K in respect of that conduct.

Compensation and notification requirements

Section 15HF of the Crimes Act imposes an obligation on the Commonwealth to compensate persons who suffer loss or serious damage to property, or personal injury, as a result of a controlled operation. In addition s 15HG imposes an obligation to notify property owners of

77 Law Council of Australia, *Submission 13*, p. 35.

any serious loss or damage, and to notify persons who are injured that the injury occurred in the course of or as a direct result of a controlled operation.

Contrary to the preferences of some submitters and witnesses to the inquiry, the proposed special intelligence operations regime does not include comparable provisions to those in ss 15HF and 15HG of the Crimes Act. This difference is necessary to take account of the absolute imperative to maintain the covert nature of special intelligence operations until they are, at the very least, complete. Unlike controlled operations (which are conducted for the purpose of gathering admissible evidence of serious criminal offences, including for the purposes of prosecution in open court) the intelligence collected as part of a special intelligence operation is collected solely for the purposes in s 17(a), (b), (e) and (f) of the ASIO Act, and not for the purpose of ultimate disclosure in any other way. As such, the risks to the operation associated with disclosure as a result of compensation and notification requirements are greater in relation to special intelligence operations.

Rather than prescribing statutory compensation or third party notification requirements, the IGIS may investigate operations involving the causation of loss or damage, and may make recommendations as to any action considered appropriate. This may include whether the person should be notified or compensated. The Department and ASIO note the submission of the IGIS, which suggested that reports made under proposed s 35Q could address whether loss, damage or injury was caused in the course of a special intelligence operation. As noted above, this suggestion is supported.

Reporting, oversight and record keeping requirements

Division 4 of Part 1AB of the Crimes Act establishes a detailed reporting, oversight and record keeping scheme for controlled operations. This includes specific powers of inspection, inquiry and annual reporting on controlled operations by the Ombudsman, together with Ministerial reporting requirements by relevant law enforcement agencies, and the maintenance of general registers of applications and authorities by relevant law enforcement agencies.

In contrast, proposed s 35Q of the ASIO Act requires the Director-General to provide six-monthly reports to the Attorney-General and the IGIS on operations in progress. These reports must address how the operation has assisted the Organisation in the performance of one or more special intelligence functions. The Organisation must also, under proposed s 94(2A) include in its annual reports the total number of applications made and authorities granted in the relevant reporting year. Authorising officers are also required to issue authorisations and variations (or records of urgent authorisations and variations) in writing, in accordance with proposed ss 35C and 35F.

Given the extensive general oversight jurisdiction of the IGIS, and the fact that special intelligence operations are to be conducted by ASIO alone, a detailed regime in the nature of that in Division 4 of Part IAB of the Crimes Act is not required. The arrangements for controlled operations are designed to reflect that such operations will involve participants from multiple law enforcement agencies as well as civilians. As such, an extension of the

Ombudsman's general oversight jurisdiction was necessary. Express reporting and record-keeping obligations are needed to ensure that there is clarity and coordination in relation to record keeping arrangements on the part of multiple, participating law enforcement agencies. As noted above, the Department and ASIO support the IGIS's proposal to notify her when a special intelligence operation is granted, and report on any loss, damage or injury caused by the conduct of a special intelligence operation, which would further enhance the IGIS's ability to conduct oversight.

Disclosure offences – penalties and exemptions

Part IAB of the Crimes Act contains offences in relation to the intentional disclosure of information relating to a controlled operation, where the person was reckless as to the circumstance that the information related to a controlled operation. These offences are a 'basic offence' in s 15HK (subject to a maximum penalty of two years' imprisonment) and an 'aggravated offence' in s 15HL (subject to a maximum penalty of 10 years' imprisonment). The aggravating elements in the second offence are that:

- the person intended the disclosure should endanger the health or safety of another person, or prejudice the effective conduct of a controlled operation; or
- the disclosure of the information will have the effect of one of the above.

These offences are subject to exceptions in relation to disclosures that are made:

- to the Ombudsman or the Integrity Commissioner in relation to corruption or misconduct, in good faith;
- in connection with the administration or execution of the controlled operations scheme;
- for the purpose of legal proceedings arising out of or otherwise related to the controlled operations scheme, or any report of such proceedings;
- for the purpose of obtaining legal advice in relation to the controlled operation; or
- in accordance with any requirement imposed by law; or
- in connection with the performance of functions or duties, or the exercise of powers, of a law enforcement agency.

The elements of the offences in proposed s 35P are identical to those in ss 15HK and 15HL, however there are three differences in other respects, which are discussed presently.

<u>Difference (1) in relation to offences – penalties</u>

The maximum penalty applying to the basic offence in proposed s 35P(1) is five years' imprisonment, in contrast to two years' in relation to s 15HK.

As noted in the Explanatory Memorandum to the Bill, this penalty is necessary to maintain parity with other penalties applying to disclosure offences in the ASIO Act, such as s 34ZS

(unauthorised disclosure of information relating to questioning and questioning and detention warrants) recognising the particularly significant harm or risk of harm that the compromise of such information can cause.[78]

Difference (2) in relation to offences – absence of a legal advice exception

Proposed s 35P contains exemptions for legal proceedings and reports of legal proceedings, but not the provision of legal advice. This was not included on the basis that special intelligence operations are entirely internal to ASIO, and therefore it was not considered necessary for persons who are not participants in an operation to seek advice that is not in connection with legal proceedings (noting that legal proceedings are the subject of a separate exception).

However, it would be possible to consider the inclusion of an express exemption for legal advice in light of the evidence of some submitters and witnesses to the inquiry which expressed concerns that non-participants may be exposed to legal liability for seeking legal advice about suspected activities of ASIO in relation to them.[79] A specific exemption could provide an important assurance to such persons.

Difference (3) in relation to offences – absence of an exception for disclosures to the IGIS

Proposed s 35P does not contain an equivalent exemption to that in ss 15HK(3) and 15HL(3) of the Crimes Act in relation to good faith disclosures to the Ombudsman or Law Enforcement Integrity Commissioner in relation to suspected misconduct in relation to controlled operations.

An equivalent exemption, if included in s 35P, could apply to disclosures to the IGIS in relation to the conduct of a special intelligence operation. Such an exemption was not considered necessary because the regime in the *Public Interest Disclosure Act 2013* (PID Act), together with immunities in the IGIS Act in relation to the conduct of inquiries, and the exercise of prosecutorial discretion, were considered to provide adequate protection in these circumstances.

However, on further consideration of the evidence of the IGIS to the inquiry, it is acknowledged that an express exception would be desirable to provide certainty that disclosures to the IGIS are not subject to the offences. In particular, a specific exemption to the offences could apply to disclosures made to the IGIS by persons other than public officials for the purpose of the PID Act (and who are therefore not subject to the protections of that Act); and disclosures made by staff of the IGIS to the IGIS or other staff members in that Office for the purpose of performing inspection (as distinct from inquiry) functions under the IGIS Act.

78 Explanatory Memorandum, p. 113 at [565].

79 Law Council of Australia, *Submission 13*, p. 43.

Activities excluded from special intelligence operations

Both s 15HI of the Crimes Act and proposed s 35L of the ASIO Act expressly exclude conduct which is subject to a separate form of statutory authorisation, such as a warrant. This makes clear that controlled operations and special intelligence operations cannot be used to substitute or circumvent existing authorisation requirements for the exercise of law enforcement or intelligence collection powers.

In the case of controlled operations, s 15HI of the Crimes Act excludes actions that are, or could have been, authorised under a Commonwealth or State or Territory law conferring powers of criminal investigation – for example, powers in relation to arrest, detention, person searches, entry to premises, seizure of property, forensic procedure, surveillance, telecommunications interception, identification procedures, and assumed identities.

Proposed s 35L of the ASIO Act provides that special intelligence operations authorities cannot be used to authorise actions that would otherwise require authorisation under a warrant under the ASIO Act, or a warrant under Part 2-2 of the *Telecommunications (Interception and Access) Act 1979* (TIA Act) (ASIO telecommunication interception warrants), or an authorisation under Division 3 of Part 4-1 of the TIA (permitted access to telecommunications data by ASIO).

However, some submitters and witnesses to the inquiry suggested that the exclusions in proposed s 35L are, in their view, unclear. It was suggested that it is unclear whether proposed s 35L would enable a person to rely on an immunity under s 35K in respect of conduct that was in breach of a warrant – for example, because the person exceeded his or her authorisation under the warrant in the course of executing it, or contravened a statutory prohibition on the conduct able to be authorised under a warrant.[80]

The Department and ASIO consider that this result is not open as a matter of statutory interpretation, but acknowledge that consideration could be given to making this clearer either by introducing a provision or a note in the Bill expressly stating the relationship between proposed ss 35K and 35L, or by setting this out in the Explanatory Memorandum.

In broad terms, the immunity in proposed s 35K attaches to conduct that is in accordance with a special intelligence operation authority. Proposed section 35L makes clear that an act which would require a warrant under the ASIO Act or Part 2-2 of the TIA Act, or an authorisation under Division 3 of Part 4-1 of the TIA Act, cannot be the subject of a special intelligence operation authority.[81] Accordingly, the immunity in proposed s 35K cannot apply to persons who engage in conduct that would, in order to be lawful, require authorisation under a warrant (including compliance with any warrant conditions or limitations).

---

80 Law Council of Australia, *Submission 13*, p. 35.

81 This is achieved by the phrase "this Division does not allow the Organisation to do the act without the warrant" or "this Division does not allow the Organisation to obtain the information otherwise than in accordance with" the TIA. (Hence s 35D is read subject to s 35L).

Variation of authority

Subdivisions B and C of Division 2, Part 1AB of the Crimes Act sets out detailed requirements for variation applications and decisions in relation to controlled operation authorities. These prescribe: the matters to which a variation may relate; the ability of an authorising officer to make a variation at any time (either on application or on his or her own initiative); the contents of variation applications; the requirements for the granting of a variation; the required manner and form of a variation; and a limitation on variations involving an extension of duration, so that the total period of effect cannot exceed the maximum of 24 months. In particular, ss 15GQ(2) and 15GV(2) prescribe the matters in respect of which the relevant authorising officer or nominated tribunal member (in the case of operations exceeding three months) must be satisfied, on reasonable grounds. These replicate the original authorisation criteria in full (as discussed above).

In contrast, proposed s 35F is less prescriptive, relevantly providing that an authorising officer may make a variation at any time and for any reason: proposed s 35F(1) The original authorisation criteria in s 35C are not reproduced in full in s 35F. Rather, proposed s 35F(4) provides that a variation must not be granted unless the authorising officer is satisfied, on reasonable grounds, that the operation as varied will assist the Organisation in the performance of one or more statutory functions; and the authorising officer considers it appropriate to vary the authority. Variation involving an extension of time cannot extend the total period of effect of an operation beyond 12 months.

As noted in the Explanatory Memorandum, the absence of a prescriptive list of matters which must be addressed in a variation application is in recognition of the internal approval process applied to variations, which is considered necessary to ensure operational flexibility and effectiveness in the conduct of special intelligence operations.[82] In addition, it is implicit in the proposed definition of a 'special intelligence operation authority' in s 4 (being an authority which is granted under s 35C) that an authorisation as varied must continue to satisfy all of the criteria in s 35C, otherwise it would no longer be capable of answering the definition.

Nonetheless, some submitters and witnesses to the inquiry have suggested that the variation criteria in proposed s 34F(4) are inadequate because there is no requirement that the authorising officer reconsiders the full range of authorisation criteria in proposed s 35C(2).[83] It has further been argued that proposed s 35(4) could allow variation of special intelligence operation authorities in a way that significantly expands their scope, without requiring the authorising officer to specifically consider any of the other safeguards in s 35C (such as limiting unlawful conduct to the extent possible, and the prohibition on conduct likely to cause death, serious injury, serious loss or damage to property, the commission of a sexual offence, or conduct in the nature of 'entrapment'). It was suggested that special intelligence operations should not be subject to variation, or at least significant variation, unless the

82 Explanatory Memorandum, p. 106.

83 Law Council of Australia, *Submission 13*, p. 36.

authorising officer is satisfied, on reasonable grounds, that all of the authorising criteria in proposed s 35C continue to apply to the operation as varied.[84]

While the Department and ASIO do not consider that the above interpretation advanced by some submitters is correct as a matter of law for the reasons set out above, it would be possible to insert an express provision in s 35F or commentary in the Explanatory Memorandum for the avoidance of doubt. This could be to the effect that all of the authorisation criteria in proposed s 35C must continue to be satisfied by the operation as varied under proposed s 35L.

Appointment of a 'principal officer' with overall responsibility for an operation

Part IAB of the Crimes Act requires the appointment of a 'principal officer' in relation to a controlled operation, who is a law enforcement officer with overall responsibility for the conduct of that operation.

Schedule 3 does not contain an equivalent provision on the basis that special intelligence operations are internal to ASIO. Unlike controlled operations, special intelligence will not typically involve participants from multiple agencies. As such, responsibility for the conduct of a special intelligence operation appropriately rests with the relevant authorising officer (being the Director-General of Security or a Deputy Director-General) who has discretion to cancel or vary an authority at any time, on application or on his or her own initiative. The Director-General's responsibility for the control of the Organisation under s 8(1) of the ASIO Act is also considered adequate to ensure that the lines of control are clear.

In addition, if appropriate in particular operations, individual special intelligence operation authorities could impose obligations on persons to follow the directions or command of other participants in an operation. An ASIO employee or an ASIO affiliate may have additional obligations to adhere to directions of responsible persons by reason of their employment (in the case of an ASIO employee) or their contract, agreement or other arrangement for the performance of functions or services for the Organisation (in the case of an ASIO affiliate).

Suggested additional / alternative requirements to those in Part 1AB of the Crimes Act

Some submitters and witnesses to the inquiry suggested that the special intelligence operations regime should, if enacted, be subject to additional requirements to those applied in Part 1AB of the Crimes Act. These suggestions appear to be motivated by either a disagreement with the inclusion of some provisions of Part IAB of the Crimes Act, or a desire to minimise the potential impacts of special intelligence operations on third parties.

<u>Proposed s 35R – evidentiary certificates</u>

One submitter to the inquiry questioned the need for proposed s 35R, as it operates in combination with proposed s 35A.[85] Proposed s 35A provides for a limited modification of

84 ibid.

85 Law Council of Australia, *Submission 13*, p. 40.

the rules of evidence in relation to information obtained as part of a special intelligence operation in two respects. These are, first, a provision that a court may not exclude evidence solely because it was obtained as a result of a person's engagement in a special intelligence operation (provided that the person was appropriately authorised and acted in accordance with his or her authority). Secondly, an authorising officer may issue a prima facie evidentiary certificate under proposed s 35R in relation to any factual matter relevant to the granting of an authority.

The need for the evidentiary certificate scheme in proposed s 35R was questioned. It was suggested that such certificates should not be able to be issued to establish prima facie evidence of the elements of any criminal offence. It was also suggested that certificates should be expressly limited to matters of a technical nature only.[86] These proposed additional limitations are not included in the corresponding provisions of the Crimes Act in relation to controlled operations. (These are ss 15GA and 15HZ. However the evidentiary certificate provision in s 15HZ contains a limitation of a different kind, which excludes the certificates from being used as prima facie evidence in criminal or disciplinary proceedings against a law enforcement officer, reflecting that controlled operations can be used in combination with law enforcement integrity testing.)

Section 35R is designed to protect decisions to grant authorities, and not the intelligence that is obtained pursuant to an operation, or the question of whether or not a participant acted in accordance with their authorisation. (That is, the certificates are limited to the factual basis on which the authorising officer was satisfied the relevant authorisation criteria in s 35C were met.) As such, s 35R(1) expressly limits the matters which may be the subject of a certificate to "facts … with respect to the *granting of a special intelligence operation authority*" (emphasis added). As such, the suggested additional limitations are not necessary because the provision does not cover them in any event.

Additional requirements – authorisation criteria

Some submitters and witnesses proposed additional requirements in the authorisation criteria in proposed s 35C, including:

- an authorisation threshold in the nature of a 'last resort' requirement, whereby it must be established that all other means of collecting the relevant intelligence have been exhausted;[87] and

- a requirement that the authorising officer must be satisfied, on reasonable grounds, that the proposed operation will not cause any kind of injury to any person (not merely serious injury).[88]

86 ibid.

87 Blueprint for Free Speech, *Submission 22*, p, 6.

88 ibid, p. 7.

The Department and ASIO do not support the inclusion of these additional measures on the basis that they would unduly limit the effectiveness of special intelligence operations.

An authorisation threshold in the nature of a 'last resort' could prevent some operations from being commenced if there are other means available of gathering the relevant intelligence, but which are less effective and may involve a greater risk of detection. In other circumstances, a last resort threshold may be meaningless because close access to a target (such as a terrorist organisation) may be the only means of obtaining the intelligence sought, and such close access could not be obtained because it would otherwise constitute a criminal offence (such as associating with a terrorist organisation, or receiving training from a terrorist organisation).

Accordingly, considerations of this kind are appropriately managed by the requirement in proposed s 35C(2), in particular that the special intelligence operation will assist in the Organisation's performance of one or more special intelligence functions, the circumstances are such to justify a special intelligence operation, any unlawful conduct will be limited to the maximum extent consistent with conducting an efficient operation, and the operation will not involve engagement in certain types of conduct (namely, conduct constituting entrapment, or serious offences against the person or property).

In addition, the exclusion from the special intelligence operations scheme of conduct causing minor injury could frustrate the operation of the scheme. It may be necessary for participants to engage in conduct causing minor injury either as part of infiltrating a target, or to protect themselves. The reference in proposed s 35C(2)(e)(i) to 'serious' injury is consistent with the authorisation for controlled operations in s 15GI(2)(g)(ii).

Special intelligence operations – disclosure offences – proposed s 35P

Possible further exceptions – disclosures to the IGIS, and obtaining legal advice

As noted in the above analysis of differences between the proposed provisions on special intelligence operations and those in relation to controlled operations, the Department and ASIO support the inclusion of an additional exemption to the offences in s 35P, which would make clear that the offences do not apply to the disclosure of matters to the IGIS in circumstances in which the protections under the PID Act do not apply. This includes: disclosures made as part of complaints made to the IGIS by persons other than public officials; the disclosure of information to the IGIS in the course of inspections or pro-active disclosure (as distinct from inquiries conducted under the IGIS Act); and the communication of information by IGIS staff to the IGIS and other staff within the Office of the IGIS for the purpose of carrying out functions under the IGIS Act.

For the reasons set out above, a further exception could feasibly be included for legal advice, in addition to legal proceedings, in relation to the special intelligence operations regime. This could provide a greater degree of reassurance to persons who may wish to consult a lawyer to better understand any legal rights or obligations that may apply to them, but not necessarily for the purpose of commencing legal proceedings.

Potential application to journalists

The Department and ASIO refer to the Department's responses to matters taken on notice at the public hearing of 15 August in relation to this matter. Consistent with these comments, the Department and ASIO do not support the inclusion of a further exception in favour of journalists (or any other class of person) or the inclusion of a general 'public interest defence'. The inclusion of such exceptions is inconsistent with established principles of Commonwealth legal policy in relation to secrecy offences. The harm targeted by the offences in s 35P is not the identity of the person making the disclosure or their subjective motivation, but the harm or significant risk of harm inherent in the very disclosure of operationally sensitive information. As such, it is appropriate that all members of the community are expected to adhere to the relevant non-disclosure obligations, which should apply equally to all persons.

The Department and ASIO further refer to the Department's evidence and responses to matters taken on notice about the meaning of the fault element of recklessness which applies to the physical element of these offences in proposed ss 35P(1)(b) and 35P(2)(b). This element requires the prosecution to prove, beyond reasonable doubt, that a person was reckless as to whether the information disclosed related to a special intelligence operation. Given the special meaning of recklessness in the criminal law (under s 5.4 of the *Criminal Code 1995*) this fault element is considered to impose a rigorous burden of proof on the prosecution and appropriately limit the ambit of the offence.

In addition to these remarks, the Department confirms that no persons (including journalists) have been investigated, referred for prosecution or prosecuted in relation to the corresponding disclosure offences in ss 15HK and 15HL of the Crimes Act, which have been in force since 2010. This tends to suggest that the concerns raised by some submitters and witnesses to the inquiry in relation to possible exposures to criminal liability are not substantiated by the practical operation of these provisions.

Other disclosure offences – Schedule 6

Possible additional exceptions – disclosures to the IGIS

The Department and ASIO note the remarks in the IGIS's submission in relation to the potential impact of the proposed amended and new offences in Schedule 6 on the work of her Office. (As noted above, these remarks have suggested a need to give express effect to the policy intention that the offences do not apply to complaints or pro-active disclosures made to the IGIS, or to the communication of information by IGIS staff to the IGIS or other staff of her Office.)

The Department and ASIO are of the view that pro-active disclosures made to the IGIS by 'entrusted persons' – such as complaints or as part of inspections – are not captured by the elements of the offences in Schedule 6, in relation to the ASIO Act and the Intelligence Services Act. (The offences apply to the unauthorised communication of information, dealings with records, and recording of information by an 'entrusted person'.)

To be unauthorised, the relevant communication, recording or dealing must have been made or done contrary to a person's existing authority, or without authority, to engage in that conduct. Authority may be found in the person's duties of employment; in accordance with a contract, agreement or arrangement; or within an authority conferred on the person by the Director-General; or with the specific approval of the Director-General or another staff member authorised to give an approval. In the Department and ASIO's view, the disclosures to the IGIS referred to above will have been authorised, either under a person's ordinary duties of employment or a specific authority or direction to disclose particular information.

To the extent that a complaint is made to the IGIS by an 'entrusted person', the regime under the PID Act would apply in relation to the disclosure, with s 10 of that Act conferring an immunity from liability to any secrecy offence in relation to the disclosure. To the extent that a disclosure is made in accordance with the IGIS's statutory powers of inquiry, s 18(9) of the IGIS Act will provide the person with an immunity from liability to any secrecy offence.

However, the Department and ASIO acknowledge the preference of the IGIS for these matters to be made clear on the face of the legislation, and agree that it is important the offences do not operate as a perceived barrier to disclosing information to, or cooperating with, the IGIS in the performance of her statutory functions. The Department and ASIO will assist the Government in considering possible amendments to give effect to this preference, taking into account any views of the Committee on this matter.

Additional issues raised by submitters and witnesses on Schedule 6 (addressed in Part 2)

Part 2 of this submission provides a response to further comments of some submitters and witnesses to the inquiry in relation to the coverage of existing secrecy offences, suggested limitations in the PID regime and the penalties applied to the offences.

Coverage of the proposed new term 'ASIO affiliate' – application to legal persons

Submissions and evidence

Some submitters and witnesses to the inquiry have suggested that the proposed new term 'ASIO affiliate' in s 4 of the ASIO Act represents an expansion of the powers presently conferred on persons other than ASIO employees.[89] The proposed term 'ASIO affiliate' is defined as "a person performing functions or services for the Organisation, in accordance with a contract, agreement or other arrangement, and includes a person engaged under section 85 [consultants and contractors] and a person performing services under section 87 [secondment of persons to the Organisation] but does not include the Director-General or an ASIO employee".

As noted in the Department's responses to the matters taken on notice at the public hearing of 15 August (provided on 18 August), the new term 'ASIO affiliate' does not represent a material expansion of the range of individuals who are not ASIO employees, who perform

89 For example, Law Council of Australia, *Submission 13*, pp. 13-15.

functions or services for ASIO. Rather, it is a collective label to replace the existing 'patchwork' of terms used to describe such persons in the ASIO Act and other Commonwealth legislation. (Some further comments in response to stakeholder comments on this issue are provided in Part 2 below. These relate to the proposed consequential amendments in Part 2 of Schedule 1 to the Bill, which will apply the new terms 'ASIO affiliate' and 'ASIO employee' wherever ASIO personnel are referenced in other Commonwealth legislation.)

However, some submitters are additionally concerned that the concept of an 'ASIO affiliate' could apply to a legal person (such as a foreign intelligence agency) with the result that the relevant entity can, in effect, be tasked to perform functions or services for the Organisation. The Committee has sought a response from the Department and ASIO on this issue.

Departmental and ASIO comments

The reference to 'a person' in the new term 'ASIO affiliate' is intended to be limited to natural persons. The actions that constitute performance of functions or services for ASIO would, in context, be the actions physically done by an individual (that is, a natural person). It is considered that the proposed definition evinces a contrary intention to the general rule of interpretation in s 2C(1) of the *Acts Interpretation Act 1901* that expressions used to denote persons generally (such as the word "person") include a body politic or corporate as well as an individual. As such, an amendment to the provision is not considered necessary. To address this concern, however, the Department and ASIO will assist the Government in considering amendments to the Explanatory Memorandum to include an express statement of this intention.

Safeguards referenced in the Explanatory Memorandum

Submissions and evidence

Some submitters and witnesses to the inquiry commented that various safeguards referenced in the Explanatory Memorandum were not, in their view, readily identifiable on the face of the corresponding provisions of the Bill.

For example, Electronic Frontiers Australia commented that the 'recklessness' safeguard for the proposed new s 35P offence is in the Explanatory Memorandum but is not in the legislation.[90] As the Department has explained (in the 15 and 18 August hearings, and in supplementary material provided to the Committee), the element of recklessness applies through the normal operation, and application of subsection 5.6(2), of the Criminal Code. This is specifically mentioned in paragraph 556 of the Explanatory Memorandum.

In addition, the Civil Liberties Councils suggested there was a difference between the Explanatory Memorandum and the Bill on the immunities provided by a special intelligence operation authority suggesting that the Explanatory Memorandum refers to a limited

90 Proof Committee Hansard, 18 August 2014, p. 12.

immunity while the Bill says "anything unlawful can be done with three exceptions."[91] This is misleading. The Explanatory Memorandum and the Bill are consistent on this issue. It is clear from both that, among other things, the protections apply only to a 'special intelligence operation' (for which certain requirements need to be satisfied, as set out in new s 35C), the authority must contain certain information including the 'special intelligence conduct' a person can engage in (new s 35D), and the protection is constrained in the ways set out in new s 35K. This is consistent with the Explanatory Memorandum. In particular, the Explanatory Memorandum:

- states that the immunity from liability applies exclusively to conduct that is engaged in as part of an SIO that is authorised and carried out in accordance with the requirements in the new Division (at paragraph 482),
- notes that the issuing criteria ensure SIOs are only able to be conducted where necessary and appropriate, and unlawful conduct is limited (at paragraph 502 which includes references to Bill provisions),
- provides that the nature and scope of an SIO authority are required to be particularised and documented, to promote clarity and certainty in operation (at paragraph 509, with reference to Bill provisions), and
- clearly spells out the limited nature of the immunity, including by reference to the relevant parts of section 35K (paragraphs 532-539).

The IGIS commented that the Bill, unlike the Explanatory Memorandum, is not explicit that ASIO employees who are seconded to another body or organisation will not retain their ASIO powers while on secondment.[92] As observed by the Department in response to matters taken on notice (at p 27), the intended result (as articulated in the Explanatory Memorandum at p. 43) is considered to be inherent in the nature of a 'secondment'. However, if further clarification is thought desirable, an 'avoidance of doubt' provision could be added to proposed new s 86 to confirm the intended meaning of the term 'secondment'.

Departmental and ASIO comments

In light of these and other comments about the Explanatory Memorandum, the Department is assessing whether further material could be added in relevant places to assist in the understanding of the legislative package.

The Department has identified some potential improvements, including in the Statement of Compatibility with Human Rights. In particular, references to particular provisions of the Bill could be inserted alongside references to specific safeguards in the Statement, in order to further assist in understanding the range of safeguards and accountability measures that apply to the proposed new measures.

---

91 Proof Committee Hansard, 18 August 2014, pp. 21-22.

92 Inspector-General of Intelligence and Security, *Submission 4*, pp. 6-7.

There may also be places where the Explanatory Memorandum could further make clear that, apart from specific safeguards in the Bill, there are also various existing safeguards that apply generally to intelligence agencies' conduct and activities, including the significant oversight role of the IGIS and, in ASIO's case, the Attorney-General's Guidelines which guide ASIO in the performance of its security intelligence functions.[93]

The Department and ASIO will assist the Government in considering possible revisions to the Explanatory Memorandum, including consideration of any views the Committee may provide on this matter.

Part 2 – Additional issues raised by submitters and witnesses

Schedule 1 – ASIO employment, etc

Secondment – further limitations

Submissions and evidence

Some submitters to the inquiry suggested that proposed new ss 86 and 87 should include additional statutory conditions or limitations in relation to the secondment of persons to and from ASIO. The Law Council of Australia, for example, suggested that there should be statutory requirements (or alternatively provision in the Attorney-General's Guidelines to ASIO) for a reasonable minimum secondment period. The Law Council further recommended that the secondment arrangements be the subject of specific oversight and reporting by the IGIS, by way of classified annual reports on their operation and effectiveness.[94] These were said to be necessary to prevent the possibility identified by some submitters to the Committee's 2012-2013 inquiry that the proposed secondment arrangements could be used to circumvent existing statutory limitations on ASIO employees or persons subject to limitations in other legislation such as the Intelligence Services Act.

Departmental and ASIO comments

The Department and ASIO do not consider it necessary to write such additional limitations and conditions into the ASIO Act or the Attorney-General's Guidelines, or to confer a specific oversight function on the IGIS in relation to secondment.

As has been noted previously, the Department and ASIO are of the view that the term 'secondment' would not, in this context, be applied to enable arrangements for the purpose of enabling an employee of one agency (the 'home agency') to perform functions or exercise powers under another agency's legislation (which are not available under the home agency's legislation) for the benefit of the home agency. The use of secondments, including across the Commonwealth, is not new, nor unique to an intelligence agency such as ASIO. A secondment regime is a tool for resourcing agencies, building networks and sharing

93 Further details of these safeguards are provided in ASIO's submission to the inquiry, *Submission 16*, pp. 4-6.

94 Law Council of Australia, *Submission 13*, pp. 12-13.

expertise – which can often be in short supply. Host employers ordinarily enter secondment arrangements to add resources to the host agency and to assist the host agency to undertake its functions. Secondments are not about achieving the functions of the home agency.

As indicated in the Department's response to the matters taken on notice at the Committee's public hearing on 15 August, the Department considers that it is inherent in the nature of a secondment, in the context of proposed new ss 86 and 87, that a secondee ceases to perform any statutory functions under his or her employment by the home agency, and performs exclusively those of the incoming or host agency – for the host agency alone – for the duration of the secondment. In light of stakeholder concern about this matter, however, the Department and ASIO will assist the Government in giving consideration to whether the Explanatory Memorandum could be revised to include an explanation of this point.

In addition, the general oversight jurisdiction of the IGIS will extend to the examination of secondments to and from ASIO under the new provisions, and is considered adequate to enable effective oversight of such arrangements. The Department and ASIO note that the IGIS has not sought a specific, additional power to review secondment arrangements, and has indicated that, if the Bill is passed, she intends to adapt her existing oversight arrangements and practices in order to maintain "awareness and oversight of the activities of ASIO employees wherever they are working".[95] In addition, the Director-General of Security may, if considered necessary, include conditions or limitations in written secondment arrangements or agreements made under proposed ss 86(1) and 87(2).

ASIO affiliate – suggestions that amendments are an extension of powers

Submissions and evidence

Some submitters and witnesses disputed the statement at p. 7 of the Explanatory Memorandum that the application of the proposed new term 'ASIO affiliate' is a minor and technical amendment that simply affixes a new, uniform label to the range of disparate terminology in the ASIO Act and across Commonwealth legislation used to describe persons who are in a form of relationship with ASIO other than employment.

The provisions of Part 2 of Schedule 1 to the Bill make a range of consequential amendments to other Commonwealth legislation which confers upon ASIO personnel various powers, authorities, duties, obligations, immunities and liabilities. Such personnel are generally

95 Inspector-General of Intelligence and Security, *Submission 4*, p. 7. (By way of clarification, it is noted that, where ASIO employees are seconded to a non-Intelligence Services Act agency – for example to an Australian Public Service Agency with no national security or intelligence-related responsibilities – the IGIS may not have jurisdiction over the duties or functions that person performs on secondment. However, if there was any suggestion that person was continuing to perform duties or functions in relation to their employment by ASIO, the IGIS would likely have jurisdiction to inquire into such matters. In addition, ASIO employees seconded to such agencies would be subject to the oversight and accountability arrangements applying to those agencies, in relation to the activities they perform on secondment. For example, the oversight and accountability arrangements applying to the Australian Public Service, or the Australian Parliamentary Service.)

referred to as 'officers' or 'employees' of ASIO, and this terminology is not defined in the relevant legislation to be amended by Part 2 of Schedule 1.

The consequential amendments in Part 2 of Schedule 1 to the Bill generally substitute the phrase 'officer or employee' of ASIO with the phrase 'ASIO employee or ASIO affiliate', or in some instances uses the term 'ASIO employee' alone or insert separate provisions, in substantially the same terms, for ASIO employees and ASIO affiliates respectively. It was suggested by some submitters that the use of the new term 'ASIO affiliate' means that the proposed consequential amendments would "increase the number of people able to perform duties and functions and exercise powers currently only permitted to be carried out by an officer or employee of ASIO.[96] (This conclusion appears to be based on an interpretation of the word 'officer', as that term is used in the relevant legislation to be amended consequentially by Part 2 of Schedule 1, that excludes the persons covered by the proposed new term of 'ASIO affiliate'.)

For example, the Law Council of Australia submitted that the following consequential amendments to the TIA Act may expand the classes of persons able to be authorised to undertake interception or other activities under that Act:

- Exceptions to the prohibition on intercepting telecommunications: s 7(2) (amending items 60-61 of Part 2, Schedule 1 to the Bill)[97]
- Evidentiary certificates – execution of warrants: s 18(4) (amending item 64 of Part 2 of Schedule 1).[98]
- Dealing with TI-related information in connection with ASIO's functions: ss 136(2)-(4) (amending items 70-72 of Part 2 of Schedule 1)[99]

---

96 Law Council of Australia, *Submission 13*, p. 13.

97 Subparagraph 7(2)(ac) of the TIA Act provides for an exception to the general exception on the prohibition on intercepting telecommunications in s 7(1) in favour of actions taken by "an officer of the Organisation" in the lawful performance of duties for the purpose of discovering whether a listening device is being used. or determining the location of a listening device. Amending item 60 replaces the phrase "officer of the Organisation" with "ASIO employee". Amending item 61 creates an identical provision, in new paragraph (ad), specifically for ASIO affiliates. A separate provision was needed to make clear that an ASIO affiliate who engages in such action must have been authorised under his or her contract, agreement or other arrangement for the performance of functions or services for ASIO; and that an ASIO employee must have been authorised by his or her duties of employment.

98 Subsection 18(4) of the TIA Act provides that the Director-General of Security or a Deputy Director-General of Security may issue a prima facie evidentiary certificate in relation to anything done by "an officer or employee of the Organisation" in connection with the execution of an interception warrant, or certain actions in relation to information obtained under a warrant. Amending item 64 replaces the phrase "officer or employee of the Organisation" with the new terms 'ASIO employee' and 'ASIO affiliate'.

99 Subsections 136(2)-(3) of the TIA Act provide for the communication of foreign intelligence information by the Director-General of Security to "an officer or employee of the Organisation", and by such an officer or employee to the Director-General or another officer or employee. This is provided that such communication is made in connection with the Organisation's performance of its statutory functions. Subsection (4) further permits the Director-General or "an officer or employee of the Organisation" to make use of, or make records of, foreign intelligence information. Amending

- Exemption from offence of accessing stored communications: s 108. (amending items 68 and 69 of Part 2 of Schedule 1).[100]

Based on its view that the measures in Part 2 of Schedule 1 will expand the classes of persons who are currently subject to the relevant provisions, the Law Council suggested that clarification is needed about the following matters:

- how the proposed amendments expand the ability of individuals other than ASIO employees to utilise significant powers and protections;
- which kinds of people are covered under these arrangements, the types of services they provide to ASIO and under what arrangements; and
- what arrangements will be in place to ensure that such individuals have the professional skills, conduct and ethics and are able to be held accountable to undertake each of the specific functions and duties which are currently limited to ASIO employees.[101]

Departmental and ASIO comments

Suggested expansion of categories of persons able to exercise powers / perform functions, etc

The Department and ASIO acknowledge that there is a need to provide public reassurance about the scope of powers, authorisations, duties, liabilities and immunities conferred upon persons who are performing services or functions for ASIO. The Department and ASIO remain of the view that the term "ASIO affiliate" is a label describing a range of persons, who are not employees, who perform functions or services for ASIO.

It should be recognised that there are two limitations on an ASIO affiliate's ability to exercise powers, or perform functions, for ASIO. The first arises from the definition of "ASIO affiliate" – being a person who performs functions or services for ASIO pursuant to a contract, agreement or arrangement. The validity of activities or actions undertaken by an ASIO affiliate depends on the person acting in accordance with the relevant contract, agreement or arrangement. The second arises because the term identifies the pool of persons

---

items 70-72 substitute the phrase "officer or employee of the Organisation" with the new terms 'ASIO employee' and 'ASIO affiliate'.

100 Subsection 108(2) is an exception to the offence in s 108(1) of accessing a stored communication. Paragraph 108(2)(g) creates an exception for access as a result of, or incidental to, action taken "by an officer of the Organisation" in the lawful performance of his or her duties for the purpose of discovering whether a listening device is being used, or determining the location of a listening device. Amending item 68 replaces the reference to "officer" with the new term 'ASIO employee'. Amending item 69 inserts a new paragraph (ga) which applies the same exception to ASIO affiliates who have acted in accordance with their contract, agreement or arrangement. Like amending items 60 and 61 above (in relation to the prohibition on interception in s 7), a separate provision was needed to make clear that an ASIO affiliate who engages in such action must have been authorised under his or her contract, agreement or other arrangement for the performance of functions or services for ASIO; and that an ASIO employee must have been authorised by his or her duties of employment.

101 Law Council of Australia, *Submission 13*, p. 15.

who might be able to do certain things under legislation. To exercise legislative powers, an ASIO affiliate would also need to be specifically authorised, in accordance with any legislative requirements, or other policy considerations, that may additionally apply. This is consistent with the authorisation necessary for an ASIO employee to exercise legislative powers.

The development of the consequential amendments gave consideration to the consistency with the overarching policy intent of the relevant legislation being amended. For example, paragraph 7(2)(ac) of the TIA provides that an activity is not prohibited by subsection 7(1) if that activity is for the purpose of determining if a listening device is being used, or to determine the location of it (similar provisions are provided for in s. 108 for stored communications). It is appropriate that this regime applies to persons (ie "ASIO affiliates") required to undertake these activities as part of their role within ASIO.

A further example is the consequential amendments to Division 105 of the *Criminal Code 1995* (Cth) (Code) in amending items 38-41 of Part 2 of Schedule 1 to the Bill. These amendments relate to the Commonwealth's preventative detention order scheme, under which persons can be detained for up to 48 hours for the purpose of preventing an imminent terrorist act. Division 105 of the Code imposes certain prohibitions and obligations on ASIO personnel (such as prohibitions on questioning persons who are detained under a preventative detention order). It would be inappropriate for an ASIO affiliate, because of nature of his or her legal relationship with ASIO, to be able to question a person detained under a preventative detention order. Expressly including the new label of "ASIO affiliate" in this context is necessary to maintain the policy intention underlying the relevant provisions of Division 105 of the Code. As such, to the extent that there may be any ambiguity or scope for argument about a contrary interpretation of the phrase "officer or employee" of ASIO as it is used in Division 105 of the Criminal Code, the proposed amendments will ensure that the policy intention underlying the relevant provisions in Division 105 is given effect.

Accordingly, the Department and ASIO will assist the Government in considering whether the Explanatory Memorandum should be amended to better explain the effect of the proposed amendments in Part 2 of Schedule 1, having regard to the concerns raised by some submitters and witnesses participating in the Committee's inquiry and the responses provided above.

Request for further information about ASIO affiliates – coverage and control/oversight

The Department and ASIO note the suggestion of the Law Council that the Committee seeks further information about the coverage of the term 'ASIO affiliate' (in terms of the persons to whom it applies), and the arrangements for ensuring appropriate control, oversight and accountability in relation to these persons. The following additional information is provided to assist the Committee, and submitters and witnesses to the inquiry, in considering these matters.

The term 'ASIO affiliate' reflects the existing position under the ASIO Act that non-employees may exercise ASIO functions and perform services for ASIO, if and when appropriately authorised to do so. The operational requirements of the Organisation are such

that it is necessary to have a range of persons available in order to flexibly utilise resources and respond to threats. The classes of persons within the term 'ASIO affiliate' can include consultants and contractors and secondees to ASIO[102] and sources.[103]

Appropriate control and oversight is exercised in relation to ASIO affiliates by way of such mechanisms as:

- Decisions by the Director-General of Security about the engagement of a person as an 'ASIO affiliate', consistent with the Director-General's overall control of, and responsibility for, ASIO. (That is, the Director-General has responsibility for decisions about whether to enter into a contract, agreement or some other arrangement with a person for the performance of functions or services for the Organisation, and the terms of any such contract, agreement or arrangement.)

- The terms of an ASIO affiliate's contract, agreement or arrangement for the performance of functions or services for the Organisation.

- Statutory[104] and administrative[105] limitations on ASIO affiliates' authority to engage in activities as part of the services and functions they perform for ASIO.

- The exposure to criminal liability of ASIO affiliates who act without authorisation. (For example, ASIO affiliates who contravene a statutory prohibition, or who act in excess of a statutory authority or the scope of authority conferred upon them in a contract, agreement or arrangement).[106]

---

102 As per the proposed definition in s 4 (amending item 1 of Schedule 1) which includes persons engaged under proposed s 85 (consultants and contractors) and s 87 (persons seconded to ASIO) who are performing functions or services for ASIO in accordance with the relevant contract, agreement or other arrangement.

103 Proof Committee Hansard, 15 August 2014, pp.12, 13. (In addition, as noted in the Department's responses to matters taken on notice at the hearing on 15 August, consideration was given to drafting the relevant legislative provisions to allow the Director-General to authorise any person, for any purposes, without any limitation. However, the use of the term 'ASIO affiliate' was preferred as a more measured and transparent approach of expressly identifying the range of persons who could be authorised.)

104 Statutory limitations include: limiting certain powers or authorisations to ASIO employees only (such as the ability to make an application for a special intelligence operation authority under proposed s 35B); and limiting certain authorisations to ASIO affiliates who are 'senior position holders' (such as the authority under s 24 to approve others to authorise the exercise of powers under warrants).

105 Administrative limitations include investing the Director-General with the power to exclude specific ASIO affiliates (including classes of affiliates) from exercising some powers which they are authorised to exercise under the ASIO Act (namely, warrantless surveillance powers in proposed new ss 26C-26E, as per proposed s 26F).

106 The non-disclosure offences in the ASIO Act as amended or inserted by Schedule 6 to the Bill apply to affiliates who disclose information, handle records or record information outside the scope of their authority (including under their contract, agreement or arrangement). Amending item 26 of Part 2 of Schedule 1 to the Bill also provides that an ASIO affiliate is a Commonwealth officer for the purpose of the Crimes Act, and therefore liable to the secrecy offences in that Act in respect of unauthorised disclosures.

- The ability of the Director-General to issue directions to, or make internal guidelines or policies applicable to, ASIO affiliates; and to vary or terminate contracts, agreements or arrangements), consistent with the Director-General's authority to exercise control of the Organisation under s 8(1) of the ASIO Act.

- The oversight jurisdiction of the IGIS in relation to ASIO affiliates.[107]

The Department and ASIO acknowledge that there would be benefit in including a statement in the Explanatory Memorandum to the Bill outlining the control and oversight mechanisms in relation to ASIO affiliates, and will assist the Government in making a decision on this matter, including with the benefit of any comments the Committee may wish to make.

Schedule 2 – powers of the Organisation

Reporting and oversight

Submissions and evidence

There were some suggestions that ASIO's reports to the Attorney-General in relation to warrants could address some additional matters, particularly relating to activities which impact on third party privacy or other interests (such as use of force and third party computer use). The IGIS's submission and evidence to the inquiry indicated that additional reporting on these kinds of matters could assist in the performance of her oversight role.[108] Noting the IGIS's broad oversight powers and existing inspection practices, the IGIS has not suggested that it is necessarily the case that specific additional requirements should be added into the legislation, noting that she is "cautious to have any more prescriptive record-keeping requirements in legislation,"[109] but has emphasised the value of this kind of information to her oversight role.

Departmental and ASIO comments

The Department and ASIO acknowledge the importance of the IGIS's oversight role and the value of good record-keeping and reporting practices in facilitating the performance of that role. As noted in the Department's response to matters taken on notice in the 15 August hearing, careful consideration is needed in determining whether there are additional matters considered to be sufficiently 'exceptional' to justify an indefinite, statutory reporting requirement to the Minister, as opposed to managing the issues of most interest to the IGIS through practical measures such as good internal record-keeping and inspections by the IGIS.

107 See amending items 42-48 of Part 2 of Schedule 1 to the Bill which amend the IGIS Act accordingly.

108 Inspector-General of Intelligence and Security, *Submission 4*, pp. 10, 11, 12, 14.

109 Inspector-General of Intelligence and Security, Proof Committee Hansard, 15 August 2014, p.6.

Additional privacy related requirements

Submissions and evidence

Some submitters and witnesses to the inquiry suggested that the Attorney-General's Guidelines to ASIO under s 8A of the ASIO Act be reviewed, particularly in light of privacy impacts of the proposed amendments.[110] For example, both the Law Council of Australia and the Office of the Australian Information Commissioner (OAIC) noted the current value of the Guidelines and the importance of reviewing them in light of the impact of the proposed new powers and the changing broader environment.

There were also suggestions that the issuing criteria for ASIO warrants under Division 2 of Part III should include a specific privacy impact test.[111] The Law Council of Australia suggested that such a test should require satisfaction that the likely benefit of the access provided under the warrant would substantially outweigh the extent to which the disclosure is likely to interfere with privacy of each person affected.

Departmental and ASIO comments

The Department and ASIO consider that it is not necessary to include a 'privacy impact' or proportionality test in the warrant provisions. The objective of such a suggestion is addressed through a range of existing mechanisms including the issuing thresholds, the Attorney-General's Guidelines, and the oversight role of the IGIS.

The Guidelines issued by the Attorney-General under s 8A of the ASIO Act[112] impose requirements on ASIO relating to its handling of personal information and the proportionality of any intrusion into individual privacy having regard to the gravity of the threat posed and the probability of its occurrence.

In particular, clause 10.4 of the Guidelines requires that any means used for obtaining information "must be proportionate to the gravity of the threat posed and the probability of its occurrence … and [investigations] should be undertaken using as little intrusion into individual privacy as is possible".

Accordingly, before requesting a warrant ASIO is required to consider whether other, less intrusive methods of investigation are possible, and whether the obtaining of the information through warranted means of collection is proportionate to the gravity of the threat and the probability of its occurrence. Wherever possible, the least intrusive techniques of information collection should be used before more intrusive techniques.

The oversight power of the IGIS covers ASIO's compliance with these Guidelines.

---

110 Office of the Australian Information Commissioner, *Submission 11*, pp. 2-3 and Proof Committee Hansard 18 August 2014, pp. 29-30. See also Law Council of Australia, *Submission 13*, pp. 11-12.

111 Law Council of Australia, *Submission 13*, pp. 8, 17-18, 21, 26.

112 Attorney-General's Guidelines in relation to the performance by the Australian Security Intelligence Organisation of its function of obtaining, correlating, evaluating and communicating intelligence relevant to security (including politically motivated violence) – available on ASIO's website.

The Department and ASIO agree that the Guidelines and rigorous application of them will continue to be important in ensuring community confidence in safeguards, particularly by requiring ASIO to consider the necessity and proportionality of handling personal information and in ensuring inquiries and investigations be undertaken using as little intrusion into individuals' privacy as is possible.

Noting the concerns about the potential impact of the new measures, the Department and ASIO acknowledge that it may be timely to reconsider the Guidelines to determine if they remain appropriate in their current form or would benefit from relevant amendments. The Department will assist the Attorney-General in giving consideration to this matter, in consultation with ASIO, the OAIC and the IGIS.

Entry to third party premises

Submissions and evidence

Submitters to the inquiry argued that powers to enter third party premises for the purposes of entering and exiting target premises should be made subject to additional thresholds, such as a 'last resort' requirement, or a requirement that there is a substantial risk of detection unless third party premises are accessed.[113] Some submitters further supported a requirement that ASIO notify owners or occupants of third party premises, and to rectify any interferences.[114]

Departmental and ASIO comments

The Department and ASIO do not consider that such additional requirements are necessary or appropriate. The ability of ASIO to enter premises is limited to the purpose of gaining access to target premises. The general test for the issuing of a warrant and the specific activities authorised apply, as well as the privacy requirements in ASIO's Guidelines mentioned previously. As further noted previously, thresholds in the nature of a 'last resort' requirement are not supported because they may preclude the collection of intelligence on the basis that other, higher risk or less effective ways of collecting the relevant intelligence exist.

Third party notification requirements are not supported because they would frustrate the necessarily covert nature of intelligence operations. The general oversight jurisdiction of the IGIS – including the ability to recommend the payment of compensation in appropriate case – is considered to be an appropriate means of balancing operational need with the rights and interests of third parties.

113 Law Council of Australia, *Submission 13*, p. 26.

114 Civil Liberties Councils, *Submission 20*, p. 8.

Use of force against persons

Submissions and evidence

Some submitters and witnesses argued that the use of force provisions are unnecessary.[115] Others argued that there should be a specific exclusion of force that is likely to be lethal or cause grievous bodily harm.[116]

Departmental and ASIO comments

Need for the use of force against persons

The proposed amendments will expressly provide that ASIO has the power to use any force against any persons or things necessary and reasonable to do the things specified in a warrant. The power is not limited to the purpose of gaining entry to the premises, but can be exercised at any time during the execution of the warrant.

Force can only be used against a person when it is reasonable and necessary to do the things specified in the warrant. The authorised force used must be reasonable and necessary in the circumstances, it does not constitute grievous bodily harm or lethal force. Any use of unauthorised force against a person may attract civil and criminal liability.

The use of force is necessary to enable the effective execution of a warrant for intelligence purposes, for example it may be necessary to use force to obtain access to a thing on the premises, such as a door or cabinet lock or to use force to install or remove a surveillance device.

It is also necessary to be able to use force against a person when executing a warrant otherwise a person may obstruct the execution of the warrant and the executing officers will have no ability to prevent them from doing so. For example, a person may prevent access to a room or an item or may prevent a person authorised to execute the warrant from leaving the premises by blocking the exit. Therefore without the ability to use reasonable and necessary force against a person the warrant may be rendered ineffective and may additionally endanger persons lawfully authorised to execute the warrant.

ASIO is unable to rely on police assisting an ASIO search warrant as police, like ASIO employees, are reliant on use of force provisions within the ASIO search warrant power. Further, while ASIO will typically request law enforcement attendance at warrants that have some form of operational risk, given their extensive training in relation to use of force principles, police may not be present in some instances depending on the associated risk planning for a particular operation

115 Law Council of Australia, *Submission 13*, pp. 8-9, 28-29.

116 Muslim Legal Network, *Submission 21*, p. 11.

Suggested express exclusion of lethal force and grievous bodily harm

While consideration could be given to an express exclusion of force that is likely to be lethal or cause grievous bodily harm, the provision already has this legal effect due to the absence of specific authorisation of such force. The Department and ASIO acknowledge there may be benefit in expressly stating this in the Explanatory Memorandum.

Evidentiary certificates

Submissions and evidence

It was suggested that proposed s 34AA should expressly exclude from its scope any material that may address or prove the substantive elements of a criminal offence.[117]

Departmental and ASIO comments

Express exclusion of material that may address or prove the elements of an offence

The Department and ASIO are of the view that such an express exclusion is unnecessary because proposed s 34AA certificates are limited to technical matters relevant to the collection of evidence under a warrant – such as capabilities and sources. Certificates are not directed to proving the veracity or weight of evidence that may apply to the content of the relevant intelligence obtained under a warrant, in the event that it is sought to be relied upon as evidence in a criminal prosecution. In these instances, the general protections available for classified and sensitive information in judicial proceedings would apply, including under the *National Security Information (Criminal and Civil Proceedings) Act 2004*. In the event a defendant or respondent had concerns as to the breadth and scope of the facts covered by such a certificate because it appeared to include material or facts that would address or prove the ultimate facts in the case (or elements of the offence), the prima facie nature of the certificate means it would be challenged in court and both parties given an opportunity to test its limits. In such circumstances, a certificate would likely be struck out on the basis that it covered ultimate facts or facts that went to proving the elements of the offence, in excess of the matters covered by s 34AA.

Additional matter – unintended omission of search warrants authorising computer access

The Department and ASIO also draw the Committee's attention to an unintended oversight in the classes of warrants to which proposed s 34AA applies. Proposed subsection (1) provides that the evidentiary certificate scheme applies to acts or things done in connection with a relevant warrant, which is defined in proposed subsection (5) as meaning a computer access warrant, a surveillance warrant, or an identified person warrant or an emergency warrant to the extent that those warrants authorise computer access or surveillance, as per proposed subsection (2). This is consistent with the intention that evidentiary certificates are limited to the protection of capability and methodology, not the intelligence collected under a warrant.

117 Law Council of Australia, *Submission 13*, pp. 26-27.

However, search warrants issued under s 25 are not included as relevant warrants, despite the fact that computer access can be authorised under these warrants. The Department and ASIO consider that s 25 should be included in the definition of a relevant warrant, in relation to computer access under a search warrant. Identical considerations apply in relation to the protection of capability under s 25 (in relation to computer access) as for all other types of warrants within the definition of a relevant warrant in subsection (5).

Classes of persons authorised to exercise powers under warrants

Some submitters and witnesses have suggested that the need for the proposed amendments to s 24 (which would enable the authorisation of classes of persons to exercise powers under a warrant) has not been demonstrated.[118] The Department and ASIO do not agree with these suggestions, and refer to the reasoning in support of recommendation 32 of the Committee's 2013 report.

Variation of warrants

Submissions and evidence

It has been suggested that the power to vary warrants should be limited to variations of a minor and technical nature.[119]

Departmental and ASIO comments

The Department and ASIO do not support this proposal because it is inherent in the nature of a variation power – as distinct from an issuing power in relation to a subsequent warrant – that the warrant, as varied, must continue to meet all relevant issuing and authorisation requirements. As such, a variation power could not be relied upon to circumvent the issuing or authorisation requirements applying to warrants. In addition, variations will be subject to the oversight of the IGIS as part of the general jurisdiction under the IGIS Act.

Identified persons warrants

Submissions and evidence

Some submitters and witnesses suggested that investing the Director-General of Security with the power to authorise the exercise of powers under an identified person warrant issued by the Attorney-General, together with the threshold for authorisation, represents a lowering of the threshold and the dilution of accountability.[120] Others, however, acknowledged the safeguards built into the system. For example, the Law Council of Australia noted that while it holds in-principle concerns with a warrant approach that enables ASIO to request a single

118 Law Council of Australia, *Submission 13*, p. 28.

119 Law Council of Australia, *Submission 13*, pp. 9, 29.

120 Associate Professor Greg Carne, *Submission 5*, pp.5-6. See also Muslim Legal Network, *Submission 21*, pp. 9-10.

warrant specifying multiple powers against a single target, "these concerns are addressed to some degree by the type of safeguards and criteria outlined in the … Bill".[121]

Departmental and ASIO comments

The Department and ASIO strongly disagree with suggestions that thresholds will be lowered or safeguards weakened under the new identified person warrants.

The threshold for an identified person warrant will not be lower or weaker than the threshold for any of the individual special powers warrants. There are two different thresholds that currently apply to ASIO special powers warrants:

- the threshold in surveillance devices and postal/delivery articles warrants is that the Attorney-General must be satisfied that the **person** is engaged in, or is reasonably suspected by the Director-General of being engaged in, or being likely to engage in, **activities prejudicial to security**.

- the other threshold (in search warrants and computer access warrants) is that the Attorney-General must be satisfied that there are reasonable grounds for believing that **access by** ASIO to records, data and other things **will substantially assist** the collection of intelligence in respect of a matter that is **important in relation to security**.

As the proposed new warrant would be sought in relation to an 'identified person', one option in developing the threshold was to use the threshold that requires satisfaction of facts relating to the activities of that person.

However, in order to ensure no weakening of the threshold in relation to any of the special powers to be used under the new warrant, the two thresholds have been merged. The proposed new threshold in s 27C(2) has two limbs. The Attorney-General must be satisfied that:

- the person is engaged in or is reasonably suspected by the Director-General of being engaged in, or of being likely to engage in, activities prejudicial to security, and

- the issuing of an identified person warrant will, or is likely to, substantially assist the collection of intelligence relevant to security.

In addition to the two-limbed threshold for the issue of the identified person warrant, there is an *additional* threshold test to be met before any powers can be exercised by ASIO under the warrant. This requires the Attorney-General or Director-General to be satisfied on reasonable grounds that the use of the specific power in the particular circumstances will substantially assist the collection of intelligence in relation to the activities prejudicial to security.[122]

---

121 Law Council of Australia, *Submission 13*, pp. 19-20.

122 This test is set out in the specific provisions relating to each particular power: s 27D(3) for search of premises and persons; s 27E(4) for computer access; s 27F(3) for surveillance devices; s 27G(4) for inspection of postal articles; and s 27H(4) for inspection of delivery articles.

The use of an identified person warrant can enhance accountability and oversight, as the decision maker will be required to consider the appropriateness of the use of multiple powers against a single person which may not always be apparent to the decision maker where warrants against the same person are sought on an individual basis.

Although the proposed measures would enable the Director-General (as well as the Attorney-General) to authorise the exercise of powers under warrants issued by the Attorney-General, the Department and ASIO view is that this does not result in a reduction in accountability or oversight measures.

There is a range of existing accountability mechanisms to ensure that these powers are appropriately used. Mechanisms include:

- The Attorney-General may specify conditions and restrictions in the warrant (under proposed new s 27C(6)), which could include that it only provides authority to use certain special powers in certain circumstances.
- The Director-General is required to report to the Attorney-General on how each special powers warrant has assisted ASIO in carrying out its functions.
- The IGIS's independent oversight role includes an ability to inquire into legality and propriety of ASIO's actions. The IGIS has specifically noted that authorisation decisions by the Director-General will be subject to IGIS oversight,[123] and the IGIS's role would also include assessing ASIO's adherence to legislative and non-legislative requirements in relation to these warrants.

Surveillance devices

A handful of submitters and witnesses made various suggestions to increase the thresholds for the issuing of surveillance device warrants by replicating those in s 16(2) of the Surveillance Devices Act, and the reporting requirements in relation to such warrants under that Act. Concern was also expressed about the ability of ASIO affiliates to undertake warrantless surveillance activities.

The Department and ASIO provide the following general remarks, in addition to the content in submissions to this inquiry and the Explanatory Memorandum to the Bill, and would be pleased to assist the Committee with any further information if needed. In general terms, the issuing criteria in s 16(2) are specific to law enforcement and were not considered suitable for inclusion in an intelligence-specific scheme. In addition, to the extent that privacy considerations are expressly included in s 16(2) of the Surveillance Devices Act, it is considered that functionally equivalent requirements are in the Attorney-General's Guidelines to ASIO. Similarly, the more detailed reporting scheme in the Surveillance Devices Act was not considered appropriate given the general oversight of the IGIS.

123 Inspector-General of Intelligence and Security, *Submission 4*, p.14.

In addition, the Department and ASIO are of the view that it is appropriate for ASIO affiliates to be authorised to exercise warrantless surveillance powers. Existing provisions of the Act authorise 'agents of the Organisation' to exercise surveillance powers. The concept of an 'ASIO affiliate' replaces the term 'agent of the Organisation' and offers greater transparency as to who may use surveillance devices without warrant because it is a defined term with a single meaning throughout the ASIO Act (in contrast to the term 'agents'). The use of warrantless surveillance powers only extends to an ASIO affiliate to the extent that they are acting in accordance with a contract, agreement or arrangement, under which the affiliate is performing functions or services for ASIO. Further, the Director-General, or an authorised delegate, may exclude specified affiliates or specified classes of affiliates from the operation of these provisions.

A submission was also made that the proposed surveillance devices warrants regime dilutes the degree of specificity currently required under the device-specific provisions, particularly the assessment of how each device is necessary, if multiple devices are specified in a single warrant application.[124] The Department and ASIO confirm that, although a single surveillance device warrant will replace the current multiple device warrant regime to streamline the existing framework in line with the Surveillance Devices Act, the existing safeguards will remain. The proposed warrant is focussed on the subject of intelligence collection (a person, a premises, or an object) rather than the particular device to be used in order to obtain the intelligence. Before intrusive activities directed at a person, a premises or an object respectively may be authorised, the corresponding legislative threshold must be addressed and satisfied. As such, a proposed warrant may authorise only the use of multiple devices against a person if the threshold is satisfied in the circumstances.

A submission was also made that it is unclear how, in practice, an issuing authority will be able to ensure that the relevant thresholds are met in relation to a person whose identity may not be known.[125] The Department and ASIO note that the legislative thresholds under both the proposed and current surveillance device regime require a consideration of the activities of a person, specifically that the person has engaged or is likely to engage in activities prejudicial to security. There must always be sufficient intelligence available about the person's security related activities in order to satisfy the threshold, even though it may not always be possible to accurately identify an individual.

Computer access

Submissions and evidence

One submitter suggested that the limited ability to add, copy, delete or alter data on a computer under s 25A may limit any evidential value of intelligence obtained under a computer access warrant because it may give rise to suggestions that relevant data was tampered with. It was additionally noted that the limited power may adversely impact on the

124 Associate Professor Greg Carne, *Submission 5*, pp. 4-5.

125 Law Council of Australia, *Submission 13*, p. 23.

ability of a person to receive a fair trial in prosecutions in which intelligence is adduced as evidence.[126]

Departmental and ASIO comments

The Department and ASIO are satisfied that neither of these circumstances are plausible. If information obtained under a computer access warrant is admitted or sought to be admitted in evidence in a prosecution or another type of enforcement action, it would be a matter for the court to determine its admissibility and the appropriate weight it should be afforded. Issues in relation to the integrity or provenance of evidence from electronic sources are not novel, and are capable of judicial determination in individual cases, in accordance with the ordinary rules of evidence.

Schedule 3 – special intelligence operations

Demonstrated need

Submissions and evidence

Notwithstanding the Committee's 2013 recommendation to proceed with a scheme of special intelligence operations, some submitters and witnesses were unconvinced of the need for such a scheme.[127] Key arguments against the enactment of a special intelligence operations scheme included: ASIO is not a law enforcement agency and should not automatically be given the same kinds of powers; comparable countries do not have such a regime; statistics on terrorism convictions in Australia do not suggest any significant gaps in intelligence gathering capabilities; cooperation between intelligence and law enforcement agencies should be fully utilised instead of a new legislative regime; the scheme would not be needed if counter-terrorism offences were not so broad; and prosecutorial and investigative discretion should be sufficient to protect participants in a covert intelligence operation from exposure to criminal liability.

Departmental and ASIO comments

The Department and ASIO remain of the firm view that the proposed scheme of special intelligence operations is necessary, for the reasons articulated in the Committee's 2013 report and as provided to the Committee in private session in the present inquiry.

The Department and ASIO note this view is further supported by the (then) Independent National Security Legislation Monitor, Mr Bret Walker SC, in his Fourth Annual Report dated 28 March 2014. The Monitor stated (at page 93 of this report) that he "considers it to be not only entirely appropriate for ASIO to be able to access such a scheme for its officers and human sources but also necessary for ASIO to perform its statutory functions, including its counter-terrorism role." The Monitor further noted (at page 94) that reliance on prosecutorial discretion is "neither an appropriate nor viable course to take in resolving the

126 Electronic Frontiers Australia, *Submission 9*, p. 4.

127 See footnote 27 above.

problem of criminal liability for activities done by ASIO officers and human sources in furtherance of the performance of ASIO's functions." The Monitor acknowledged (at page 95) that ASIO's statutory functions relating to intelligence and security are very different to the functions of law enforcement agencies, and that accordingly any scheme for ASIO would need to reflect ASIO's operating environment and the nature of security investigations and intelligence operations.

ASIO's continued ability to collect useful and relevant anticipatory intelligence, on the most serious threats to the security of Australia and Australians, relies on its capacity to covertly gain and maintain close access to highly sensitive information. This often involves engaging and associating closely with those who may be involved in criminal activity. This may expose an ASIO employee or affiliate to criminal and civil liability. Counter-terrorism criminal laws, which are intentionally designed to cover activity at an earlier stage than some other criminal laws in order to prevent terrorist acts, are capable of capturing the activities of ASIO employees and affiliates who are associating covertly with targets for lawful intelligence collection purposes.

Reliance upon the AFP controlled operation provisions or prosecutorial discretion are not viable options. The current AFP controlled operations scheme is not aimed at assisting ASIO in the performance of its functions such as the collection of security relevant intelligence. It can only be used by law enforcement for the collection of evidence about a serious offence and as such may only be used for the incidental production of intelligence where there is a correlation between the security matter and a relevant serious offence. This excludes a significant proportion of ASIO's legislative functions.

ASIO does and should, at all times, act lawfully. It is not considered appropriate for ASIO employees and affiliates to break the law and rely on the hope that prosecutorial discretion will be exercised in their favour. Whether to commence or continue a prosecution is a decision for the Commonwealth Department of Public Prosecutions (CDPP) or State or Territory Directors of Public Prosecutions. While the CDPP or State or Territory DPPs may decide not to prosecute a matter, this cannot be relied upon in ASIO's operational planning and does not mitigate ASIO's responsibility to collect intelligence in a lawful manner. A special intelligence operation scheme provides greater accountability in that the discretion of the DPP is not limited by the type of offence. A scheme which allows specific immunities and indemnities to be granted in a considered manner prior to the act in question occurring is considered to be more appropriate as a matter of policy.

Protections of a similar nature are in place in the United States and the United Kingdom. As mentioned above, the United States *Attorney-General's Guidelines on Federal Bureau of Investigation Undercover Operations* enables the FBI, in relation to both law enforcement and security functions, to authorise and conduct undercover operations which involve the conduct of activities which would otherwise constitute an offence.

Sunsetting requirements

Submissions and evidence

Some submitters and witnesses argued that the provisions should sunset after a specified period of operation, such as five years. This was said to be in recognition of the 'exceptional' nature of the scheme, which was said to warrant Parliament's further assessment of the effectiveness and continued necessity of the scheme after some operational experience has been acquired.[128]

Departmental and ASIO comments

The Department and ASIO do not support the application of a sunset provision to the provisions in Schedule 3 to the Bill. The need to provide participants in covert intelligence operations with limited protection from legal liability is not temporary in nature. Rather, its ongoing availability is needed to ensure that the Organisation has the capacity to meet emerging and future security challenges, by ensuring its capacity to gain close access to persons and groups of security concern, and providing legal certainty to persons assisting the Organisation in the performance of its functions.

The permanent nature of a special intelligence operations regime is consistent with the controlled operations scheme in Part 1AB of the Crimes Act, and the immunity from liability conferred upon staff members and agents of Intelligence Services Act agencies under s 14 of that Act. Both of these measures were enacted without sunset clauses, and this was found acceptable to the Parliament in 2010 and 2001 respectively.

Schedule 4 – ASIO cooperation with the private sector

Attorney-General's Guidelines – private sector cooperation

Submissions and evidence

Evidence to the inquiry from the OAIC suggested there should be greater clarity around the types of activities envisaged to be carried out under the new private sector cooperation ground in s.19(1)(d) of the ASIO Act.[129] The OAIC acknowledged the importance of ASIO's ability to cooperate with the private sector and the safeguards around that cooperation, but suggested there may be some value in considering whether further clarity could be provided in light of the potential privacy impact. The OAIC suggested consideration could be given to including additional material in the Explanatory Memorandum[130] or to including greater specificity about this role in the Attorney-General's Guidelines.[131]

128 See footnote 28 above.

129 Office of the Australian Information Commissioner, *Submission 11*, p. 3; Proof Committee Hansard, 18 August 2014, p. 30

130 Office of the Australian Information Commissioner, *Submission 11*, p.3.

131 Office of the Australian Information Commissioner, Proof Committee Hansard, 18 August 2014, p. 30.

Departmental and ASIO comments

The Department and ASIO note the importance of ASIO's cooperation with the private sector, as explained in the Explanatory Memorandum (paragraph 592).

In relation to privacy impact concerns, there are protections in place to ensure the privacy of information obtained through private sector cooperation, particularly personal information. Cooperation with private sector entities is limited to the purpose of ASIO's performance of its statutory functions under s 17 of the ASIO Act. Such cooperation will also be subject to the significant accountability framework under which ASIO operates. This includes independent oversight by the IGIS, who has the power to review ASIO's records and procedures when cooperating with the private sector. In addition, the Attorney-General's Guidelines under s 8A of the ASIO Act apply to any engagement between ASIO and the private sector. The Attorney-General may also, pursuant to s 19(1) of the ASIO Act, make arrangements or give directions in relation to ASIO's cooperation with the private sector. Such directions have been issued in relation to cooperation with State and Territory governments, law enforcement agencies and various courts under s 19 of the ASIO Act.

In light of the OIAC's comments, the Department and ASIO will assist the Government in considering whether any additional material could be provided in the Explanatory Memorandum. The OAIC comments will also be taken into account in any reconsideration of the Attorney-General's Guidelines (as referred to above under additional privacy related requirements in warrant provisions).

Schedule 4 – publication of identity of ASIO employee or ASIO affiliate

Submissions and evidence

Some submitters and witnesses argued that there should be circumstances in which the publication of the identity of an ASIO employee or an ASIO affiliate is permitted – for example, in connection with criminal proceedings initiated against such a person, or other forms of alleged misconduct or maladministration by such a person.[132]

Departmental and ASIO comments

The Department and ASIO do not support the consideration of any exceptions to the offence in s 92. The amendments to this provision are limited to implementation of recommendation 34 of the Committee's 2013 report concerning the ability of ASIO to refer suspected breaches of s 92 to law enforcement agencies. The absolute nature of the prohibition reflects that publicising the identity of an ASIO employee or an ASIO affiliate could have significant ramifications, including posing a threat to intelligence operations, in addition to risking the personal safety of the individual and persons connected to him or her. Given the potentially grave nature of these risks, it is necessary and appropriate that a penalty applies to such publication. It is important to bear in mind, however, that the offence is limited to the

132 Law Council of Australia, *Submission 13*, p. 46; Muslim Legal Network, *Submission 21*, p. 6.

making public of the identity of an ASIO employee or affiliate. As such, it does not preclude complaints about suspected maladministration or misconduct to the IGIS or internal reporting to the Director-General, or the ability of a person to report a suspected crime to the police in a manner that is intended to be confidential or in-confidence.

Schedule 5 – Intelligence Services Act amendments – Ministerial authorisation ground

Need for, and breadth of, the new ground

A small number of submitters and witnesses suggested that, contrary to recommendation 38 of the Committee's 2013 report, the proposed new ground of Ministerial authorisation in relation to the operational security of ASIS was unnecessary. This was largely said to be because there was overlap with the general 'security' ground, and complaints about perceived vagueness in the provision.[133]

While this is a matter for the Minister for Foreign Affairs, the Department and ASIO concur with the remarks of the IGIS that, although there may be overlap between grounds, it does not follow that this is necessarily problematic.[134] The objective is to ensure the availability of Ministerial authorisation grounds to address the circumstances identified in recommendation 28 of the Committee's 2013 report, while maintaining appropriate oversight and accountability arrangements.[135]

Privacy impact test

Submissions and evidence

The Law Council of Australia recommended that a privacy impact test should be applied to Ministerial authorisations by the Defence Minister for defence intelligence agencies to undertake activities in relation to the operational security of ASIS under the proposed new ground.[136]

Departmental and ASIO comments

While recognising that this issue is a matter for other agencies, the Department and ASIO do not support the adoption of a privacy impact test as part of the new Ministerial authorisation ground. This is consistent with previous comments in this submission in response to similar proposals in relation to ASIO's special powers in Division 2 of Part III of the ASIO Act. As noted in the submission of ASIS to the inquiry, a number of safeguards already apply in relation to the protection of privacy, which are incorporated in the requirements of s 9(1), which sets out the matters in respect of which the Minister responsible for the relevant agency must be satisfied. In addition, any intelligence produced may only be retained and

133 See, for example, Law Council of Australia, *Submission 13,* pp. 50-51 and Associate Professor Greg Carne, *Submission 5,* pp. 9-10.

134 Inspector-General of Intelligence and Security, *Submission 4,* p. 17.

135 See further, the submission of ASIS, *Submission 8,* p. 1.

136 Law Council of Australia, *Submission 13,* p. 51.

communicated in accordance with the rules to protect the privacy of Australians made by the responsible Minister under s 15 of the Intelligence Services Act.[137]

Schedule 5 – Intelligence Services Act amendments – ASIO cooperation with ASIS

Record keeping

Submissions and evidence

In her submission to the inquiry, the IGIS noted that the proposed amendments do not contain a requirement that ASIS maintain a register of Australian persons who are the subject of activity in response to an ASIO request under the new scheme.[138] To the extent that this comment may prompt the Committee to consider whether there would be value in recommending such a scheme, the Department and ASIO provide the following comments.

Departmental and ASIO view

While recognising that this is a matter for ASIS, the Department and ASIO acknowledge that good record keeping practices are important to effective oversight and accountability, and that the IGIS is of the view that oversight will be more complex as a result of the proposed amendments. However, to ensure the agility of the enhanced cooperative arrangements, it is preferable that record keeping of the kind identified in the IGIS's submission is undertaken as a matter of practice rather than being entrenched as a statutory obligation.

The Department and ASIO note the general record-keeping obligation in proposed s 13F(3), which requires copies of notices from ASIO to be kept by ASIS and available for inspection by the IGIS on request.

Accountability / demonstrated need for the amendments

A handful of submissions made general comments that, in their view, the need for the proposed enhanced cooperative arrangements in proposed s 13B was not established. There was some further suggestion that the proposed arrangements may undermine existing standards of accountability.

The Department and ASIO do not accept either suggestion, and refer to the submission of ASIS to this inquiry in relation to the operational need for the proposal and the applicable safeguards,[139] together with the findings of this Committee in its 2012-2013 inquiry in relation to recommendation 39 of its 2013 report.

---

137 ASIS, *Submission 8,* pp. 1-2. The matters in s 9(1) are: that any activities which may be done in reliance on the authorisation are necessary for the proper performance of a function of the agency; that 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 to ensure that the nature and consequences of acts done in reliance on the authorisation will be reasonable, having regard for the purposes for which they are carried out.

138 Inspector-General of Intelligence and Security, *Submission 4,* p. 19.

139 ASIS, *Submission 8,* p. 2 (operational need) and p. 3 (safeguards and oversight).

The amendments are required to streamline the legal authority for ASIS to collect intelligence on Australians relevant to security, to support ASIO in the performance of ASIO's functions. Collection by ASIS under these new provisions will only be in response to a notice from ASIO about ASIO's intelligence requirements, except where ASIS reasonably believes it is not practicable in the circumstances for ASIO to notify ASIS of ASIO's intelligence requirements. ASIS can currently assist ASIO in this manner but must obtain a Ministerial authorisation. In some circumstances, the relevant threshold for obtaining a Ministerial authorisation cannot be met and this prevents ASIS from assisting ASIO for the purpose of ASIO's security investigations.

The proposed amendments also address an existing risk with the current Ministerial authorisation regime, where ASIS could become aware of a serious threat to national security involving an Australian person but is not able to act quickly to seek further intelligence on that threat (for example, in the event of a possible terrorist attack) without first seeking a Ministerial authorisation.

Prescription of relevant activities, etc, in proposed s 13B

The Law Council of Australia considered that proposed s 13B should prescribe the kinds of activities that may be undertaken, a maximum duration of any cooperation, and the specific requirements for internal approvals and proposed renewals.

While recognising that this is a matter on which the Foreign Affairs portfolio would also need to comment, the Department and ASIO are of the view that specific details such as these are not suitable for inclusion in legislation, given that there may be significant variation across individual matters. Instead, these specifics are best addressed in the relevant notices, arrangements and guidelines that must be issued under ss 13B(1)(d), 13E and 13G – and in particular the s 13G Guidelines to be made jointly by the Attorney-General and Minister for Foreign Affairs in relation to the undertaking of activities under s 13B. In addition, the IGIS will also have oversight of the arrangements, including the ability to examine these specific matters.

In addition, the Department and ASIO note that the activities able to be undertaken in accordance with proposed s 13B are expressly limited by proposed s 13D to those activities in respect of which ASIO would not be required to obtain a warrant, if ASIO were to undertake those activities in Australia. This is a significant limitation on the types of activities that may be undertaken.

Schedule 5 – Intelligence Services Act amendments – clarification of DIGO functions

Submissions

One submitter argued that the Explanatory Memorandum inaccurately describes the proposed amendments to s 6B of the Intelligence Services Act as clarifications. These amendments implement recommendation 27 of the Committee's 2013 report, concerning the statutory functions of the Australian Geospatial-Intelligence Organisation (AGO), as renamed by Schedule 7 to the Bill from its previous name as the Defence Imagery and Geospatial Organisation (DIGO). It was suggested that these amendments could potentially be significant as they may allow for foreign intelligence entities to collect intelligence on Australians, or may enable AGO to assist such foreign entities in doing so. [140]

Departmental and ASIO comments

While recognising that these provisions are administered by the Minister for Defence (to the extent of their application to a Defence portfolio agency) the Department and ASIO are of the view that they are described accurately in the Explanatory Memorandum, consistent with recommendation 27 of the Committee's 2013 report and the supporting reasoning set out therein.

Schedule 6 – protection of information

Coverage of existing secrecy offences of general application

Submissions and evidence

Some submitters and witnesses argued that there is "no demonstrable need"[141] for the proposed new and amended offences in Schedule 6 to the Bill because the wrongdoing to which they are directed is covered adequately by existing secrecy offences of general application. The Gilbert + Tobin Centre of Public Law commented:

> [T]he government's claim that there are 'significant gaps' in the law is simply not supported. There is a wide range of existing offences that could apply to the disclosure of classified information, including severe penalties for terrorism, espionage and treason, as well as other penalties for disclosing official secrets and the disclosure of information by Commonwealth officers. And, contrary to the government's suggestion that 'no such offences exist', many of these offences would also apply to the situation where a person merely possesses or retains information. Section 79 of the Crimes Act provides for a maximum penalty of seven years imprisonment where a person retains a classified document 'when it is contrary to his or her duty to retain it'. Given this comprehensive array of existing offences, there is not demonstrable need to create a new 'three-tier structure' for regulating the disclosure of classified information.[142]

140 Muslim Legal Network, *Submission 21*, pp. 15-17.

141 Gilbert + Tobin Cente of Public Law, *Submission 13*, p. 14.

142 Gilbert + Tobin Centre of Public Law, *Submission 2*, pp. 13-14 (footnotes omitted). See also Proof Committee Hansard, 18 August 2014, p. 28. See further Law Council of Australia, *Submission 13*, pp. 52-53.

Departmental and ASIO comments

The material issue before the Committee and the Parliament is whether the particular wrongdoing sought to be targeted by the measures in Schedule 6 to the Bill is meritorious of being singled out for the imposition of a dedicated criminal sanction. That is, the Parliament is called upon to decide whether conduct that compromises, or places at risk of compromise, intelligence-related information ought to be the subject of specific criminal offences and penalties in the manner proposed by Schedule 6.

As the Attorney-General's remarks in his second reading speech on the Bill indicate, the Government has taken the view that intelligence-specific secrecy offences are needed to recognise the particular harm inherent in the compromise of intelligence-related information, which goes over and above the offences and penalties applying to the compromise of other types of official information of a confidential nature. The need for intelligence-specific secrecy offences was endorsed in 1976 by the Hope Royal Commission on Intelligence and Security, which led to the introduction of the unauthorised communication offence in s 18(2) of the ASIO Act. As Justice Hope commented in his Fourth Report:

> The intelligence held by ASIO … is often highly prejudicial … and its dissemination should be strictly controlled by legislation as well as ethical rules. The minimum controls which should be contained in the legislation are that the communication may only be made by the Director-General or by somebody authorised by him, either generally or in the particular matter; and that communication of any intelligence by an unauthorised person, or otherwise than for the purposes of the Act, should be prohibited. Persons who infringe these provisions or who authorise its infringement should be subject to severe penalties.
>
> It is true that legislation alone will not ensure that no-one with access to ASIO's intelligence speaks out of turn. But the least that must be done … is to prohibit and penalise it.[143]

The Attorney-General's second reading remarks, together with the commentary in the Explanatory Memorandum to the Bill, further outline the Government's view that there are significant gaps in the coverage of existing intelligence-specific secrecy offences in the contemporary security environment in two key respects – namely:

- the disproportionately low penalties (two years' imprisonment) applying to the existing offences in the ASIO Act and the Intelligence Services Act which target the unauthorised communication of intelligence-related information by persons to whom it is entrusted; and

- the absence of offences directed specifically to persons who place intelligence-related information at risk of compromise, but whose conduct stops short of communication of that information.

Accordingly, the material issue is not that a survey of existing criminal laws might identify various offences of general application that could potentially apply – in particular fact

143 Royal Commission on Intelligence and Security (1976), Fourth Report, Vol 1, pp. 116-117. In making these findings, the Royal Commission had regard to the official secrets and espionage offences (both then in Part VII of the Crimes Act 1914.)

scenarios – to the conduct constituting the proposed new or amended offences in Schedule 6. Rather, the focus of any useful analysis of existing offences is whether or not they adequately cover the particular form of wrongdoing sought to be addressed by those in Schedule 6. (That is, the compromising of intelligence-related information, or placing such information at risk of compromise.)[144]

As indicated in the Department's responses to the matters taken on notice at the hearing of 15 August, there are significant limitations in the range of existing secrecy offences of general application, insofar as they may apply to the unauthorised communication of intelligence-related information, or dealings with or the making of records of such information. Limitations in the key categories of general offences are discussed below.

Offences in the Criminal Code

The espionage offences in Division 91 of the Criminal Code require that a person must intend 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 they are directed to conduct which causes, or is intended to cause, harm of the gravest possible nature to Australia's security interests. They are not of application to the comparatively lesser, but still highly significant, degree of harm or risk that may be occasioned by unauthorised communication of intelligence-related information, or unauthorised dealings with records or recording of information, in the absence of a specific intent to cause harm. (Further issues in relation to a specific harm requirement are considered separately below.)

Similarly, while some submitters have suggested that other offences such as treason (s 80.1) and materially assisting enemies (s 80.1AA) and a range of terrorism offences in Part 5.3 may potentially be relevant,[145] their application is limited to very specific fact scenarios. They do not squarely address the wrongdoing to which the Schedule 6 offences are directed.

Offences in the Crimes Act – Part VII

Some submissions to the inquiry have also suggested that adequate coverage is provided by offences in s 79 of the Crimes Act, which are directed to the disclosure of official secrets.[146] 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);

144 To this end, the comments in Submission 2 quoted above might fairly be described as a misrepresentation of the remarks in the Attorney-General's second reading speech.

145 See, for example, Gilbert + Tobin Centre of Public Law, *Submission 2*, attachment 1.

146 Gilbert + Tobin Centre of Public Law, *Submission 2*, p. 12; Proof Committee Hansard, 18 August 2014, p. 28.

- 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.

It is considered, however, that the maximum penalties applying to these offences are disproportionately low to the wrongdoing targeted by the offences in Schedule 6. (The issue of penalties is discussed separately below.)

Elements of the offences and penalties

Submissions and evidence

Some submitters and witnesses were critical of the elements of and penalties applied to the proposed offences in the following respects:

- The absence of a requirement to prove that the person intended to cause harm, or that the conduct did in fact or was likely to cause harm, to security.[147]

- The proposed penalties, particularly those applying to the unauthorised communication offences, are higher than those applying to existing secrecy offences of general application.[148]

- The application of the offences to a person who is in an "agreement or an arrangement" with an intelligence agency, notwithstanding that such a person may not "understand the special responsibilities associated with handling classified information to the same degree as intelligence employees".[149]

Details of these criticisms, together with the Department and ASIO's comments are set out below.

147 Gilbert + Tobin Centre of Public Law, *Submission 2*, pp. 12, 13; Law Council of Australia, *Submission 13*, pp. 53, 54, 55.

148 Gilbert + Tobin Centre of Public Law, *Submission 2*, p. 12. See also Law Council of Australia, *Submission 13*, pp. 52-53.

149 Gilbert + Tobin Centre of Public Law, *Submission 2*, p. 13.

Harm requirement

Submissions and evidence

Some submitters argued that criminal liability should not be enlivened unless a person intended to cause harm in making the disclosure. It was argued that a breach of a non-disclosure obligation was not, of itself, an appropriate basis for imposing criminal liability. As such, it was suggested that all of the proposed offences in Schedule 6 should include an additional element that the person who engaged in the unauthorised conduct intended to cause some form of harm, or was aware that some form of harm was the likely result of his or her conduct.[150]

For example, it was suggested that the unauthorised communication offences should require the prosecution to prove that the person intended to cause prejudice to national security. It was further suggested that the unauthorised dealing offences should require the prosecution to prove that the person know that his or her conduct would be likely to result in the communication of intelligence-related information to another person.[151]

It was asserted that this approach would be consistent with a recommendation of the Australian Law Reform Commission (ALRC) in its 2009 report on *Secrecy Laws and Open Government in Australia.* Submitters referred to ALRC recommendation 5-1 that a general secrecy offence should be enacted, which requires proof that the disclosure of Commonwealth information did, or was reasonably likely to, cause a specified form of harm, including damage to the security, defence or international relations of the Commonwealth.[152] (The ALRC relevantly made a further recommendation that 'security' should be defined by reference to s 4 of the ASIO Act).[153]

However, these submitters did not appear to acknowledge that this recommendation was directed to the ALRC's proposal for a general secrecy offence, and that the ALRC also made specific findings and recommendations about secrecy offences in relation to intelligence information (being that which is obtained or generated by or on behalf of Australian Intelligence Community agencies). In relation to this more specific category of information, the ALRC considered that there was not an imperative to require proof of harm, or intent to cause harm, as an element of the offences, on the basis that the harm is implicit.[154]

150 Gilbert + Tobin Centre of Public Law, *Submission 2*, p. 12; Law Council of Australia, *Submission 13*, pp. 52-55.

151 Gilbert + Tobin Centre of Public Law, *Submission 2*, p. 13. See further: Law Council of Australia, *Submission 13*, pp. 52-55.

152 Gilbert + Tobin Centre of Public Law, *Submission 2*, p. 12; Proof Committee Hansard, 18 August 2014, p. 28.

153 ALRC Report 112, recommendation 5-2.

154 ALRC Report 112, p. 289 at [8.65] and recommendation 8-2 at p. 307.

It was further argued by some submitters that the penalties applying to the offences in Schedule 6 – particularly the proposed 10-year penalties for the unauthorised communication offences – were sufficiently high as to justify the inclusion of a harm element.[155]

Departmental and ASIO comments

The Department and ASIO strongly oppose the inclusion of an additional element in any of the offences in Schedule 6 that would require the prosecution to prove that the person intended to cause harm by engaging in the relevant unauthorised conduct, or that the unauthorised conduct was likely to cause harm.

The Department's responses to the matters taken on notice at the Committee's hearing on 15 August in relation to the offences in proposed s 35P (in relation to special intelligence operations) apply equally to the proposed new and amended offences in Schedule 6. The wrongdoing to which the offences are directed is the harm inherent in the disclosure, or placing at risk of compromise, information of a highly sensitive nature. This harm is not contingent on a person's motivation, except that it may be aggravated by persons who act with a malicious intention.

Accordingly, it is appropriate that the harm occasioned by the conduct constituting an offence against Schedule 6 is taken into account on sentencing, in accordance with ordinary principles, and not in the adjudication of guilt. The proposed maximum penalties applying to the offences – particularly those concerning the unauthorised communication of information – have been designed to reflect this.

In addition, the Department and ASIO reject suggestions that the very concept of criminalising the contravention of a non-disclosure obligation is problematic unless accompanied by an element requiring proof of harm or likely harm, or an intent to cause harm. The better view is – as recognised by Justice Hope in the Royal Commission on Intelligence and Security – that the criminal law can, and should, be used to hold persons who are entrusted with information of the most sensitive kind to a high standard in relation to its proper use.[156]

As the ALRC also acknowledged in its 2009 secrecy report, "specific secrecy offences relating to intelligence and security agencies which do not include an express harm requirement place a higher duty on members of those agencies, in recognition of the sensitivity of the information they handle, and the higher duties of secrecy associated with

155 Gilbert + Tobin Centre of Public Law, *Submission 2*, p. 12.

156 This view was also held by the Gibbs Review of Commonwealth Criminal Law, in which that review committee, chaired by the Hon Sir Harry Gibbs, concluded that "undoubtedly, a member of the intelligence and security services stands in a special position and it is not unreasonable … that he or she should be subject to a lifelong duty of secrecy as regards information obtained by virtue of his or her position … [D]isclosures by such persons should be prohibited by criminal sanctions without proof of harm.": *Review of Commonwealth Criminal Law: Final Report* (1991), p. 323.

their work". On this basis, the ALRC agreed that it is "appropriate for people in this position to be subject to higher responsibilities to protect inherently sensitive information".[157]

Comparison of penalties

Submissions and evidence

Some submitters appeared to suggest that the penalties applying to the proposed offences in Schedule 6 are too high because they "far exceed" those applying to secrecy offences of general application.[158] (For example, it was noted that the offence in s 79(2) of the Crimes Act in relation to the unauthorised disclosure of official secrets with intent to prejudice the security or defence of the Commonwealth carries a maximum penalty of seven years' imprisonment. This is in contrast to the proposed 10-year maximum penalty in relation to the unauthorised communication offences in the ASIO Act and the Intelligence Services Act. Additionally, the unauthorised retention offence in s 79(4) of the Crimes Act carries a maximum penalty of six months' imprisonment, compared to a proposed maximum penalty of three years' imprisonment for the offences in relation to the unauthorised dealing with intelligence-related information.)

Departmental and ASIO comments

The rationale for the penalty structure is set out in considerable detail in the Explanatory Memorandum to the Bill. In particular, the rationale for the 10-year maximum penalty for the unauthorised communication offences is as follows:

> 680. Given the potentially devastating consequences of the unauthorised disclosure of security intelligence-related information, it is appropriate that the maximum penalty applying to subsection 18(2) is of a sufficient magnitude to communicate clearly the gravity of the wrongdoing involved and Parliament's strong expectation that persons to whom intelligence and national security-related information is entrusted will handle that information lawfully at all times.
>
> 681. A maximum penalty of 10 years' imprisonment gives effect to the policy objective of recognising and communicating the gravity of the wrongdoing inherent in the unauthorised communication of intelligence information, and establishing a strong deterrent to such conduct. In particular, the penalty reflects an appropriate gradation with that applying to the espionage offences in Division 91 of the Criminal Code 1995 (Criminal Code), which is 25 years' imprisonment.
>
> 682. The higher penalty applying to espionage offences in the Criminal Code reflects that these offences contain additional elements to those in subsection 18(2) of the ASIO Act. Namely, the espionage offences require proof of a person's intent to cause certain harm to Commonwealth interests, and proof that the person's conduct resulted in, or was likely to result in, the communication of information to another country or a foreign organisation.
>
> 683. In contrast, the conduct constituting an offence under subsection 18(2) of the ASIO Act is less culpable than that constituting the offence of espionage because it does not require a person to form a specific intention that a particular unauthorised communication should cause harm, and nor does it require proof that a foreign government or organisation was the recipient, or likely recipient, of an

157 ALRC Report 112, p. 283 at [8.42] and p. 289 at [8.62].

158 Gilbert + Tobin Centre of Public Law, *Submission 2*, p. 12. See also Law Council of Australia, *Submission 13*, p. 52.

> unauthorised communication. Rather, the wrongdoing inherent in an offence against subsection 18(2) of the ASIO Act is the unauthorised communication of information which is, by definition, of a sensitive nature and carries a high risk of harming national security interests. That is, information which is acquired or prepared by or for the Organisation in connection with the performance of its statutory functions, or information which relates to the performance by the Organisation of its functions.

The rationale for the three-year maximum penalty for the unauthorised dealing offences and unauthorised recording of information offences is as follows:

> 731. The offence in new subsection 18A(1) *[unauthorised dealing]* is subject to a maximum penalty of imprisonment for three years. This gives effect to a policy intention that the conduct constituting the offence is less culpable than the conduct constituting an offence against subsection 18(2) (which is increased to 10 years' imprisonment by item 1 of this Schedule). This gradation of penalties reflects that the wrongdoing targeted by subsection 18A(1) is the placing of security intelligence-related information at risk of unauthorised communication, while the wrongdoing targeted by subsection 18(2) is the unauthorised communication of such information.
>
> 732. The maximum penalty of three years' imprisonment is an appropriate deterrent to the conduct constituting an offence against subsection 18A(1), by communicating clearly an expectation that persons who are entrusted with access to records of the Organisation in the course of their official duties are held to a high standard in relation to the handing and use of those records. This penalty is further consistent with the established principle of Commonwealth criminal law policy, documented in the Guide to Framing Commonwealth Offences, Infringement Notices and Enforcement Powers, that a heavier penalty is appropriate where the consequences of the offence are particularly dangerous or damaging. Criminal conduct which carries a significant risk of jeopardising Australia's national security, by placing at risk the confidentiality of intelligence-related information, is one such instance of particularly dangerous or damaging conduct.
>
> 733. Accordingly, it is appropriate that the offence in subsection 18A(1) is subject to a higher maximum penalty than other statutory secrecy offences that do not specifically target conduct which creates a significant risk that security intelligence information may be compromised. For example, a number of other secrecy offences, such as that in section 70 of the Crimes Act 1914, are subject to a maximum penalty of two years' imprisonment.

The Department and ASIO consider that, given the broad scope of application of non-intelligence specific Commonwealth secrecy laws – and the specific wrongdoing to which intelligence-specific secret offences are targeted – greatest weight should be placed on a coherent penalty structure for intelligence-specific offences rather than across the Commonwealth statute book.

Application of offences to persons in an 'agreement or arrangement'

Submissions and evidence

Some submitters further argued that the offences should be limited to employees of an intelligence agency or those engaged under a contract. It was suggested that persons who are subject to an "agreement or an arrangement" may not understand the special responsibilities

associated with handling classified information. Alternatively, it was suggested that the offences could apply lesser penalties to such persons.[159]

Departmental and ASIO comments

Suggestions along the lines of those outlined above are, in the Department and ASIO's view, without merit. Such proposals would create an arbitrary distinction between categories of persons to whom sensitive information is entrusted, on the basis of the nature of the instrument through which their relationship with the relevant intelligence agency is established. (For example, a person who is engaged under a contract, and a person who is subject to an agreement or arrangement, may have legitimate access to the same information, and might have identical non-disclosure obligations. There is no logical basis on which to require, as a matter of law, that a lesser maximum penalty should apply to the persons subject to an agreement or an arrangement.)

In addition, the prosecution must prove, in all offences, that a person engaged in the relevant conduct without authorisation. As this physical element is a circumstance, the standard fault element of recklessness applies by reason of ss 5.4 and 5.6 of the Criminal Code. The prosecution must prove that a person was aware of a substantial risk that his or her conduct was not authorised, and that he or she nonetheless and unjustifiably in the circumstances took the risk by engaging in the relevant conduct (such as by communicating the information, or dealing with the record). A person's degree of understanding of their obligations will be directly relevant to an assessment of whether a person was reckless in relation to authorisation.

Exemptions / Interaction with the Public Interest Disclosure Act 2013

Submissions and evidence

Some submitters and witnesses commented that the disclosure regime in the PID Act is very limited, and provides "virtually no protection for intelligence employees who disclose information obtained in the course of their duties (even where such a disclosure would involve gross misconduct or unlawful activities in which an intelligence agency was involved)."[160] A range of exceptions to the offences or extensions of the PID Act were proposed.[161]

Departmental and ASIO comments

Subject to consideration of the matters raised by the IGIS about the making of complaints, the conduct of inspections and the sharing of information within the Office of the IGIS, the Department and ASIO support the scope of the offences and the PID Act as drafted, for the

159 Gilbert + Tobin Centre of Public Law, *Submission 2*, p. 13.

160 Gilbert + Tobin Centre of Public Law, *Submission 2*, p. 13. See also Law Council of Australia, *Submission 13*, p. 52.

161 Gilbert + Tobin Centre of Public Law, *Submission 2*, p. 13; Professor AJ Brown, *Submission 19*, especially at pp.3-4;

reasons discussed in relation to proposed s 35P above. With specific reference to the inability of intelligence employees to make public disclosures under the PID Act, the Department and ASIO note that the limitations do not extend to internal disclosures (including those to the IGIS, as an independent and external oversight mechanism). Limits on public disclosure of intelligence information are within the permitted restrictions provided for in Article 19(2) of the International Covenant on Civil and Political Rights for the protection of national security and public order.

Suggestions for further review of the Bill

Submissions and evidence

Some submitters argued that the Bill should be referred to the Independent National Security Legislation Monitor (INSLM) for review before it is voted upon by the Parliament. This was suggested because the INSLM was identified in recommendation 41 of the Committee's 2013 report as one of the persons the Committee considered should be consulted on a draft Bill. It was also argued by some submitters that a further review of the Bill is needed to enable a more detailed analysis of its provisions (including further examination of operational need), and that this task should be undertaken by a person independent of the Government and the Parliament.[162]

Departmental and ASIO comments

The Department and ASIO note that the Government has supported the intent of recommendation 41 of the Committee's 2013 report that the Bill should be the subject of scrutiny and consultation. The Government has implemented this primarily by the referral of the Bill to this Committee, given its considerable background to the relevant measures.

Consistent with s 6 of the *Independent National Security Legislation Monitor Act 2010* (INSLM Act), the mandate of the INSLM is to review the operation of counter-terrorism and national security legislation that has been passed by the Parliament, and to provide advisory recommendations on its continued necessity and appropriateness. As such, the Office of the INSLM is not designed to be a source of policy advice on proposed legislation. (In addition, as the Office of the INSLM has been vacant since 20 April 2014 and a new appointment has not been announced, it was not possible to undertake any such consultations on a draft Bill.)

The Government has elected to put the Bill through the normal processes of Parliamentary scrutiny, including via the Committee inquiry system. Parliamentary scrutiny has proven rigorous in relation to, and has played an important role in the development of, all major pieces of national security legislation introduced and passed to date.

The Department and ASIO further note that the Committee has, in addition to the conduct of its 2013 inquiry, received a number of detailed submissions and taken evidence at multiple

162 Law Council of Australia, *Submission 13*, p. 7. See also Australian Lawyers' Alliance, *Submission 7*, p. 7 (comments on perceived limitations in Parliamentary Committee review in relation to anti-terrorism and intelligence legislation).

hearings. This has included the examination of relevant operational issues in private session. In the event that the Committee would like further information about the intended use or operation of the proposed measures in the Bill, the Department and ASIO would be pleased to provide any additional evidence required in private session in the course of its inquiry.

In the event that the Bill is passed, the operation of the relevant Act could be examined by a future INSLM in accordance with s 6(1)(a)(ii) of the INSLM Act. This provision enables the examination of "any other law of the Commonwealth to the extent that it relates to Australia's counter-terrorism and national security legislation," (noting that the Acts or parts of the Acts proposed to be amended by the Bill are not within the definition of 'counter-terrorism and national security legislation' in s 4 of the INSLM Act).

Concluding remarks

The Department and ASIO welcome the Committee's thorough consideration and constructive scrutiny of the measures proposed in the Bill, together with the contributions of submitters and witnesses participating in the inquiry. The Department and ASIO will assist the Government in considering the Committee's recommendations and findings, and would be pleased to provide the Committee with any further information it may require in completing its inquiry into this important package of proposed reforms.

Attachment 1

Not included in unclassified submission

Attachment 2

Summary of key differences:
special intelligence operations (proposed new Division 4 of Part III of the *ASIO Act 1979*) and
controlled operations (Part IAB of the *Crimes Act 1914*)

Issue	Special Intelligence Operations	Controlled Operations	Explanation of differences.
Definition of relevant scheme	Special intelligence operation (s 4) is defined as an operation: (a) in relation to which an authority has been granted under s 35C; (b) that is carried out for a purpose relevant to the performance of one or more special intelligence functions *(Defined in s 4 as those of the Organisation's statutory functions in s 17 that pertain to intelligence collection – paras (a), (b), (e) and (f).)* (c) that may involve an ASIO employee or an ASIO affiliate in special intelligence conduct.	Controlled operation is defined in s 15GD(1) as an operation involving: • participation of law enforcement officers; • for the purpose of obtaining evidence that may lead to the prosecution of a serious offence; and • may involve a law enforcement officer in conduct that would, apart from the immunity for liability provided under the controlled operations provisions, constitute an offence. Also uses an additional term of 'major controlled operation' which relates to operations involving more serious conduct – infiltration of criminal group for more than 7 days; an operation for	Differences reflect the different purposes to which the schemes are directed (intelligence v law enforcement). A different scheme for 'major special intelligence operations' involving more 'serious' matters is not necessary because the special intelligence functions in s 17(1)(a), (b), (e) and (f) are by definition serious. This is in contrast to criminal offences which cover a wide spectrum of conduct.

Issue	Special Intelligence Operations	Controlled Operations	Explanation of differences.
Definition of relevant scheme (continued)		more than three months; or directed to criminal conduct that includes a threat to life. (Special authorisation requirements apply to such operations, mainly to do with the level of authorisation – AFP Commissioner.)	
Admissibility of evidence obtained in an authorised operation	**Proposed s 35A**: Division not intended to limit judicial discretion in relation to the admission of evidence or staying criminal proceedings, other than to clarify that evidence gathered as part of a special intelligence operation should not be automatically disregarded because it involved (authorised) conduct that attracted the immunity from criminal liability in s 35K and would otherwise have constituted an offence.	Same approach is taken in s 15GA.	N/A
Authorising person	Authorising officer (s 4) is the DG or a DDG. May grant an authority under s 35C on application from an ASIO employee under s 35B. Authorising officer can also vary and cancel authorities: ss 35F, 35G.	**Authorising officers are senior law enforcement officials** – eg, AFP Commissioner/Deputy Commissioner/approved Senior Executive: s 15GF. However, a nominated AAT member must authorise extensions of operations beyond 3 months: ss 15GG; Subdiv C of Div 2	**Extensions of time – external authorisation** ASIO's SIOs are an exclusively internal authorisation scheme (including for variations involving an extension of time within the 12 month maximum). This is considered appropriate having regard to the security intelligence purpose of operations.

Issue	Special Intelligence Operations	Controlled Operations	Explanation of differences.
Issuing criteria	**Proposed s 35C(2):** Authorising officer must be satisfied on reasonable grounds of the following: (a) Matter will assist the Organisation in the performance of one or more 'special intelligence function'. *[Defined in s 4 as ASIO's intelligence collection, but not advisory, functions under ss 17(1)(a), (b), (e) and (f).]* (b) circumstances are such as to justify the conduct of an SIO. (c) any unlawful conduct will be limited to the maximum extent consistent with conducting an effective SIO. (d) the SIO will not be conducted in such a way that a person is likely to be induced to commit an offence they would not otherwise have intended to commit. (e) any conduct involved will not cause death/serious injury to any person, involve the commission of a sexual offence, result in a significant loss of, or serious damage to, property. In addition, an authority cannot authorise conduct for which ASIO would require a warrant: s 35L	**Section 15GI(2):** Authorising officer must be satisfied on reasonable grounds of the following: • commission / likely commission of serious offence • nature and extent of suspected criminal activity is such to justify controlled operation • any unlawful conduct is limited to the maximum extent consistent with conducting an effective controlled operation. • proposed controlled conduct will be capable of being accounted for in accordance with reporting/oversight arrangements in Div 4 • operation will not involve conduct in the nature of entrapment, serious offences against the person, serious loss or damage to property.	**Issuing criteria are broadly similar but have some necessary differences**, given the different purposes to which these operations are put (intelligence v law enforcement, noting the latter has a focus on evidence collection in relation to an offence). For this reason it is not possible for ASIO to simply participate in a controlled operation as an alternative to a designated scheme for the protection of covert intelligence-only operations from liability.
Applications for authority	**Proposed s 35B** ***Applicant:*** Applications may be made by an ASIO employee (not an affiliate). ***Manner and form:*** Must be in writing and	Broadly similar requirements: written application by law enforcement officer to authorising officer: ss 15GH.	N/A.

Issue	Special Intelligence Operations	Controlled Operations	Explanation of differences.
Applications for authority (continued)	signed, unless urgent (below). ***Urgent applications:*** If applicant reasonably believes that the delay caused may be prejudicial to security, may make an oral application, or an application by other means of communication. If an application is made urgently, the applicant must make and provide to the authorising officer a written record of the application as soon as practicable after making it. ***No bar on multiple applications:*** applications can be made in relation to proposed operations that have been the subject of a previous application.		
Issuing of authority	**Conditional authorisations** ***Proposed s 35C(3)*** Authorisation may be granted on such conditions as authorising officer sees fit. **Manner and form requirements** ***Proposed s 35C*** Authority must be in writing and signed unless urgent. **Urgent authorisations** ***Proposed ss 35C(4) and (5)*** If authorising officer reasonably believes the delay caused by giving a written authority may	Broadly similar requirements: s 15GI	N/A

Issue	Special Intelligence Operations	Controlled Operations	Explanation of differences.
Issuing of authority (continued)	be prejudicial to security, authority can be issued verbally or by any other means of communication. **No bar on multiple authorities** ***Proposed s 35C(6)*** An authority may be granted in respect of an operation that has been the subject of a previous authority. **Authorities /records of urgent authorities not legislative instruments** ***Proposed s 35C(7)*** This means they are not subject to registration or disallowance.		
Contents of authority	**Proposed s 35D** Authority must specify: (a) how the SIO will assist in the performance of one or more special intelligence functions (b) identify the persons authorised to engage in special intelligence conduct (that which would otherwise attract criminal or civil liability) (c) state a general description of the nature of special intelligence conduct that authorised persons may engage in (d) specify the period of operation, within a	Broadly similar requirements: ss 15GK, 15GL.	N/A

Issue	Special Intelligence Operations	Controlled Operations	Explanation of differences.
Contents of authority (continued)	maximum of 12 months. (e) specify any conditions to which authority is subject. (f) state date and time of granting. A person is sufficiently identified if they are specified by an assumed name or a code name or number, as long as the authorising officer can match the assumed name etc to the person's identity.		
Duration and commencement	**Duration:** Maximum of 12 months: s 35D(1)(d). Effective for the period specified in the authorisation within this maximum, unless cancelled or period varied under s 35F (still within total maximum of 12 months): s 35E. **Commencement:** at time authorisation granted: s 35E.	Duration is three months (extendable, by authorisation of a AAT member) in increments of up to three months, within a 24 month cap: s 15GH(4)(c) and Subdivision C of Div 2. Commencement is at the time authorisation is granted: s 15GN.	**Different durations reflect different purposes to which SIOs and controlled operations are put**. Intelligence operations typically run over a longer period of time. Necessary to tailor duration to operational need.
Variation	**Proposed s 35F:** Authorising officer may vary at any time, on own initiative or application of ASIO employee. **Criteria for variation: ss 35E(4)-(5)** Authorising officer must be satisfied on reasonable grounds that the SIO as varied will assist the Organisation in the performance of one or more special intelligence functions, and	Variation (other than extensions of duration) can be made by an authorising officer on application or on own initiative: s 15GO. Some differences: • specific list of matters which can be varied – eg, adding or removing participants / conduct: ss (2)	Differences in limitations on variations reflect different purpose of SIO scheme compared to controlled operations.

Issue	Special Intelligence Operations	Controlled Operations	Explanation of differences.
Variation (continued)	must consider it appropriate to vary the authority. Variation of duration cannot exceed the maximum period of 12 months. **Multiple and urgent variations are permitted:** ss 35E(6), (7).	• variations cannot be made to urgent authorities: ss (3) • requirement that authorising officer must be satisfied on reasonable grounds that the variation will not authorise a significant alteration of the nature of the controlled operation concerned: ss (5).	
Cancellation	Authorising officer may cancel at any time for any reason: s 35G. Cancellation must be in writing and specify when it takes effect.	Same approach taken in s 15GY.	N/A
Effect of authority	**Proposed s 35H** Authorises each person to engage in the relevant special intelligence conduct as specified in authority, for the relevant period of effect unless cancelled or varied.	Same approach taken in s 15GZ.	N/A
Immunity / protection from liability	**Proposed s 35K:** Immunity from criminal and civil liability in respect of special intelligence conduct (being authorised conduct, by authorised participants). Exclusion of conduct that causes death, serious injury or significant loss or property damage. Also excludes conduct in the nature of 'entrapment', and that which involves commission of a sexual offence. **Proposed s 35N:** Immunity for conduct ancillary to authorised special intelligence	Immunity from criminal liability (s 15HA), but only indemnifies participants from civil liability (so the Cth is still potentially liable) (s 15HB). Corresponding immunity from criminal liability for ancillary conduct: s 15HE.	**Different treatment of civil liability.** Indemnity not appropriate in relation to SIOs, due to importance of maintaining covert nature of SIOs. IGIS's oversight power, including to recommend payment of compensation, is considered an adequate remedy. An immunity is also consistent with s 14(1) of the IS Act (which provides an immunity for IS Act agency staff members and agents from civil and

Issue	Special Intelligence Operations	Controlled Operations	Explanation of differences.
Immunity / protection from liability (continued)	conduct (eg, immunity from prosecution for a conspiracy or aiding/abetting offence for assisting a participant). The person engaging in the ancillary conduct must believe that he or she was doing so for the purpose enabling a participant in an SIO to engage in authorised special intelligence conduct.		criminal liability in respect of acts done in the proper performance of the agency's functions).
Defects in authority	**Proposed s 35J** Defect in authority or variation will not invalidate it, unless it relates to a material particular.	Same approach taken in s 15H.	N/A
Effect of being unaware of variation / cancellation	**Proposed s 35M** Immunity from legal liability applies to participants who act in accordance with an authority that is are unaware of a cancellation or variation of authority, and are not reckless as to the existence of a variation or cancellation.	Same approach taken in s 15HD.	N/A
Offences – unauthorised disclosure of information	**Proposed s 35P** **Offences / penalties** • Basic offence – person intentionally discloses information, reckless as to the circumstance that it relates to an SIO.	**Offences / penalties** Non-disclosure offences identical, but penalty is lower for the basic offence (two years' imprisonment): ss 15HK(1) (basic offence) and 15HL (aggravated	**Differences in penalties** are to ensure that SIO offences maintain parity with penalties for other offences in the ASIO Act, which reflect the significant risks to security (and life and safety of participants) that unauthorised

Issue	Special Intelligence Operations	Controlled Operations	Explanation of differences.
Offences (continued)	Penalty: 5 years' imprisonment. • Aggravated offence – the person making the disclosure intends to endanger the health or safety of a participant or prejudice the effective conduct of an SIO ; or the disclosure has that result. Penalty: 10 years' imprisonment. **Exceptions** • disclosures in connection with administration or execution of SIO scheme • for the purposes of legal proceedings arising out of or otherwise related to the SIO scheme, or any report of proceedings • in accordance with requirements imposed by law. • in connection with performance of functions or duties, or in the exercise of powers of the Organisation. [Note: exceptions to statutory secrecy offences may apply under the PID Act.] **Extended geographical jurisdiction:** Category D per s 15.4 of the Criminal Code. *(Offences apply to any person whether or not an Australian Citizen or resident; conduct anywhere in the world; whether or not that conduct has an equivalent in the local laws of another country in which it is engaged.)*	offence) **Exceptions** The offences have an additional exception for reporting suspected misconduct, in good faith, to the Ombudsman or ACLEI: ss 15HK(3) and 15HL(3). **No extended geographical jurisdiction** (no express provision, therefore standard geographical jurisdiction applies under the Criminal Code.)	disclosures of information can cause. **Absence of an express exception for whistleblowers in SIOs** is because the PID Act provides for this (immunity from secrecy offences for disclosures authorised under that Act. In the case of intelligence agencies, this is a disclosure to the agency head and IGIS. (The relevant offences in the Crimes Act were inserted in 2010 and pre-dated the PID Act of 2013.) **Absence of extended geographical jurisdiction:** extended geographical jurisdiction is necessary for the ASIO Act offences to accommodate the possibility that foreign persons may be involved in operations. It is appropriate that they should be liable for unauthorised disclosures in relation to an SIO after leaving Australia.

Issue	Special Intelligence Operations	Controlled Operations	Explanation of differences.
Reporting / oversight Reporting / oversight	**Proposed s 35Q** DG must report six monthly on each operation to the AG and DG (or once at the end of an operation for less than six months). Reports must address how the SIO has, during the relevant period, assisted the Organisation in the performance of a special intelligence function. **Amendments to annual reporting requirement: proposed s 94(2A)** The Organisation's annual reports must also address the total number of applications and authorities granted in a reporting year	**Division 4 of Part 1AB (ss 15HM-15HY)** sets out a detailed scheme for the keeping of a register of authorities, and specific investigative and reporting powers for the Ombudsman (including a requirement that the Ombudsman submit annual reports). This is additional to a requirement that the chief officer must submit six monthly reports to the Minister and Ombudsman.	It is not necessary to have a specific IGIS reporting regime because the IGIS's general powers of inquiry under the IGIS Act are considered adequate to cover SIOs. The IGIS was agreeable to this approach in consultations on the draft Bill.
Evidentiary certificates	**Proposed s 35R** An authorising officer may issue a prima facie evidentiary certificate, setting out such facts as the authorising officer considers relevant with respect to the granting of an authority.	**Similar provision in s 15HZ –** an authority is (prima facie) evidence that the authorising officer was satisfied of the relevant facts required to grant the authority.	N/A.
Compensation for loss/damage	No express provision.	**Section 15HF:** Commonwealth is liable to pay compensation for loss or serious property damage as a direct result of controlled operation. (Either by agreement or by court order in default of agreement.)	An express provision in relation to the payment of compensation was not considered necessary because the IGIS has discretion to recommend the payment of compensation. An obligation to pay compensation may jeopardise the confidentiality of operations.

Issue	Special Intelligence Operations	Controlled Operations	Explanation of differences.
Notification requirements	No notification requirements.	**Section 15HG:** loss or serious damage or personal injury must be reported to chief officer of relevant law enforcement agency, who must take all reasonable steps to notify the owner of the property / notify the person injured that the injury occurred in the course of a controlled operation. Exception for disclosures considered to compromise the operation or endanger life or safety, prejudice legal proceedings or otherwise be contrary to the public interest.	Notification requirement not included in special intelligence operation provisions because it would jeopardise operations. However consideration could be given to an IGIS notification requirement.