SENATE STANDING COMMITTEE

FOR THE

SCRUTINY OF BILLS

TWELFTH REPORT

OF

2014

24 September 2014

ISSN 0729-6258

Members of the Committee

Current members

Senator Helen Polley (Chair)	ALP, Tasmania
Senator John Williams (Deputy Chair)	NATS, New South Wales
Senator Cory Bernardi	LP, South Australia
Senator the Hon Bill Heffernan	LP, New South Wales
Senator the Hon Kate Lundy	ALP, Australian Capital Territory
Senator Rachel Siewert	AG, Western Australia

Secretariat

Ms Toni Dawes, Secretary
Mr Gerry McInally, Acting Secretary
Mr Glenn Ryall, Principal Research Officer
Ms Ingrid Zappe, Legislative Research Officer

Committee legal adviser

Associate Professor Leighton McDonald

Committee contacts

PO Box 6100
Parliament House
Canberra ACT 2600
Phone: 02 6277 3050
Email: scrutiny.sen@aph.gov.au
Website: http://www.aph.gov.au/senate_scrutiny

Terms of Reference

Extract from **Standing Order 24**

(1) (a) At the commencement of each Parliament, a Standing Committee for the Scrutiny of Bills shall be appointed to report, in respect of the clauses of bills introduced into the Senate or the provisions of bills not yet before the Senate, and in respect of Acts of the Parliament, whether such bills or Acts, by express words or otherwise:

(i) trespass unduly on personal rights and liberties;

(ii) make rights, liberties or obligations unduly dependent upon insufficiently defined administrative powers;

(iii) make rights, liberties or obligations unduly dependent upon non-reviewable decisions;

(iv) inappropriately delegate legislative powers; or

(v) insufficiently subject the exercise of legislative power to parliamentary scrutiny.

(b) The committee, for the purpose of reporting on its terms of reference, may consider any proposed law or other document or information available to it, including an exposure draft of proposed legislation, notwithstanding that such proposed law, document or information has not been presented to the Senate.

(c) The committee, for the purpose of reporting on term of reference (a)(iv), shall take into account the extent to which a proposed law relies on delegated legislation and whether a draft of that legislation is available to the Senate at the time the bill is considered.

SENATE STANDING COMMITTEE FOR THE SCRUTINY OF BILLS

TWELFTH REPORT OF 2014

The committee presents its *Twelfth Report of 2014* to the Senate.

The committee draws the attention of the Senate to clauses of the following bills which contain provisions that the committee considers may fall within principles 1(a)(i) to 1(a)(v) of Standing Order 24:

Competition and Consumer Amendment (Industry Code Penalties) Bill 2014

Introduced into the House of Representatives on 17 July 2014
The bill passed both Houses on 4 September 2014
Portfolio: Treasury

Introduction

The committee dealt with this bill in *Alert Digest No. 10 of 2014*. The Minister responded to the committee's comments in a letter dated 1 September 2014. A copy of the letter is attached to this report.

Alert Digest No. 10 of 2014 - extract

Background

This bill amends the *Competition and Consumer Act 2010* to:

- allow regulations to be made that prescribe a pecuniary penalty not exceeding 300 penalty units for the breach of a civil penalty provision of an industry code; and

- allow the Australian Competition and Consumer Commission to issue an infringement notice where it has reasonable grounds to believe a person has contravened a civil penalty provision of an industry code.

Delegation of legislative power
Schedule 1, item 5, proposed subsection 51AE(2)

This provision will allow regulations that prescribe an industry code to 'prescribe pecuniary penalties not exceeding 300 penalty units for civil penalty provisions of the industry code.' Currently section 51AD of the *Competition and Consumer Act 2010* provides that a contravention of a prescribed industry code is a contravention of the Act, however no pecuniary penalty can be imposed for such a contravention.

Proposed subsection 51AE(2) raises two scrutiny issues relating to appropriate delegation of legislative power.

First, the proposal means that the content of a civil penalty provision will be determined in an instrument (the industry code) that will be given legal effect by the regulation. The committee routinely draws attention to the incorporation of legislative provisions by reference to other documents because these provisions raise the prospect of changes being

made to the law in the absence of Parliamentary scrutiny. In addition, such provisions can create uncertainty in the law and those obliged to obey the law may have inadequate access to its terms.

The second scrutiny issue relates to the level of penalty that may be prescribed in the regulations (up to 300 penalty units). This is a significant penalty. The *Guide to Framing Commonwealth Offences, Infringement Notices and Enforcement Powers* recommends that where an Act authorises the creation of offences in subordinate instruments it should generally specify that the offences may carry a maximum fine of 50 penalty units for an individual and 250 for a body corporate. The underlying principle is that serious penalties should be contained in Acts of Parliament so as to enable appropriate parliamentary scrutiny.

The committee notes that the explanatory memorandum describes the operation of this provision (at p. 11) and overall objective of the bill in relation to the Franchising Code (at p. 6), however, it does not provide specific details as to the rationale for this provision. **The committee therefore seeks the Minister's advice in relation to both of the above scrutiny issues. In particular, the committee seeks advice in relation to:**

- **the rationale as to why the significant matter of the *content of a civil penalty offence* is not provided for in primary legislation;**
- **the justification for the *significant penalty* (up to 300 penalty units) that may be prescribed for the breach of a civil penalty provision in an industry code;**
- **the type of industry codes that may be prescribed by regulations under this provision (including whether it is intended that this provision will only apply to the Franchising Code);**
- **whether industry codes, including but not limited to the Franchising Code, will be available for scrutiny and disallowance by the Parliament; and**
- **any measures in place to ensure that industry code civil penalty provisions will be readily accessible to regulated persons.**

Pending the Minister's reply, the committee draws Senators' attention to the provision, as it may be considered to delegate legislative powers inappropriately, in breach of principle 1(a)(iv) of the committee's terms of reference.

Minister's response - extract

The reasons for the Government's decision to introduce the Bill are set out in its policy statement, *The Future of Franchising*, which addresses the implementation of recommendations of the 2013 review of the Franchising Code by Mr Alan Wein. The policy statement identifies that:

> Consultation during the review presented consistent anecdotal evidence of questionable behaviours in franchising. As franchisors are usually in a more powerful economic and contractual position than the franchisee, poor conduct by franchisors can have a disproportionate effect on franchisees. On the other hand, due to the network nature of franchising, poor conduct by isolated franchisees can affect the reputation of the system as a whole. To address this, the Government proposes to:
>
> - Improve compliance and enforcement outcomes through a range of flexible tools for use by the regulator, the Australian Competition and Consumer Commission ('ACCC'). The Government will introduce penalties of up to $51,000 for serious breaches of the Code. This will mean stronger consequences for breaching the Code and will further deter parties from breaching the Code. The ACCC will also be given powers to issue infringement notices.

In response to the specific issues raised in Ms Dawes letter:

The rationale why the content of a civil penalty offence is not provided for in primary legislation:

Introducing a general power to allow penalties to be applied for a breach of an industry code made under the Act was considered the simplest and most efficient means of providing a flexible tool that can be adopted, where required, in different industry codes.

Providing for pecuniary penalties and infringement notices in primary legislation would require the reproduction in the Act of the proposed pecuniary penalty provisions for each individual industry code. Further, there could be less flexibility and less clarity for industry participants around which specific clauses of each industry code would have an associated pecuniary penalty or an infringement notice. This option was considered unwieldy in practical terms.

The justification for the penalty of up to 300 penalty units being prescribed for the breach of a civil penalty provision in an industry code:

Mr Wein's recommendation, after considering all the evidence, was for a pecuniary penalty of $50,000 for a breach of the Franchising Code. The Government agreed with Mr Wein that this amount would act as a deterrent to a breach of the Franchising Code, without punishing the breaching party excessively. The court may order a lower penalty if it believes one is warranted and one of the factors a court may take into account is the financial capacity of the breaching company.

It was considered preferable to express the penalty in penalty units, as expressed in the *Crimes Act 1914.* At present, 300 penalty units is $51,000.

On 27 August 2014, the Shadow Minister Assisting the Leader for Small Business, the Hon Bernie Ripoll MP, spoke in relation to the Bill, stating:

> The Bill will allow for a pecuniary penalty of up to $51,000, which is equal to 300 penalty units. From what I can tell, it is very, very similar to the former Labor government supported changes to the code which would have allowed for pecuniary penalties of up to $50,000. So if that is the only change then, of course, I welcome the bill that we had introduced in those terms.

The type of industry codes that may be prescribed by regulations under this provision (including whether it is intended that this provision will only apply to the Franchising Code):

The provisions may be applied to any industry code prescribed under section 51AC of the Act.

A new Franchising Code is expected to be introduced later in 2014 and be in place by 1 January 2015. It is the only Code that has currently made the case for the introduction of pecuniary penalties, to date. The case for the introduction of penalties for breach of a civil penalty provision will have to be made for each code separately.

Whether industry codes, including but not limited to the Franchising Code of Conduct, will be available for scrutiny and disallowance by the Parliament:

Section 51ACA of the Act provides that an industry code prescribed under section 51AC must be declared by a regulation. Any new industry code or amendment to existing industry codes will be subject to scrutiny and disallowance by the Parliament.

Measures in place to ensure that industry civil code penalty provisions will be readily accessible to regulated persons:

The inclusion of penalty provisions in the industry code itself, and not the Act, makes them more readily accessible to participants in the industry. The Government has consulted widely and is working with the industry codes regulator, the ACCC, to ensure guidance material is made available to participants and potential participants in the sector.

Committee Response

The committee thanks the Minister for this detailed response.

The committee notes that this bill has already been passed by both Houses of Parliament; however the committee takes this opportunity to reiterate its general concern about the incorporation of legislative provisions by reference to other documents. The committee notes that such provisions may create uncertainty in the law and raise the prospect of changes being made to the law in the absence of Parliamentary scrutiny.

The committee notes that it would have been useful if the key information above had been included in the explanatory memorandum.

The committee also draws this matter to the attention of the Regulations and Ordinances Committee for information.

Corporations Amendment (Streamlining of Future of Financial Advice) Bill 2014

Introduced into the House of Representatives 19 March 2014
Portfolio: Treasury

Introduction

The committee dealt with this bill in the amendment section of *Alert Digest No. 11 of 2014*. The Acting Assistant Treasurer responded to the committee's comments in a letter dated 13 September 2014. A copy of the letter is attached to this report.

Alert Digest No. 11 of 2014 - extract

Background

This bill seeks to amend Part 7.7A the *Corporations Act 2001* (in relation to the financial advice industry) to:

- remove the need for clients to renew their ongoing fee arrangement with their financial adviser every two years;
- make the requirement that financial advisers provide a fee disclosure statement only applicable to clients who entered into their arrangement after 1 July 2013;
- remove paragraph 961B(2)(g) (the 'catch-all' provision) from the list of steps an advice provider may take in order to satisfy the best interests obligation;
- facilitate the provision of scaled advice; and
- provide a targeted exemption for general advice from the ban on conflicted remuneration in certain circumstances.

Regulation-making powers
Section 963B and subsection 963C(1)

Government amendments (4), (5) and (6) will allow regulations to prescribe circumstances in which, despite another provision of the section, 'all or part of a benefit is to be treated as conflicted remuneration.'

The supplementary explanatory memorandum simply restates the effect of the provisions without providing advice as to the justification for the use of delegated legislation for

potentially significant material and also without explaining why it is appropriate for delegated legislation to be able to override the effect of the primary legislation. While it appears that the provisions might be intended to have a beneficial effect for consumers, it would be appropriate for this to be clearly expressed in the explanatory memorandum and to include possible examples for the use of these regulation-making powers. **The committee therefore seeks the Minister advice about these matters.**

> *Pending the Minister's reply, the committee draws Senators' attention to the provisions as they may be considered to delegate legislative powers inappropriately in breach of principle 1(a)(iv) of the committee's terms of reference.*

Minister's response - extract

In its Scrutiny of Bills Alert Digest *No. 11 of 2014,* the Committee sought advice in relation to amendments 4, 5 and 6 to the Bill: these amendments extend the regulation-making powers in the Bill to allow regulations to prescribe circumstances when a benefit is to be treated as conflicted remuneration (amendment 4 relates to section 963B, amendment 5 to subsection 963C(1) and amendment 6 to subsection 963C(1)).

In addition to the regulation-making powers, amendment 4 inserts a new targeted general advice provision that is comprised of five limbs: all five limbs must be satisfied for the benefit to not be considered conflicted remuneration. There is also a specific limb that clarifies – beyond doubt – that payments known as commissions cannot be paid.

Whilst I believe the future of Financial Advice amendments have been well tested, there is always the possibility – given the complexity of arrangements in the financial services sector – that unintended consequences may arise. As such, the enhanced regulation-making powers would permit the Government to address any unintended consequences should they arise.

The Government has endeavoured to ensure that there is adequate flexibility in the new amendments to address the concerns of industry and consumers at a time of legislative change. I believe that the Bill achieves the appropriate regulatory balance. Any regulations would be subject to consultation with stakeholders, as well as subject to the disallowance procedure under the *Legislative Instruments Act 2003,* providing Parliament with the opportunity to scrutinise the application of new regulations.

I also note that the Bill - including the amendments - is currently being reviewed by the Senate Economics Legislation Committee. The Committee is due to report later this month and the Government will carefully consider any amendments recommended by the Committee.

Committee Response

The committee thanks the Assistant Treasurer for this response in relation to the government amendments to this bill (which have been passed by the House of Representatives and now form part of the bill under consideration in the Senate).

The committee notes the 'complexity of arrangements in the financial services sector' and the Assistant Treasurer's statement that the regulation-making powers contained in the amendments 'would permit the Government to address any unintended consequences should they arise'. Although unintended consequences may arise in complex regulatory environments, it may be doubted whether this risk is in itself a sufficient justification for broad delegations of power which enable regulations to override the effect of the primary legislation. The committee further notes that the Assistant Treasurer's response does not provide examples of possible exercises of this power. **The committee therefore remains concerned about the breadth of the power to override the effect of the primary legislation and draws this issue to the attention of Senators.**

The committee also draws this matter to the attention of the Regulations and Ordinances Committee for information.

Migration Amendment (Protection and Other Measures) Bill 2014

Introduced into the House of Representatives on 25 June 2014
Portfolio: Immigration and Border Protection

Introduction

The committee dealt with this bill in *Alert Digest No. 8 of 2014*. The Minister responded to the committee's comments in a letter dated 11 August 2014. The committee sought further information and the Minister responded in a letter dated 19 September 2014. A copy of the letter is attached to this report.

Alert Digest No. 8 of 2014 - extract

Background

This bill seeks to amend the *Migration Act 1958* to:

- clarify that it is an asylum seeker's responsibility to specify the particulars of their claim to be a person in respect of whom Australia has protection obligations and to provide sufficient evidence to establish their claim;

- provide for the Refugee Review Tribunal (RRT) to draw an unfavourable inference with regard to the credibility of claims or evidence that are raised by a protection visa applicant at the review stage for the first time, if the applicant has no reasonable explanation to justify why those claims and evidence were not raised before a primary decision was made;

- create grounds to refuse a protection visa application when an applicant refuses or fails to establish their identity, nationality or citizenship, and does not have a reasonable explanation for doing so, including when an applicant provides bogus documents to establish their identity or either destroys or discards such evidence, or has caused that evidence to be destroyed or discarded;

- clarify when an applicant who applies for a protection visa, where a criterion for the grant of a visa is that they are a member of the same family unit of a person who engages Australia's protection obligations, is to make their application for a protection visa;

- define the risk threshold for assessing Australia's protection obligations under the *International Covenant on Civil and Political Rights* (ICCPR) and the *Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment* (CAT);

- simplify the legal framework relating to unauthorised maritime arrivals and transitory persons who can make a valid application for a visa;

- amend the processing and administrative duties of the Migration Review Tribunal including:
  - a Principal Member being able to issue guidance decisions and practice directions;
  - enabling Tribunals to make an oral statement of reasons where there is an oral decision without the need for a written statement of reasons; and
  - Tribunals will be able to dismiss an application where an applicant fails to appear before the Tribunal after being invited to do so, then being able to reinstate the application where an applicant applies for reinstatement within a specified period of time; and

- make a technical amendment to put beyond doubt when a review of a decision that has been made in respect of an application under the Migration Act is 'finally determined'.

Undefined scope of administrative power
Delegation of legislative power
Schedule 4, Part 1, item 7, proposed section 353B
Schedule 4, Part 1, item 22, proposed section 420B

Proposed subsection 353B(1) provides that the Principal Member of the Migration Review Tribunal (MRT) may, in writing, direct that a decision (a 'guidance decision') of the MRT specified in the direction is to be complied with by the MRT in reaching a decision on review of cases involving similar facts and circumstances. Proposed subsection 420B provides the same powers in relation to the Refugee Review Tribunal (RRT).

Proposed subsections 353B(2) and 420B(2) provide that 'in reaching a decision on a review of a decision of that kind, the Tribunal must comply with the guidance decision unless the tribunal is satisfied that the facts or circumstances of the decision under review are clearly distinguishable from the facts or circumstances of the guidance decision'.

It is not immediately apparent what it means to 'comply' with a 'decision', as opposed to a rule or standard. It may not be clear which of the facts or reasons accepted in a guidance decision have binding force and are considered to have general application. This may

create uncertainty as to how the rights of applicants to the MRT are affected by a direction that a guidance decision is to be complied with.

The explanatory memorandum (at pp 36 and 48) states that a 'guidance decision' will relate to 'identifiable common issues in matters before the MRT and RRT, and Members of the MRT and RRT would be expected to follow them unless the facts or circumstances in the current matter before them could be distinguished'. The purpose of the provision is thus said to 'promote consistency in decision-making…in relation to common issues and/or the same or similar facts or circumstances'. It may be accepted that consistency in decision-making is a legitimate objective for merits review tribunals. However, it remains the case that this proposed section does little to indicate what aspects of a 'guidance decision' are considered binding (unless distinguishable) and the sense in which the decision has binding force.

One possible way of understanding this provision is that it enables the Principal Member to create something like a judicially created precedent. A guidance decision plays a determinative role in establishing an applicant's rights (because the application of the law to facts in the guidance decision *must* be complied with). For this reason, the power to issue a guidance decision may take on the character of an exercise of judicial power. The creation of binding legal precedent is typically thought to be an exercise of judicial rather than administrative power.

If, however, the power to issue a guidance decision is not characterised as an exercise of judicial power (judicial powers cannot, in general, be conferred on administrators for constitutional reasons), questions arise about whether a guidance decision constitutes an exercise of legislative power as it appears to determine how the law should be applied in a general category of cases. If this interpretation is accurate, then it would seem that this power falls within the definition of a legislative instrument in the *Legislative Instruments Act 2003* (the LI Act). Section 5 of the LI Act provides that an instrument will be taken to be of a legislative character if: (a) it determines the law or alters the content of the law, rather than applying the law in a particular case; and (b) it has the direct or indirect effect of affecting a privilege or interest, imposing an obligation, creating a right, or varying or removing an obligation or right.

In light of the above comments the committee seeks the Minister's advice as to whether the proposed sections are to be characterised as:

a) an exercise in judicial power and, if so, whether it is appropriate to confer them on an administrator; or

b) legislative in character and subject to disallowance under the *Legislative Instruments Act 2003*.

In addition, in light of the Minister's response to the above, the committee requests the Minister's further advice as to what aspects (facts or reasons) of a 'guidance decision' will be binding and how a decision-maker will be able to identify them.

Pending the Minister's reply, the committee draws Senators' attention to the provisions, as they may be considered to constitute an inappropriate review of decisions, in breach of principle 1(a)(iii) of the committee's terms of reference. The provisions may also delegate Parliament's powers inappropriately in breach of principle 1(a)(iv) of the committee's terms of reference.

Minister's response - extract

Undefined scope of administrative power
Delegation of legislative power
Schedule 4, Part 1, item 7, proposed section 353B
Schedule 4, Part 1, item 22, proposed section 420B

In light of the above comments the committee seeks the Minister's advice as to whether the proposed sections are to be characterised as:

a) an exercise in judicial power and, if so, whether it is appropriate to confer them on an administrator; or

b) legislative in character and subject to disallowance under the Legislative Instruments Act 2003.

The amendments under proposed sections 353B and 420B will align and reduce inconsistencies in decision-making and increase efficiency by enabling the Principal Member of the Migration Review Tribunal (MRT) and RRT to issue guidance decisions. Guidance decisions are intended to be issued by the Principal Member in relation to identifiable common issues in matters before the MRT and RRT respectively, and tribunal members would be expected to follow them unless the facts or circumstances in the current matter before them could be distinguished. Use of the powers created by these amendments will promote consistency in decision-making across the MRT and RRT respectively in relation to common issues and/or the same or similar facts or circumstances.

Guidance decisions are not intended to go to the conduct of the review, but are intended to provide guidance on how to decide factual or evidentiary issues that might arise in review cases. Proposed subsections 3538(2) and 420B(2) provide that while tribunal members are required to comply with a guidance decision in reaching a decision on review in cases with like issues and evidence, the tribunal does not need to comply with the guidance decision if the facts or circumstances of the decision under review are clearly distinguishable from the facts or circumstances of the guidance decision. In addition, proposed subsections 353B(3) and 420B(3) provide that non-compliance by tribunal members does not mean that the tribunal's decision on a review is an invalid decision.

The power of the Principal Member of the MRT and RRT to issue guidance decisions is not an exercise of judicial power. Only the courts stipulated in section 71 of the Constitution can exercise the judicial power of the Commonwealth[1]. A person or body which is part of the executive government, such as the Principal Member of the MRT and RRT, cannot exercise the judicial power of the Commonwealth. As such, proposed sections 353B and 420B will involve the exercise of legislative power by the Principal Member.

The guidance decision is an exercise of legislative power, but is not subject to disallowance under the *Legislative Instruments Act 2003* (LIA). Section 7 of the LIA provides for instruments declared not to be legislative instruments. Paragraph 7(1)(a) of the LIA provides that an instrument is not a legislative instrument for the purposes of the LIA if it is included in the table in section 7. Item 24 of that table relevantly provides that instruments that are prescribed by the regulations for the purposes of this table are not legislative instruments.

Regulation 7 of the *Legislative Instruments Regulations 2004* (LIR) provides that for item 24 of the table in subsection 7(1) of the LIA, and subject to section 6 and 7 of the LIA, instruments mentioned in Schedule I of the LIR are prescribed. Item 6 of Part 1 of Schedule I provides that a practice direction made by a court or tribunal are not legislative instruments. As such the direction of a Principal Member in relation to a guidance decision is not a legislative instrument for the purposes of the LIA and is not subject to disallowance.

In addition, in light of the Minister's response to the above, the committee requests the Minister's further advice as to what aspects (facts or reasons) of a 'guidance decision' will be binding and how a decision-maker will be able to identify them.

What aspects of a guidance decision will be required to be complied with is a matter for the Principal Member when deciding to issue a guidance decision. The Principal Member will issue a direction that the guidance decision is to be complied with when the Tribunal is reaching a decision of a kind specified in the direction. The issuance of the direction allows the Principal Member the flexibility to tell the decision maker what needs to be complied with to assist the tribunal members. A guidance decision will not be complied with where members are satisfied that the facts or circumstances of the decision under review are clearly distinguishable from that of the particular guidance decision. Non-compliance by Tribunal members with a guidance decision will not invalidate that decision on a review.

[1] *R v Kirby; Ex partre Boilermakers' Society of Australia* (1956) 94 CLR 254.

Committee Response

The committee thanks the Minister for this detailed response and **requests that the key information be included in the explanatory memorandum.**

The committee remains unclear about what it means to comply with a guidance decision if, as explained, such decisions relate to issues of fact. **However, in light of the explanation offered, the committee leaves to the Senate as a whole the question of whether the requirement on tribunal members to comply with such decisions leaves the scope of the administrative powers being exercised sufficiently well defined.**

The committee, however, is interested in a further explanation of the rationale for the exemption of guidance decisions from the requirements of the LI Act as it is concerned that the exemption for tribunal and court 'practice directions' may not be appropriate in this instance. Practice directions (in general) concern matters of procedure whereas guidance decisions clearly raise issues of substance. **The committee therefore seeks the Minister's advice as to why the general exemption from the LI Act for practice directions is appropriate in relation to 'guidance decisions'. The committee would also be interested to know whether there are other examples of practice directions, covered by the exemption from the LI Act, which relate to questions of substance falling for determination by a Court or Tribunal.**

The committee draws this matter to the attention of the Senate Regulations and Ordinances Committee for information in relation to this proposed exemption from the requirements of the LI Act.

Minister's further response - extract

A practice direction is not just confined to matters of procedure, but encompasses matters of practice and procedure. The application of a guidance decision in a direction of the Principal Member of the Migration Review Tribunal or Refugee Review Tribunal depends on if the facts or circumstances in the guidance decision can be distinguished from the current matter before the relevant tribunal. Once those matters of substance are determined, it becomes clear whether or not the tribunal must follow the direction and apply a decision (the guidance decision) of the Tribunal as a matter of practice. That is, the question of whether a guidance decision must, as a matter of practice, be applied is resolved. The application of guidance decisions will align and reduce inconsistencies in decision-making and increase efficiency of the review process. However, there will be no derogation of the responsibility of the tribunal to investigate the individual circumstances of an applicant.

As noted in the response to the Committee dated 11 August 2014, the guidance decision is an exercise of legislative power, but is not subject to disallowance under the LI Act. Regulation 7 of the *Legislative Instruments Regulations 4004* (LIR) provides that for item 24 of the table in subsection 7(1) of the LI Act, and, subject to section 6 and 7 of the LI Act, instruments mentioned in Schedule 1 of the LIR are prescribed. Item 6 of Part 1 of Schedule 1 provides that practice directions made by a court or tribunal are not legislative instruments.

As the concept of a guidance decision is a specific concept in respect of a practice direction of a tribunal, I am unable to provide another similar example of a practice direction.

To make it clear that 'guidance decisions' are not subject to disallowance, it is my intention to provide an Addendum to the Explanatory Memorandum.

I note that the Committee has also recommended that a number of other amendments be made to the Explanatory Memorandum for this Bill. I will make such amendments by way of an addendum to be Explanatory Memorandum, based on the further information already provided to the Committee, at an appropriate time.

Thank you for considering this advice.

Committee's further response

The committee thanks the Minister for this response and welcomes further clarification being added to the explanatory memorandum.

The committee notes the Minister's explanation that a 'guidance decision' is a matter of practice not substance. The implication appears to be that for this reason it is appropriate to exempt guidance decisions from the operation of the LI Act. The committee, however, remains to be convinced that a meaningful distinction can be drawn between a matter of practice, as explained by the Minister, and the application of a substantive rule or precedent. In relation to a rule or precedent it may also be said that once it is determined that the facts are covered by the rule or precedent case that it then becomes clear whether or not the tribunal must apply the rule or precedent as 'a matter of practice'.

The committee further notes the advice that the Minister is unable to provide examples of practice directions, which are also covered by the general exemption from the LI Act, that are of a similar nature to 'guidance decisions'.

The committee therefore draws this matter to the attention of senators and, in light of the explanation provided by the Minister, leaves the appropriateness of the exemption of practice directions from the LI Act to the Senate as a whole.

National Security Legislation Amendment Bill (No. 1) 2014

Introduced into the Senate on 16 July 2014
Portfolio: Attorney-General

Introduction

The committee dealt with this bill in *Alert Digest No. 11 of 2014*. The Attorney-General responded to the committee's comments in a letter dated 16 September 2014. A copy of the letter is attached to this report.

Alert Digest No. 11 of 2014 - extract

Background

This bill amends the *Australian Security Intelligence Organisation Act 1979* (the ASIO Act) and the *Intelligence Services Act 2001* (the IS Act) to implement the Government's response to recommendations in Chapter 4 of the Parliamentary Joint Committee on Intelligence and Security's *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation* (tabled in June 2013) relating to reforms of the legislation governing the Australian Intelligence Community.

Schedule 1 amends ASIO's statutory employment framework.

Schedule 2 amends ASIO's warrant based intelligence collection powers, including in relation to computer access warrants, surveillance devices and warrants against an identified person of security concern.

Schedule 3 provides ASIO employees and affiliates with certain protection from criminal and civil liability in authorised covert intelligence operations (referred to as 'special intelligence operations').

Schedule 4 amends the statutory framework for ASIO's co-operative and information-sharing activities.

Schedule 5 amends the IS Act to enable the Australian Secret Intelligence Service (ASIS) to undertake a new function of co-operating with ASIO in relation to the production of intelligence on Australian persons in limited circumstances. This schedule will also:

- create a new ground of ministerial authorisation in relation to the protection of ASIS's operational security;

- allow ASIS to train certain individuals in the use of weapons and self-defence techniques;
- extend immunity for IS Act agencies for actions taken in relation to an overseas activity of an agency; and
- provide a limited exception for the use of a weapon or self-defence technique in a controlled environment.

Schedule 6 amends secrecy offences in the IS Act and ASIO Act in relation to unauthorised communication of intelligence-related information.

Schedule 7 provides for the renaming of the Defence Imagery and Geospatial Organisation (DIGO) as the Australian Geospatial Intelligence Organisation (AGO) and the Defence Signals Directorate (DSD) and the Australian Signals Directorate (ASD).

General comment by the Attorney-General

I now provide responses to each of the 19 matters in respect of which your Committee has sought further information from me. **(Enclosure 1.)**

I have also taken the liberty of providing three additional documents at **Enclosure 2**, which may be of assistance to the Committee in completing its examination of the Bill. These are unclassified submissions from my Department (AGD) and the Australian Security Intelligence Organisation (ASIO) to the Parliamentary Joint Committee on Intelligence and Security (PJCIS) inquiry into the Bill, which is due to provide its report in the week commencing 22 September 2014. A number of issues raised in Alert Digest No. 11 were also the subject of evidence before the PJCIS. My responses to your Committee's questions refer to relevant passages in these additional materials.

[The AGD and ASIO submissions to the PJCIS inquiry are not included in this report and may be accessed using the following link:
http://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/National_Security_Amendment_Bill_2014/Submissions]

I trust that this information is of assistance to your Committee. I would be pleased to provide any further assistance that may be required, and look forward to considering your Committee's report on the Bill in due course.

Thank you again for writing to me on this matter.

Alert Digest No. 11 of 2014 - extract

Insufficiently defined administrative power—delegation to 'a person'
Schedule 1, item 5

This item repeals current section 16 of the ASIO Act, which enables the Director-General to delegate any of his or her powers relating to the management of the staff of ASIO or the financial management powers provided under the ASIO Act to 'an officer of the Organisation'. The proposed replacement provision makes two key changes to the power of delegation:

- (1) to describe the delegable powers by reference to powers, functions or duties that relate to the management of 'ASIO employees or ASIO affiliates', rather than by reference to staff of ASIO, and
- (2) to provide that the powers may be delegated to 'any person', rather than to 'an officer of the Organisation'.

The first change is justified by reference to item 1 of Schedule 1 which introduces new definitions of categories of persons who work within or for ASIO, namely, an ASIO affiliate and ASIO employee. ASIO affiliates are persons who perform functions or services for ASIO in accordance with a contract, agreement or other arrangement. These amendments are said to 'both streamline and provide consistency in relation to the use of descriptors in the Act' (explanatory memorandum, p. 36). In the circumstances, the committee has no further comment in relation to this aspect of the proposed replacement power of delegation in replacement section 16.

In relation to the second change to be introduced by item 5 of Schedule 1, the committee consistently draws attention to legislation which allows significant and wide-ranging powers to be delegated to 'a person'. Generally, the committee prefers to see limits on the categories of persons to whom significant powers may be delegated (the committee usually expects that delegates will be confined to members of the Senior Executive Service or to the holders of nominated offices unless there is a strong justification for a broader approach).

The explanatory memorandum (p. 38) briefly addresses this issue:

> Providing for the delegation of the particular powers, functions or duties covered by new section 16 to 'any person' is consistent with the operational requirements of the Organisation and the exercise of other powers across the ASIO Act.

The committee notes that this explanation of the need for such a broad power of delegation does not enable the committee to properly consider its appropriateness. The operational requirements necessitating the power remain unexplained. It is not clear why the

delegation of powers and functions relating to the general management of employees and affiliates and the financial management of the organisation cannot be subject to some limitations.

The committee therefore seeks more detailed advice from the Attorney-General as to why departure from this well established principle as proposed in the bill is appropriate in the circumstances. In this respect it is noted that the existing provision already casts the power to delegate in very broad terms, that is, to 'an officer of the Organisation'. The committee's consideration of the new provision would likely be assisted examples of the sorts of delegations that would be appropriately authorised by the proposed new power of delegation, but are not possible under the terms of the existing provision.

> *Pending the Attorney-General's reply the committee draws Senators' attention to the provision, as it may be considered to make rights, liberties or obligations unduly dependent upon insufficiently defined administrative powers, in breach of principle 1(a)(ii) of the committee's terms of reference.*

Attorney-General's response - extract

Amending item 5 of Schedule 1 to the Bill replaces the phrase "officer of the Organisation" in s 16 with "a person". It is consequential to the updated terminology proposed to be included in s 4 of the ASIO Act of 'ASIO employee' and 'ASIO affiliate' (per amending item 1 of Schedule 1 to the Bill). The adoption of these terms will mean that the term 'an officer of the Organisation' (which is undefined) is no longer used in Part V of the ASIO Act. As such, another term is required in s 16(1) to describe those to whom the Director-General of Security may delegate powers, functions or duties under the ASIO Act in respect of the management of ASIO employees and ASIO affiliates, and the financial management of the Organisation.

The term 'a person' has been used in proposed new s 16(1) to ensure that the Director-General can exercise his or her power of delegation in favour of persons who, for a range of reasons, may not be within the definition of an 'ASIO employee' or an 'ASIO affiliate',[2] in addition to persons within the Organisation who may fall within the definition of those terms (for example, a Chief Financial Officer or a Deputy Director-General). I acknowledge the Committee's comments on the breadth of the existing delegation under s 16 and that proposed to be included by amending item 5. Consideration was given to limiting the provision to an identified class or classes of persons. However, it was determined that the balance of interests in ensuring necessary flexibility and placing

[2] The contingency that certain persons may not be ASIO employees or ASIO affiliates (or within the meaning of the former term 'officers of the Organisation') is presently recognised in other provisions of the ASIO Act. For example, the Minister is empowered under s 14 to appoint 'a person' to act as Director-General of Security.

appropriate limitations on the power of delegation is best achieved through the limited nature of the powers, functions and duties of the Director-General which are subject to delegation under proposed new s 16(1). Further safeguards are contained in new s 16(2) and the independent oversight of the Inspector-General of Intelligence and Security (IGIS) in relation to the activities of ASIO, which could include the activities of delegates under proposed s 16(1).

In particular, the functions and powers of the Director-General that may be the subject of a delegation under proposed new s 16(1) are very limited. The provision does not extend to any or all of the Director-General's functions and powers under the ASIO Act. It is only those powers relating to management of ASIO employees or ASIO affiliates, and the financial management powers provided for in the ASIO Act. Almost all financial management within ASIO is carried out under the *Public Governance Performance and Accountability Act 2013*, and delegations of those powers are made in accordance with that Act. The power of delegation in proposed new s 16(1) is consistent with the scope of other such powers of delegation invested in agency heads under Commonwealth legislation. For example, s 78(7) of the *Public Service Act 1999* allows an Agency Head to delegate to "another person any of the Agency Head's powers or functions under that Act", which includes various staff management powers.[3]

In addition, the delegation power in proposed new s 16(1) must be exercised subject to any written directions given by the Director-General under proposed new s 16(2). The exercise of the power of delegation under proposed s 16(1), the issuing of any directions under s 16(2), and the activities of a delegate would also be subject to the independent oversight of IGIS under the *Inspector-General of Intelligence and Security Act 1986* (IGIS Act). The IGIS is empowered under s 8 of the IGIS Act to examine both the legality and the propriety of the activities of ASIO. The IGIS also has power under s 8(1)(b) of the IGIS Act to examine, at the request of the Attorney-General, the procedures of ASIO relating to redress of grievances of employees of ASIO (which is proposed to be amended by item 43 of Schedule 1 to cover ASIO employees and ASIO affiliates). The IGIS further has power under s 8(6) to inquire into complaints made by ASIO employees about certain staff management issues. (A similar power is proposed to be inserted in relation to ASIO affiliates by amending item 45 in Schedule 1 to the Bill in proposed ss 8(8) and 8(8A).) These powers would be exercisable in relation to the activities of delegates under proposed s 16(1).

---

[3] It is acknowledged, however that an additional limitation is applied under s 78(8) of the *Public Service Act 1999*. An Agency Head cannot delegate powers or functions to a non-APS employee or a person who does not hold an executive or statutory office (referred to as an 'outsider') without the prior written consent of the Public Service Commissioner. An additional approval requirement was not considered necessary for inclusion in the ASIO Act, given the limited scope of delegation within s 16(1), and nor appropriate within the context of an intelligence agency where vulnerabilities may be created if the identities of those performing work for ASIO are revealed unnecessarily. Instead, adequate provision is made for oversight under proposed new s 16(2) (in which the delegate must comply with any written direction given by the Director-General) and the general oversight jurisdiction of the IGIS in respect of the activities of ASIO.

To take account of the Committee's comments on this proposed provision, I have asked my Department to revise the Explanatory Memorandum to the Bill to include an explanation of these matters.

Committee Response

The committee thanks the Attorney-General for this detailed response and for indicating that the explanatory memorandum to the bill will be revised to include an explanation of the above matters.

The committee reiterates its general preference that limits are placed on the categories of persons to whom significant powers may be delegated. **In this instance, and in light of the detailed explanation above, the committee leaves the question of whether the proposed approach is appropriate to the Senate as a whole.**

Alert Digest No. 11 of 2014 - extract

Undue trespass on personal rights and liberties—privacy
Delegation of legislative power—broad delegation
Schedule 1, item 6, proposed paragraphs 18(2)(e) and (f)

Section 18 of the ASIO Act provides that the Director-General or a person acting with the limits of authority conferred on the person by the Director-General may communicate intelligence or information on behalf of the organisation. Subsection 18(2) currently establishes an offence for a person to communicate information which has come to the knowledge or into the possession of the person by reason of the person being or having been an officer or employee of the organisation or having entered into any contract, agreement or arrangement with the organisation.

This item replaces existing subsection 18(2) with a new provision. Proposed paragraph 18(2)(e) provides that the offence for unauthorised communication will not be made out if the communication was by a person within the limits of authority conferred on the person by the Director-General. Paragraph 18(2)(f) provides that the offence for unauthorised communication will not be made out if the communication was made with the approval of the Director-General or of a person having the authority of the Director-General to give such an approval.

The explanatory memorandum (p. 39) states that:

> Allowing the Director-General to authorise any person to give approval for the communication of information is consistent with the operational requirements of the Organisation and the exercise of other powers across the ASIO Act [and that the authorisation] is conferred on the basis that the Director-General believes such a person should reasonably be able to exercise this power.

The ability of the Director-General to approve 'a person' to communicate information has the potential to adversely impact on privacy if it includes the release of personal information. **The committee therefore seeks more detailed advice from the Attorney-General as to the justification for this proposed approach, including whether consideration has been given to limitations being placed on the category of persons whom may be authorised to communicate information.**

> *Pending the Attorney-General's reply, the committee draws Senators' attention to the provision as it may be considered to trespass unduly on personal rights and liberties, in breach of principle 1(a)(i) of the committee's terms of reference.*

Attorney-General's response - extract

The Bill retains the existing ability of the Director-General under s 18(1) to authorise a person to communicate intelligence on behalf of the Organisation, within the limits of that person's authority as conferred by the Director-General. Amending item 6 updates the unauthorised communication offence in s 18(2) to apply the new terminology of 'ASIO employee' and 'ASIO affiliate' proposed to be included by amending item 1 of Schedule 1, which will replace the terms presently used in that provision, consistent with other employment-related amendments proposed in the Bill.

As a result, the framework within which the Director-General communicates or authorises a person to communicate information held by ASIO is not significantly changed by the Bill. Proposed ss 18(2)(e) and 18(2)(f) reflect the existing provisions in ss 18(2)(b) and 18(2)(c) of the ASIO Act. There is no proposal to amend s 18(1), which allows the Director-General to authorise a person to communicate intelligence. Subsection 18(1) was inserted, in its present form, by the *Australian Security Intelligence Organisation Legislation Amendment (Terrorism) Act 2003* (Bills of 2002 and 2003). I note that this provision was not the subject of comment by this Committee as constituted in 2002 and 2003.[4]

I acknowledge the Committee's comment that the ability of the Director-General to approve 'a person' to communicate information may potentially impact on personal privacy. This matter is addressed in the Attorney-General's Guidelines to ASIO, issued under s 8A of the ASIO Act. Paragraph 13 of the Guidelines place obligations on ASIO in

[4] Alert Digest No 4 of 2002, Report No 12 of 2002, Alert Digest No 4 of 2003.

relation to the treatment of personal information. This includes an obligation to collect, use, handle or disclose personal information only for purposes connected with ASIO's statutory functions. The Guidelines also require the Director-General to take reasonable steps to ensure that personal information shall not be collected, used, handled or disclosed by ASIO unless necessary for the performance of its statutory functions (or as otherwise authorised or required by law). The communication of intelligence, and the authorisation by the Director-General of persons under s 18(1), is subject to the independent oversight of the IGIS.

The damage to Australia's national security interests that can be posed by the unauthorised communication of intelligence-related information should not be underestimated. The Bill, in relation to s 18(2), contains measures to reflect the culpability inherent in such wrongful conduct. However, the seriousness of such conduct must be balanced against the need to ensure that the intelligence community is able to appropriately share information with those who have associated responsibilities for protecting Australian interests. Careful consideration is given to the sharing of intelligence-related information and who is authorised to do so, in accordance with the Attorney-General's Guidelines.

Committee Response

The committee thanks the Attorney-General for this detailed response.

The committee notes the information provided by the Attorney-General about the obligations placed on ASIO in relation to the treatment of personal information under the Attorney-General's Guidelines and leaves the question of whether the proposed approach is appropriate to the Senate as a whole.

Alert Digest No. 11 of 2014 - extract

Insufficiently defined administrative power—authorisation of a person to exercise significant powers
Schedule 1, item 9, proposed subsection 23(6), ***Australian Security Intelligence Organisation Act 1979***
Schedule 1, items 34 and 35, proposed subsection 90F(1) and proposed paragraph 90F(2)(b), ***Australian Postal Corporation Act 1989***

Subsection 23(6) of the *Australian Security Intelligence Organisation Act 1979* currently provides that:

> The Director-General, or a senior officer of the Organisation appointed by the Director-General in writing to be an authorising officer for the purposes of this subsection, may authorise, in writing, an officer or employee of the Organisation, or a class of such officers or employees, for the purposes of this section.

The powers that may be exercised under this section are significant powers to request information or documents from operators of aircraft or vessels (and failure to comply with a request is an offence). The effect of the proposed new subsection 23(6) in this bill is that the Director-General or a senior-position holder may instead authorise 'a person, or a class of persons' (rather than 'an officer or employee of the Organisation') to exercise such functions.

The explanatory memorandum (at p. 40) argues that the amendment is:

- necessary to accommodate the broad range of persons who could reasonably be expected to be authorised to exercise these powers; and
- reflects the operational requirements of the organisation and is consistent with the exercise of other powers across the ASIO Act.

Neither of these arguments is elaborated further though it is noted that the powers are conferred on the basis that the Director-General 'believes such a person should reasonably be able to exercise that power'.

The committee notes that similar issues arise in relation to items 34 and 35 of Schedule 1 which propose amendments to subsection 90F(1) and paragraph 90F(2)(b) of the *Australian Postal Corporation Act 1989*.

It is a matter of concern to the committee that the legislation appears to contain no criteria or limitations on the class of persons who may be authorised to exercise these coercive powers. **The committee therefore seeks more detailed advice from the Attorney-General as to the justification for the proposed approach, including a more detailed elaboration of the above arguments.**

> *Pending the Attorney-General's reply, the committee draws Senators' attention to the provisions as they may be considered to make rights, liberties or obligations unduly dependent upon insufficiently defined administrative powers, in breach of principle 1(a)(ii) of the committee's terms of reference.*

Attorney-General's response - extract

Amending items 9, 34 and 35 replace references in the relevant provisions to officers and employees of ASIO, consequential to the updating of employment-related terminology in amending item 1 of Schedule 1 to the Bill.

Amending item 8 replaces the reference in s 23(1) of the ASIO Act to "an authorised officer or employee" with a reference to "an authorised person". Amending item 9 similarly amends the Director-General's power of authorisation under s 23(6) to authorise persons for the purpose of s 23(1).

Consideration was given to limiting the persons able to be authorised under s 23(6) for the purpose of s 23(1) to ASIO employees and ASIO affiliates (as proposed to be defined in s 4 by amending item 1 of Schedule 1). However, such a limitation was not considered appropriate from an operational perspective. It may not always be possible to locate an ASIO employee or ASIO affiliate at the same location as an aircraft or vessel operator in order to ask questions, or make a request for information. It would be unnecessarily restrictive to operational realities for the legislation to require an ASIO employee or ASIO affiliate to be physically at a particular, and often unplanned, location of the aircraft or vessel (noting that such aircraft and vessels may also depart from that location at short notice). It was considered an operational and administrative necessity that, for the purposes of carrying out ASIO's functions, another person (or class of persons) may need to be authorised to undertake that activity on ASIO's behalf. For example, it would not be unreasonable to authorise such persons as, but not limited to, Customs officers, or law enforcement officers to undertake this activity on behalf of ASIO.

The proposed amendments to ss 90F(l) and 90F(2)(b) of the *Australian Postal Corporation Act 1989* (amending items 34 and 35 of Schedule 1) are in a similar category, noting that information or documents relating to articles carried by post, or articles in the course of post, may also be available at unplanned locations that may rapidly change.

While the Committee has observed that s 23 is a "significant powers to request information or documents from operators of aircraft or vessels", the amendments proposed to s 23 are consistent with other powers for the collection of information across the ASIO Act. For example, s 24 of the ASIO Act, as currently enacted, provides for an officer, employee, or other people, to be authorised to exercise the authority of a warrant issued under the ASIO Act. (I acknowledge, however, that the Committee has also commented on the proposed amendments to s 24. My response to those comments is provided below.)

To take account of the Committee's comments on amending item 6 of Schedule 1, I have asked my Department to revise the Explanatory Memorandum to elaborate on the justification for these items, in line with my remarks above.

Committee Response

The committee thanks the Attorney-General for this detailed response and for indicating that the explanatory memorandum to the bill will be revised to include an explanation of the above matters.

The committee notes that the Attorney-General considers that it would be too restrictive to limit the class of persons who may be authorised to exercise these powers to ASIO employees and affiliates. However, the committee reiterates its general preference that limits are placed on the categories of persons who may be authorised to exercise such powers. The committee therefore remains concerned about the breadth of the power to authorise 'a person' in these provisions. **To assist the committee in further examining these provisions, the committee requests further advice from the Attorney-General in relation to whether consideration has been given to placing limits on the breadth of the power by, for example, limiting the class of persons authorised to exercise the powers to ASIO employees and affiliates, Customs officers and law enforcement officers.**

Alert Digest No. 11 of 2014 - extract

Undue trespass on personal rights and liberties—authorisation of a person to exercise significant powers
Schedule 1, item 61, proposed new paragraph 7(2)(ad), ***Telecommunications (Interception and Access) Act 1979***

This provision has the effect of extending to 'ASIO affiliates' an exception from the prohibition on the interception of a communication passing over a telecommunications system.

Item 1 of Schedule 1 of the bill inserts a definition of ASIO affiliate into the ASIO Act:

> ***ASIO affiliate*** means 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 and a person performing services under an agreement under section 87, but does not include the Director-General or an ASIO employee.

ASIO affiliates may thus include a broad range of persons and it is unclear whether the exception should appropriately apply to them given their qualifications (and it is not clear

what will be required and how this will be determined) and the nature of their 'appointment'. The explanatory memorandum merely repeats the effect of the proposed amendment.

Similar issues also arise in relation to items that extend authority to *ASIO affiliates* in a number of significant areas, including:

- item 62 enlarges the category of person who may be authorised to exercise powers conferred by Part 2-2 warrants;
- item 63 extends authorisation to intercept communications on behalf of ASIO;
- item 67 allows ASIO affiliates to communicate foreign intelligence information to another person.
- item 69 extends to affiliates an exception to an offence relating to accessing stored communications;
- items 70, 71 and 72 will extend authorisation to ASIO affiliates relating to receiving, communicating, using or recording foreign intelligence; and
- items 73 and 74 will extend provisions to ASIO affiliates which permit the disclosure of information or documents to ASIO.

A key question for each of these instances is why is it appropriate to extend a range of powers, authorisations and exemptions to ASIO affiliates. This does not appear to be addressed in the explanatory memorandum other than to say it is 'consistent with operational requirements'. It seems to the committee that there is a real issue about what powers etc. might appropriately be held by different classes of decision-makers, how appropriate qualifications will be determined and assessed and what safeguards will apply given that ASIO affiliates are not employees of the organisation.

The committee seeks more detailed advice from the Attorney-General as to the appropriateness of extending these exceptions to this broad class of persons associated with ASIO.

> *Pending the Attorney-General's reply the committee draws Senators' attention to the provisions as they may be considered to trespass unduly on personal rights and liberties, in breach of principle 1(a)(i) of the committee's terms of reference.*

Attorney-General's response - extract

Rationale for the term 'ASIO affiliate', and limitations on the scope of its coverage

I acknowledge the perception that the proposed new term 'ASIO affiliate' is an expansion of the range of persons who can be authorised to exercise the Organisation's powers and functions. My Department and ASIO recently provided a submission to the Parliamentary Joint Committee on Intelligence and Security (PJCIS) inquiry into the Bill, which responded to submissions to that inquiry on this point.[5] The commentary at pages 53-58 of the enclosed submission, and in particular at pages 57-58, may be of interest to the Committee.

As noted in the abovementioned submission, the proposed new term 'ASIO affiliate' is a label which describes a range of persons, who are not employees, who perform functions or services for ASIO. It is a label which reflects the variety of mechanisms, including secondment and consultancy arrangements, that are used to appropriately resource agencies, including an intelligence agency, to undertake their functions.

The proposed definition of the term 'ASIO affiliate' in amending item 1 of Schedule 1 to the Bill contains a mechanism for ensuring that an ASIO affiliate is an appropriate person to exercise powers for, or perform functions of, the Organisation. An ASIO affiliate is defined as a person who performs functions or services for ASIO pursuant to a contract, agreement or arrangement. An assessment of whether an individual holds the requisite or necessary qualifications to fulfil the requirements of that contract, agreement or arrangement would be an essential criterion taken into account by the Organisation before entering into any contract, agreement or arrangement with that person.

Decisions by the Director-General about the engagement of a person as an ASIO affiliate are consistent with the Director-General's overall control of, and responsibility for the Organisation in s 8, and are subject to the obligation on the Director-General in s 20 to take reasonable steps to ensure that the work of the Organisation is limited to what is necessary for purposes of the discharge of its functions, and to ensure that the Organisation is kept free from any influences or considerations not relevant to its functions, and nothing is done that might lend colour to any suggestion that it is concerned to further or protect the interests of any particular section of the community, or with any matters other than the discharge of its functions. The activities of ASIO in entering into a contract, agreement or arrangement for the performance of functions or services for that Organisation are also subject to the oversight of the IGIS.

In addition, the validity of any activities or actions undertaken by an ASIO affiliate depends on the person acting in accordance with the relevant contract, agreement or

[5] AGD and ASIO, joint supplementary submission to the PJCIS inquiry into the National Security Legislation Amendment Bill (No I) (unclassified), 29 August 2014, pp. 53-58.

arrangement. If an ASIO affiliate exceeds his or her authorisation under the relevant contract, agreement or arrangement, he or she would not be acting as an affiliate, and may also be subject to criminal liability in respect of any unauthorised actions.

Further, as the term 'ASIO affiliate' identifies the pool of persons who might be able to do certain things under legislation, the relevant 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.

Explanation of the consequential amendments in Part 2 of Schedule 1 to the Bill

As the Committee has identified, Part 2 of Schedule 1 to the Bill proposes a number of consequential amendments to provisions of Commonwealth legislation which confers upon ASIO personnel various powers, authorities, duties, obligations, immunities and liabilities. Such personnel are generally referred to '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 generally substitute the phrase "officer or employee' of ASIO" with the phrase "ASIO employee or ASIO affiliate" (or in some instances, use the term 'ASIO employee' or 'ASIO affiliate' alone). In the development of these consequential amendments, consideration was given to consistency with the overarching policy intention of the relevant legislation being amended.

For example, the Committee has specifically referred to amending item 61, which inserts a new s 7(2)(ad) in the *Telecommunications (Interception and Access) Act 1979* (TIA Act). Presently, s 7(2)(ac) of the TIA Act provides that the general prohibition on interceptions in s 7(1) of that Act does not apply to an activity undertaken by an "officer of the Organisation" for the purpose of determining if a listening device is being used, or to determine the location of such a device. Amending item 60 updates this provision to refer to an 'ASIO employee', consequential to amending item 1 of Schedule l. Amending item 61 applies a corresponding exception from s 7(1) in relation to the actions of ASIO affiliates. It is appropriate that the exception to s 7(1) applies to all persons who have been engaged to perform a role within ASIO that may include undertaking these activities. The exception in s 7(2)(ac) is directed to conduct rather than the technical nature of a person's relationship with ASIO. Limiting the exception in s 7(2) of the TIA Act to 'ASIO employees' would result in an arbitrary distinction in relation to the application (or otherwise) of s 7(1).

In recognition of the Committee's comments, I have asked my Department to revise the Explanatory Memorandum to the Bill to include a statement outlining the oversight and control mechanisms in relation to ASIO affiliates, and an elaboration of the need to apply the term, and its legal effect, in relation to each consequential amendment in Part 2 of Schedule 1 to the Bill.

Committee Response

The committee thanks the Attorney-General for this detailed response and for indicating that the explanatory memorandum to the bill will be revised to provide further information in relation to ASIO affiliates.

In light of the detailed explanation above and the proposed revisions to the explanatory memorandum, the committee leaves the question of whether extending certain powers, authorisations and exemptions to 'ASIO affiliates' is appropriate to the Senate as a whole.

Alert Digest No. 11 of 2014 - extract

Insufficiently defined administrative power—exercise of authority under warrant conferred upon a person or class of persons
Schedule 2, item 8, proposed subsection 24(2)

Proposed subsection 24(2) would enable the Director-General (or her or his delegate) to approve a class of persons as people authorised to exercise the authority conferred by relevant warrants or relevant device recovery provisions. The execution of the various warrants under the ASIO Act may involve the exercise of significant coercive powers which are apt to trespass on a number of personal rights and liberties. The explanatory memorandum (at p. 66) justifies this aspect of the amendment by pointing to inefficiencies created by the 'requirement to maintain a list of the individual names of each person involved in exercising authority under a warrant'. It is further argued that:

> Sometimes, the execution of a warrant takes place in unpredictable and volatile environments requiring ASIO to expand the list of individually authorised persons at very short notice (for example, an operational opportunity to exercise the authority of a warrant may be lost before the authorisation list can be updated).

The committee is mindful of these difficulties, however the committee also notes that there are accountability benefits associated with a requirement that persons able to exercise extensive coercive powers be identified with exactness, and that the responsibility for the appointment of such persons be clear. There is a danger that specification of persons able to exercise these extensive powers by reference to a class of persons (1) may be over-inclusive in the sense that particular persons covered may not be appropriately qualified to exercise the powers, and (2) that situations may arise in which it is uncertain whether a particular person is covered by an authorisation of a class of persons. Both of these problems may be thought to lessen the level of accountability associated with the exercise of authority under warrants. **Noting these concerns, the committee seeks the**

Attorney-General's advice as to whether consideration has been given to these matters and whether there are ways in which to address them. The committee is also interested in whether it would be appropriate to provide legislative guidance as to any parameters on the class/es of persons to whom authorisation can be granted and whether the option to authorise classes of persons could be limited to emergency situations (those involving 'very short notice').

> *Pending the Attorney-General's reply, the committee draws Senators' attention to the provision as it may be considered to make rights, liberties or obligations unduly dependent upon insufficiently defined administrative powers in breach of principle 1(a)(ii) of the committee's terms of reference.*

Attorney-General's response - extract

I confirm that consideration has been given to the matters raised by the Committee. Outlined below is further context to the use by ASIO of authorisation lists in relation to the exercise of special powers under warrant.

Context –ASIO's use of authorisation lists

In practice, to ensure compliance with the legislation and provide sufficient operational flexibility, ASIO may need to list a large number of persons as being authorised to carry out warranted activities - though they may not all be required to exercise authority under the warrant.

As a result, an authorisation list is not a record of who carried out authorised activity. Both the existing provision, and the proposed amendment, rely upon ASIO maintaining effective records in relation to the actual execution of the warrant for accountability and oversight purposes. This is an area that the IGIS will continue to inspect and monitor.

It is common that an authorisation list includes a range of persons with the range of skill-sets required. Each person authorised will possess a relevant qualification or a skill; however, not all authorised persons will possess all of the skills and qualifications required to carry out all activities authorised by the warrant. Each person who is authorised will generally perform a particular role within a team. For example, in the case of a search warrant it may be necessary to authorise:

- persons who will facilitate entry to target premises;
- persons who inspect data on a computer at the premises; and
- law enforcement officers who can provide protection to persons carrying out the warranted activities.

Members of a specified class of authorisation can be ascertained by internal records demonstrating who is occupying a certain position or role in ASIO. ASIO has a number of mechanisms and safeguards that are directed at ensuring that ASIO officers have the necessary qualifications, skills and expertise for their position or role including recruitment, training, supervision and performance management regimes.

The ability to authorise classes of persons is consistent with s 55 of the TIA Act which allows classes of officers or employees of ASIO to be authorised to exercise the authority conferred by a Part 2-5 warrant.

The need for operational flexibility means that the current practice, which requires specific officers to be authorised to exercise the authority of a warrant, has led to the authorisation lists including up to 50 names (including, for example, linguists, technical officers, case officers and analysts). The specification of a large number of names to provide operational flexibility does not provide additional meaningful accountability.

Whether legislative guidance as to any parameters on the class or classes of persons to whom authorisation can be granted

Any parameters on the classes of persons to whom authorisations can be granted would need to be sufficiently flexible so as not to defeat the purpose of enabling ASIO to achieve the required operational flexibility. In particular, the amendment seeks to provide ASIO with flexibility to encompass a broad range of appropriate persons to exercise powers under a warrant or request information or documents from operators of aircraft or vessels. I consider it is preferable that existing oversight and accountability mechanisms (including the role of the IGIS in reporting on the propriety with which ASIO carries out its functions) be the means by which ASIO's exercise of special powers, including authorisations of classes of persons, is monitored.

Whether the option to authorise classes of persons could be limited to emergency situations

As noted in the Explanatory Memorandum to the Bill, the execution of a warrant sometimes take place in unpredictable and volatile environments requiring ASIO to expand the list of individually authorised persons at very short notice. An operational opportunity to exercise the authority of a warrant may be lost before an authorisation list can be updated. For this reason, it would be impracticable to provide statutory authority for the Director-General to authorise classes of persons only in emergency situations.

Committee Response

The committee thanks the Attorney-General for this detailed response.

The committee draws this provision to the attention of Senators and leaves the question of whether it is appropriate to allow *a class of persons* to be authorised to exercise the authority conferred by warrants or device recovery provisions to the Senate as a whole.

Alert Digest No. 11 of 2014 - extract

Undue trespass on personal rights and liberties
Schedule 2, item 10, proposed new paragraph 25(4)(aa)
Schedule 2, item 19, proposed new paragraph 25A(4)(aaa)

Proposed new paragraph 25(4)(aa) provides that an authorised person in the execution of a search warrant may enter any premises for the purposes of gaining entry to or exiting the subject premises. The explanatory memorandum (at p. 66) states that:

> …it may occasionally be necessary for an authorised person to enter premises (specifically, third party premises) other than the subject premises in order to enter or exit the subject premises. This may be because there is no other way to gain access to the subject premises (for example, in an apartment complex where it is necessary to enter the premises through shared or common premises). It may also occur where, for operational reasons, entry through adjacent premises is more desirable (for example, where entry through a main entrance may involve a greater risk of detection). The need to access third party premises may also arise in emergency circumstances (for example, where a person enters the subject premises unexpectedly during a search and it is necessary to exit through third party premises to avoid detection and conceal the fact that things have been done under a warrant).

The committee recognises that it may *occasionally* be necessary for an authorised person to enter third-party premises in order to enter or exit the subject premises (as in the circumstances described above). However, the proposed provision is broadly drafted and therefore does not recognise the fact that such a power (noting the potential impact on third parties) should be limited to reflect the exceptional nature of the power.

The committee notes that similar issues arise in relation to computer access warrants in item 19 of Schedule 2.

Noting the above comments, the committee seeks the Attorney-General's advice as to whether it would be possible to constrain the power to enter third-party premises. If it is thought that it would not be possible to further constrain this power in the legislation, a detailed rationale as to why that is the case (and details of any internal safeguards or procedures in place to constrain this power) would assist the committee in assessing the appropriateness of this provision.

Pending the Attorney-General's reply, the committee draws Senators' attention to the provision as it may be considered to trespass unduly on personal rights and liberties in breach of principle 1(a)(i) of the committee's terms of reference.

Attorney-General's response - extract

In my view it would unduly limit the ability of ASIO to carry out its functions if further constraints were placed on the proposed power to enter third party premises. Consideration has been given to submissions made to the PJCIS inquiry into the Bill suggesting that the power to enter third party premises be authorised subject to a 'necessity' test.

Rationale

The purpose of the amendment is to enable ASIO to enter or exit third-party premises where necessary, but also where such entry or exit serves an operational imperative. For example, where entry via adjoining premises allows ASIO to reduce a risk of detection, or where a person unexpectedly arrives at target premises and the safest means of exit is via third party premises. In such circumstances, a requirement to meet a 'necessity test' may preclude ASIO from acting in the most operationally effective and appropriate manner.

The power to enter third party premises does not provide any power to search or otherwise collect intelligence on the third party premises - it is limited to entry to the premises.

Safeguards and procedures that would constrain this power

The range of existing safeguards provide an appropriate and effective framework of checks and balances in respect of ASIO's use of its powers and ensures that ASIO's activities are necessary and proportionate.

The proposed power to enter third party premises can only be exercised under the authority of a warrant. Before I issue a warrant, I must be satisfied that certain thresholds are met. Before entry onto third party premises can be authorised in the warrant, I must consider it appropriate in the circumstances to authorise such entry. In addition, the Attorney-General's Guidelines to ASIO, issued under s 8A of the ASIO Act, require all activities to be done with as little intrusion into individual privacy as possible. Third-party premises

would only be accessed in accordance with these Guidelines. Consistent with the Guidelines, ASIO's methodology and operating procedures place an emphasis on the principle of 'proportionality', and are designed to ensure an appropriate and proportionate response, having close regard to both individual privacy considerations and the potential gravity of the threat being investigated. All warrants are available to the IGIS for inspection pursuant to the IGIS Act.[6]

Committee Response

The committee thanks the Attorney-General for this response and **requests that the key information above be included in the explanatory memorandum.**

The committee emphasises the importance of robust safeguards in relation to potentially intrusive powers (such as access to third party premises by ASIO) and notes the safeguards outlined by the Attorney-General. To assist the committee in further examining these provisions, the committee requests further advice from the Attorney-General in relation to what the legal consequences of a breach of the principle of proportionality contained in the Guidelines (and ASIO's operating procedures) would be and whether consideration has been given to the inclusion of a proportionality requirement in the legislation.

Alert Digest No. 11 of 2014 - extract

Undue trespass on personal rights and liberties
Schedule 2, item 29

Among other things, item 29 of Schedule 2 repeals subsections 26(1) and 26A(1) of the current *Australian Security Intelligence Organisation Act 1979*. These subsections in the current ASIO Act make it unlawful for an ASIO officer, employee or agent to use a listening device, certain optical surveillance devices (that is, devices that fall within the current definition of a 'listening device') and a tracking device, where it would otherwise have been permissible in some States and Territories.

This approach is said to be 'consistent with the Surveillance Devices Act' and justified on the basis that the 'use of surveillance devices is primarily regulated by State and Territory law' and 'any inconsistent use of a surveillance device by ASIO under this framework will, generally, be regulated by State and Territory law' (explanatory memorandum, p. 75). The result is that Subdivision D 'regulates the circumstances where ASIO may use a

[6] See further, AGD and ASIO, joint supplementary submission to the PJCIS (unclassified) 29 August 2014, p. 60; and AGD, supplementary submission (8 September 2014), p. 6.

surveillance device with and without a warrant' and that 'any use outside this framework will generally be regulated by State or Territory law' (explanatory memorandum, p. 77).

It is possible that the repeal of subsections 26(1) and 26A(1) may have the result of making the use of surveillance devices by ASIO lawful in circumstances beyond those authorised by Subdivision D. The explanatory memorandum states that uses not so authorised will *generally* be regulated by State and Territory law.

The committee seeks advice from the Attorney-General as to whether there may be circumstances where use of surveillance devices by ASIO not authorised under Subdivision D may be lawful under State and Territory law and whether, therefore, the repeal of subsections 26(1) and 26A(1) will operate to enlarge the circumstances in which the use of surveillance devices is lawful. Further, if that is so, the committee seeks the Attorney-General's advice as to the rationale for not dealing comprehensively with the legality of the use of surveillance devices by ASIO in the ASIO Act.

> *Pending the Attorney-General's reply, the committee draws Senators' attention to the provision as it may be considered to trespass unduly on personal rights and liberties in breach of principle 1(a)(i) of the committee's terms of reference.*

Attorney-General's response - extract

Circumstances in which the use of surveillance devices is lawful

The proposed removal of the general prohibitions in ss 26(1) and 26A(l) of the ASIO Act is consistent with the approach taken and the rationale for introducing a surveillance device framework under the *Surveillance Devices Act 2004.*

The general prohibition of ASIO officers' use of surveillance devices reflects the Commonwealth preference for legislating some 35 years ago, at a time when the regulation of the use of listening devices by the states and territories was in its infancy. Today, a selective prohibition of this nature stands alone among Australian jurisdictions. Rather than prohibiting the use of surveillance devices, the Bill establishes a structured process for the use of surveillance devices that is clear and transparent. The draft provisions set out when an ASIO officer 'may' use a particular surveillance device without a warrant. This approach is similar to the regime applicable to Commonwealth law enforcement officers set out in the Surveillance Devices Act.

A blanket prohibition is enduring and removes the ability for the use of surveillance devices to be regulated by States and Territories. For example, an amendment in 1986 to s 22 of the ASIO Act incorporated in the definition of a 'listening device' a device that can

record images. The effect of the prohibition in s 26(1) is to make it unlawful for an ASIO officer to record images that are being communicated. Although the content of this prohibition is unclear, no other jurisdiction in the country would outlaw the covert photography of images being communicated by ASIO in and of itself. Nonetheless, the confusion and the possibility that an ASIO officer may inadvertently act unlawfully in recording an image being communicated is solely the result of the general prohibition in s 26(1).

The use of surveillance devices is normally regulated by State and Territory law and these regimes are generally more permissive than the ASIO Act - for example, some State regimes do not regulate the use of particular devices at all. The starting point for the use of surveillance devices under the ASIO Act is to prohibit all such use by ASIO officers (ss 26(1) and 26A(l) of the ASIO Act) and then to authorise particular use in certain circumstances. For this reason, the proposal to remove the general prohibition on the use of surveillance devices that currently appears in the ASIO Act will generally result in the enlargement of circumstances in which ASIO's use of surveillance devices without warrant is permitted. Examples of the practical effect of the repeal include:

- In some states, such as Queensland and South Australia, there is no general prohibition on the use of optical surveillance devices. In these jurisdictions, ASIO officers would be free to use such devices were it not for s 26(1) of the ASIO Act. The latter provision prohibits an ASIO officer from using a hand-held camera in certain circumstances except pursuant to a warrant or the specific circumstances listed in the ASIO Act. No such prohibition is imposed on other parts of the community such as private investigators, foreign intelligence officers or law enforcement officers. The removal of s 26(1) will align the permissible activities of ASIO officers with other members of the community.

- In some states, (for example, South Australia, Queensland, Tasmania and the Australian Capital Territory), it is not otherwise unlawful for persons to use a tracking device. The repeal of s 26A(l) will make uniform the application of tracking device laws in those States or Territories, irrespective of whether the person is an ASIO officer.

- The removal of the prohibition will also expand the circumstances in which the use of listening devices without warrant is lawful in certain jurisdictions. This is because the Acts relating to surveillance devices in those jurisdictions exempt ASIO from the operation of those provisions. For example, s 5(b) of the *Surveillance Devices Act 1999* (Vic) provides that nothing in that Act applies to anything done in the course of duty by the Director-General or an officer or employee of ASIO. A similar provision exists in the Western Australian and Tasmanian legislation. (I note, however, that where the installation, use, maintenance or recovery of surveillance devices contravenes any other law - for example, because it amounts to a trespass - such use of surveillance devices will not be permitted without a warrant.)

- The ASIO Act has not kept pace with developments in other Australian jurisdictions. For example, s 26(1) comprehensively states the circumstances in which ASIO may use a listening device. The removal of s 26(1) will bring ASIO's use of listening devices in line with State and Territory surveillance device legislation by pe1mitting the use of a listening device for the purpose of protecting the lawful interests of the ASIO officer, which is permitted in most other jurisdictions.

Rationale for "not dealing comprehensively with the legality of the use of surveillance devices by ASIO in the ASIO Act"

As the Committee has identified, Division 2 of Part III of the ASIO Act is not an exhaustive or comprehensive statutory 'code' in relation to the legality of the use of surveillance devices by ASIO, and is not intended to serve such a purpose. No comprehensive statute exists under Australian law in relation to the use of surveillance devices by any other entity, whether a law enforcement agency, an intelligence agency, or any other person or organisation. Legislative responsibility with respect to the use of surveillance devices is divided between the Commonwealth and the States and Territories, and regulation is subject to both statute and common law.

The measures proposed in item 29 of Schedule 2 to the Bill reflect the recommendation of the PJCIS in its 2013 *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation* that the ASIO Act be amended "to modernise the warrant provisions to align the surveillance device provisions with the *Surveillance Devices Act 2004*, in particular by optical devices" (recommendation 30). The PJCIS was motivated by a desire to align, to the extent possible, ASIO's surveillance powers for intelligence purposes with those in the Surveillance Devices Act, the main purpose of which is to regulate surveillance device operations by law enforcement agencies (per s 3 of the Surveillance Devices Act).

Consistent with my comments above, the Surveillance Devices Act does not purport to deal comprehensively with the legality of the use of surveillance devices by law enforcement agencies and, accordingly, this approach has been replicated in the ASIO Act. The Surveillance Devices Act was developed in consultation with the States and Territories, and was intended to serve as a model for the enactment of surveillance legislation in States and Territories to regulate matters within their jurisdictions (recognising that the Commonwealth does not have a general power to legislate with respect to criminal law or law enforcement).

As the Government intends to limit the proposed amendments to ASIO's surveillance powers in the Bill to the implementation of recommendation 30 of the PJCIS's 2013 inquiry, I do not propose that the Bill should make broader amendments to cause the ASIO Act to deal comprehensively with the legality of the use of surveillance devices by ASIO.

Committee Response

The committee thanks the Attorney-General for this detailed response and **requests that the key information above be included in the explanatory memorandum.**

The committee notes that the repeal of current subsections 26(1) and 26A(1) of the ASIO Act will operate to enlarge the circumstances in which the use of surveillance devices by ASIO personnel is lawful. The committee further notes that the effect of this amendment will, in certain circumstances, align the legality of ASIO's use of surveillance devices with that of other members of the community (such as private investigators, foreign intelligence officers or law enforcement officers). The committee notes, however, that the assessment of whether ASIO's use of surveillance devices should be aligned with other members of the community should also be considered in light of ASIO's further extensive and coercive powers. The committee therefore draws this provision to the attention of Senators and leaves the question of whether the proposed approach is appropriate to the Senate as a whole.

Alert Digest No. 11 of 2014 - extract

Undue trespass on personal rights and liberties
Schedule 2, item 29, proposed section 26F

Proposed section 26F allows the Director-General to determine that specified powers under the ASIO Act (section 26C or 26D or subsection 26E(1) or (2)) cannot be exercised by specified persons. This measure is said to be 'an important safeguard in ensuring that, while a particular individual, or class of individuals, may be appropriately performing certain functions or services for ASIO, they are not within the categories of persons who can perform ASIO's powers by use of surveillance devices without warrant' (explanatory memorandum, pp 78–79).

Given the importance of this objective, that is, ensuring that the use of surveillance devices without warrant is used by appropriately qualified ASIO staff, **the committee seeks further advice from the Attorney-General as to whether consideration has been given to excluding 'ASIO affiliates' from the exercise of these powers unless they are positively determined to be appropriate persons to exercise such powers. The committee notes that this approach would provide a more robust safeguard than the current proposed approach. It is not clear from the explanatory memorandum whether this alternative has been considered.**

Pending the Attorney-General's reply, the committee draws Senators' attention to the provision as it may be considered to trespass unduly on personal rights and liberties in breach of principle 1(a)(i) of the committee's terms of reference.

Attorney-General's response - extract

The existing provisions of Division 2 of Part III of the ASIO Act already provide that ASIO may use surveillance devices without a warrant, including by agents of ASIO, albeit, in limited circumstances (especially when compared to law enforcement). The inclusion of agents in the relevant provisions recognises that, in some circumstances, it may be appropriate for persons who are not employees of ASIO to use a surveillance device, for a purpose relating to security - for example, a person seconded to ASIO may be required to use a listening device to conduct a security interview with a person with that person's consent. The concept of an 'ASIO affiliate' replaces the term 'agent of the Organisation' as used in the existing provisions, and offers greater transparency ac; to who may use surveillance devices without warrant as its scope is defined in the Bill.

As I have mentioned above, the practical effect of the definition of the term 'ASIO affiliate', and the circumstances in which it is used across legislative provisions, is that such persons are 'positively determined' to be appropriate persons to exercise powers such as the use of surveillance devices without warrant. The validity of any activities or actions undertaken by an ASIO affiliate depends on the person acting in accordance with the relevant contract, agreement or arrangement. If it was envisioned that an ASIO affiliate would be in a position to exercise such a power, the suitability of that individual would be a relevant criteria taken into account before entering into a contract, agreement or arrangement with the individual to perform that particular role.

Further, the proposed framework for ASIO's use of surveillance devices without a warrant draws from Commonwealth, State and Territory surveillance device legislation. Such frameworks do not make unlawful, the use of surveillance devices in certain circumstances. For example, the use of tracking devices with consent is not prohibited in any State or Territory. Where there is no such prohibition, I do not consider there to be a justification for requiring an ASIO affiliate to be separately authorised to engage in activities that an ordinary member of the public is not prohibited from engaging in. l remain of the view that the inclusion of proposed s 26F provides an additional, and robust, safeguard consistent with that envisioned by the Committee in Alert Digest No. 11 of 2014.

Committee Response

The committee thanks the Attorney-General for this response and **requests that the key information above be included in the explanatory memorandum. The committee leaves the question of whether the proposed approach in relation to the authorisation of 'ASIO affiliates' to use surveillance devices without a warrant is appropriate to the Senate as a whole.**

Alert Digest No. 11 of 2014 - extract

Undue trespass on personal rights and liberties
Schedule 2, item 36

This item inserts the new words, 'against persons and things' after 'any force' in existing paragraph 27A(2)(a). It thereby clarifies that persons executing warrants under this section can 'use reasonable force against both persons and things in executing that warrant where the use of force is both reasonable and necessary' (explanatory memorandum, p. 80).

In general the committee expects that the necessity of authorising force against persons in the execution of warrants to be examined and justified in explanatory memoranda. **The committee therefore seeks the Attorney-General's advice as to the justification for the authorisation of force against persons in this context.**

> *Pending the Attorney-General's reply the committee draws Senators' attention to the provision as it may be considered to trespass unduly on personal rights and liberties in breach of principle 1(a)(i) of the committee's terms of reference.*

Attorney-General's response - extract

My Department and ASIO recently provided detailed evidence to the PJCIS in relation to this matter.[7]

[7] AGD, responses to questions taken on notice on 15 August 2014 (18 August 2014), pp. 10-12; AGD and ASIO, joint supplementary submission (unclassified) (29 August 2014), pp. 61-62.

In summary, 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.

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. This could occur, for example, through a person preventing access to a room or an item or preventing a person authorised to execute the warrant from leaving the premises by blocking the exit. In the absence of the ability to use reasonable force against a person, any person seeking to obstruct the execution of the warrant could do so by standing in a doorway so that anyone seeking to go through that doorway would come into physical contact with them. If, in pushing past a person obstructing a doorway, the person executing the warrant came into physical contact with the person obstructing their access, the person executing the warrant may have committed an assault. In the absence of a power to use reasonable force in the execution of a warrant, this would not be authorised and could potentially lead to civil action or criminal charges.

Additionally, where police assist in the execution of an ASIO search warrant, they rely on the powers available to them under the warrant, rather than any generic police power. This means that they would rely on the ability in the ASIO Act to use force, the absence of such a power would hamper police. Further, while ASIO will often request law enforcement attendance at the execution of warrants, police will not be present in all instances.

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 cannot constitute grievous bodily harm or lethal force. Any use of unauthorised force against a person may attract civil and criminal liability.

Committee Response

The committee thanks the Attorney-General for this detailed response.

The committee notes that the Attorney-General has provided details as to why it may be considered necessary to use force against persons in the execution of warrants, and that any use of unauthorised force against a person may attract civil and criminal liability. **The committee requests that the key information above be included in the explanatory memorandum.**

(continued)

The committee also takes this opportunity to note recommendations 6 and 7 of the Parliamentary Joint Committee on Intelligence and Security's report into the bill. In particular, the committee considers that it would be appropriate for ASIO to be required to notify the Attorney-General and the IGIS within 24 hours of any incident in which force is used against a person by an ASIO officer, and for a written report on the incident to be provided within 7 days. The committee also agrees that it would be appropriate that the IGIS provide close oversight of the design and execution of training for ASIO personnel who may be required to use force during the execution of warrants.

The committee draws this provision to the attention of Senators and leaves the question of whether the proposed approach is appropriate to the Senate as a whole.

Alert Digest No. 11 of 2014 - extract

Undue trespass on personal rights and liberties—evidentiary certificates Schedule 2, item 47, proposed section 34AA

This provision is said to be based on similar provision in the *Telecommunications (Interception and Access) Act 1979* and the *Surveillance Devices Act 2004* (the SD Act). However section 62 of the SD Act contains the following additional provisions:

- (5) A certificate must not be admitted in evidence under subsection (2) in prosecution proceedings unless the person charged or a solicitor who has appeared for the person in those proceedings has, at least 14 days before the certificate is sought to be so admitted, been given a copy of the certificate together with reasonable evidence of the intention to produce the certificate as evidence in those proceedings.

- (6) Subject to subsection (7), if, under subsection (2), a certificate is admitted in evidence in prosecution proceedings, the person charged may require the person giving the certificate to be called as a witness for the prosecution and cross-examined as if he or she had given evidence of the matters stated in the certificate.

- (7) Subsection (6) does not entitle the person charged to require the person giving a certificate to be called as a witness for the prosecution unless the court before which the prosecution proceedings are brought, by order, allows the person charged to require the person giving the certificate to be so called.

- (8) Any evidence given in support, or in rebuttal, of a matter stated in a certificate given under subsection (2) or (3) must be considered on its merits and the credibility

and probative value of such evidence must be neither increased nor diminished by reason of this section.

These subsections, especially (5) and (6) appear to provide further safeguards, and the committee is interested in whether analogous provisions would be appropriate in this context. The *Guide to Framing Commonwealth Offences, Infringement Notices and Enforcement Powers* states (p. 55) that 'procedural safeguards have generally been included with provisions for evidentiary certificates directed to a technical/scientific context', but does not specify examples. The explanatory memorandum explains how this provision works but it is not clear why it has been considered necessary to include it. **The committee therefore seeks the Attorney-General's advice as to the justification for the proposed approach, including whether the additional provisions outlined above would be appropriate in this context.**

Pending the Attorney-General's reply the committee draws Senators' attention to the provision, as it may be considered to trespass unduly on personal rights and liberties, in breach of principle 1(a)(i) of the committee's terms of reference.

Attorney-General's response - extract

While ASIO's role is to gather intelligence in accordance with its statutory functions set out in s 17 of the ASIO Act, there are occasions on which intelligence gathered by ASIO may be used in evidence in court to support criminal prosecutions or in civil proceedings. Most of the major counter-terrorism prosecutions conducted to date have made use of intelligence in evidence.

In adducing such evidence, it is important that ASIO's sensitive capabilities, including the identity of ASIO employees and others giving evidence, are not exposed in open court. In its 2013 *Report on Potential Reforms to National Security Legislation*, the PJCIS recognised the "legitimate need to protect the technological capabilities of ASIO where information under warrant is eventually led in evidence as part of the prosecution" (at pages 132-133).

Consistent with the recommendation of the PJCIS in that inquiry, proposed s 34AA will provide a mechanism to minimise the risk of revealing technical capabilities and the identity of ASIO employees or sources in evidence in proceedings. The proposed provision will also reduce the need for senior ASIO officers and other expert technical witnesses to be diverted from their duties to attend court and give evidence concerning the execution of warrants and the use of the information obtained from the warrants.

Proposed s 34AA is intended to operate in a manner that will ensure the veracity of the information gathered can be tested by the court, as certificates are of a prima facie rather

than conclusive nature. An accused person in criminal proceedings, or a party to civil proceedings, could therefore lead evidence to challenge the matters set out in a certificate.

In addition, the proposed provision is not intended to authorise the issuing of certificates to facilitate proof of any ultimate fact, or any fact so closely connected with an ultimate fact as to be indistinguishable from it, or facts that go to elements of the offence. Rather, certificates must relate to the technical matters set out in proposed s 34AA(3). Evidence adduced in support of an ultimate fact, or an element of an offence, will continue to be capable of protection under existing mechanisms such as those available under the *National Security Information (Criminal and Civil Proceedings) Act 2004.* In the event that a party to proceedings, or a presiding judge on his or her own initiative, was concerned that a certificate purported to apply to material facts or facts that would address or prove the ultimate facts in the case (or elements of an offence), the certificate could be struck out on the basis it has exceeded the limits of s 34AA.[8]

On this basis, I am of the view that proposed s 34AA strikes an effective balance between the protection of sensitive information pertaining to operational capability and the identity of sources, procedural fairness and operational efficiency.

Consideration of possible additional provisions

As the Committee has observed, proposed s 34AA is based upon similar regimes operating under the TIA Act and the Surveillance Devices Act. Due to the nature of the information associated with the execution of computer access and surveillance device warrants, it is not possible for the provision to exhaustively list the specific facts or matters that may be covered by a certificate issued under this section without putting at risk the very capabilities the regime is designed to protect.

Consideration was given to the possible inclusion in proposed s 34AA of provisions similar to those set out in ss 62(5)-(8) of the Surveillance Devices Act. On balance, it was considered it would not be appropriate to include these provisions. In some instances they would not be feasible in light of the classified nature of evidence to which they relate, and in others would unnecessarily duplicate powers already available to the court.

In particular, s 62(5) of the Surveillance Devices Act limits the court from admitting a certificate in evidence if the person charged or solicitor engaged by them has not had at least 14 days' notice as well as a copy of the certificate and reasonable evidence of the intention to produce the certificate. Certificates issued by ASIO under the TIA Act have generally borne a national security classification, as they contain facts and information that would damage national security were it to be publicly released. Noting the certificates to be issued under proposed s 34AA are designed to protect ASIO's capabilities and the identity of sources or staff, they too would likely be highly classified and therefore unable

[8] See further, AGD and ASIO joint supplementary submission to the PJCIS inquiry into the National Security Legislation Amendment Bill (No 1) 2014 (unclassified) 29 August 2014, p. 62. See also: pp. 13-14 of the Explanatory Memorandum to the Bill (Human Rights Statement of Compatibility).

to be released to a person charged, or their lawyer in an unamended form. This would make compliance with a similar provision difficult.

In addition, ss 62(6)-(8) of the Surveillance Devices Act are statements of powers that are already available to the court in a criminal prosecution when dealing with evidentiary certificates. The court's inherent powers already allow it to order that specific witnesses are called in respect of certain evidence, and the court must also consider the evidence on its merits, with no weighting or credibility to be taken from the section establishing the ability to issue evidentiary certificates. It is, in my view, appropriate to leave these matters to the domain of the court in those proceedings in which a certificate is relevant.

Committee Response

The committee thanks the Attorney-General for this detailed response and **requests that the key information above be included in the explanatory memorandum**. **The committee draws this provision to the attention of Senators and leaves the question of whether the proposed approach is appropriate to the Senate as a whole.**

Alert Digest No. 11 of 2014 - extract

Undue trespass on personal rights and liberties—immunity from civil and criminal liability
Schedule 3, general comment

Schedule 3 of the bill proposes to establish a statutory framework for the conduct of 'special intelligence operations' (SIOs), which includes granting limited immunity from civil and criminal liability for conduct undertaken by ASIO in an SIO.

The committee notes that the creation of such a scheme was recommended by the Parliamentary Joint Committee on Intelligence and Security in its *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation* (May 2013). Specifically, the committee recommended 'that the *Australian Security Intelligence Organisation Act 1979* be amended to create an authorised intelligence operations scheme, subject to similar safeguards and accountability arrangements as apply to the Australian Federal Police controlled operations regime under the *Crimes Act 1914*.' The explanatory memorandum to the bill (at p. 96), however notes that:

> While the SIO scheme is based broadly on the controlled operations scheme in the Crimes Act, appropriate modifications have been made to reflect the differences between a law enforcement operation to investigate a serious criminal offence in

order to gather admissible evidence, and a covert intelligence-gathering operation conducted for national security purposes.

The committee notes that it would assist the committee's scrutiny of this schedule if it were aware (in a systematic manner) of the differences between the proposed SIO scheme and the controlled operations scheme. **The committee therefore requests advice from the Attorney-General as to the differences between the proposed SIO scheme in schedule 3 of the bill and the controlled operations scheme in Part IAB of the *Crimes Act 1914*. In particular, the committee is interested in information as to:**

- **any differences in the authorisation process (including matters on which authorising officers must be satisfied);**
- **any differences in the immunities (civil and criminal) provided in the two schemes;**
- **any differences in reporting and oversight mechanisms; and**
- **any other safeguards which are present in the controlled operations scheme that are not replicated in the proposed SIO scheme.**

Pending the Attorney-General's reply the committee draws Senators' attention to the provision, as it may be considered to trespass unduly on personal rights and liberties, in breach of principle 1(a)(i) of the committee's terms of reference.

Attorney-General's response - extract

This issue has been the subject of extensive consideration by the Parliamentary Joint Committee on Intelligence and Security (PJCIS). On 29 August 2014, my Department and ASIO provided a detailed submission to that Committee, which included a systematic identification and explanation of differences between the two schemes.

Pages 27-30 of that submission address the authorisation process (specifically the authorising officer, including responses to suggestions that an external or Ministerial authorisation model could be adopted in relation to SIOs). Pages 31-48 address all other areas of differences, including the authorisation process, protections from legal liability, reporting and oversight mechanisms, and other safeguards. A table summarising the key areas of difference is also provided at attachment 1 to that submission (pages 86-96).[9]

[9] The Committee may also be interested in the commentary at pages 67-69, addressing two further matters raised by some submitters to the PJCIS inquiry, concerning the policy and operational justification for the scheme, and whether it should be subject to a sunset provision and a statutory review requirement after five years of operation.

By way of general observation, and as noted at page 31 of the abovementioned submission, the proposed SIO regime is based upon, and largely analogous to, controlled operations in Part IAB of the Crimes Act. These include 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 specific purposes of each scheme - namely, the collection of intelligence in the case of SIOs, and obtaining evidence that may lead to a prosecution in relation to serious criminal offences in the case of controlled operations.

In particular, SIOs are directed to covert operations for the purpose of collecting intelligence relevant to security, consistent with ASIO's statutory functions. As such, SIOs will be directed to obtaining intelligence, typically over an extended 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. 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, it is important that the guiding principle in designing the SIO scheme - and in assessing its individual provisions - is that of suitability for the 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 IAB of the Crimes Act is a relevant consideration, it is important that this assessment is not reduced to a more perfunctory exercise in identifying technical 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.

As outlined in the relevant passages of [the submission], key areas of difference include: the definition of an SIO compared to the definition of a 'controlled operation'; the duration of authorisations; relevant authorising officers; aspects of 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 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.

Committee Response

The committee thanks the Attorney-General for this detailed response and for providing the committee with a copy of the Attorney-General's Department/ASIO submission to the Parliamentary Joint Committee on Intelligence and Security, which includes a systematic identification and explanation of differences between the proposed SIO scheme in schedule 3 of the bill and the controlled operations scheme in Part IAB of the *Crimes Act 1914*.

The committee requests that the relevant contextual information above and a summary of the differences between the proposed SIO scheme and the controlled operations scheme be included in the explanatory memorandum.

The committee also takes this opportunity to note recommendations 9 and 10 of the Parliamentary Joint Committee on Intelligence and Security's report into the bill. In particular, the committee considers that it would be appropriate to require that approval must be obtained from the Attorney-General before an SIO is commenced, varied, or extended beyond six months and that it would be appropriate to implement the enhancements to the IGIS's oversight of the proposed SIO scheme as recommended by the PJCIS.

Alert Digest No. 11 of 2014 - extract

Undue trespass on personal rights and liberties—use of evidence obtained as a result of a person engaging in criminal activity
Schedule 3, item 3, proposed section 35A

Proposed section 35A modifies the operation of the courts' general discretion to exclude evidence obtained through unlawful conduct. Subsection 35A(2) provides that in determining whether evidence should be admitted or excluded, the fact that the evidence was obtained as a result of criminal activity is to be disregarded if the person was an authorised participant in an SIO (special intelligence operation) and the criminal activity was special intelligence conduct (i.e. conduct for which a person would, but for section 35K, be subject to civil or criminal liability). This modification to the rules of evidence may be considered to affect rights associated with the provision of a fair trial. The explanatory memorandum (p. 100) justifies the modification as follows:

> It is appropriate that section 35A provides statutory guidance in the exercise of judicial discretion concerning the admissibility in evidence of information

obtained during an SIO. While the focus of an SIO is on the collection of intelligence as distinct from evidence, it is appropriate as a matter of policy to remove the possibility that the discretion to exclude such evidence might be exercised by reason of its connection with an SIO alone. Section 35A makes clear that such evidence is able to be adduced if it is otherwise admissible in accordance with general rules of evidence. For example, evidence gathered via an SIO might be excluded on the basis that its probative value is outweighed by its prejudice to the interests of a party.

It is an appropriate starting point that information obtained in an SIO is admissible in accordance with general rules of evidence, as distinct from a general prohibition on the admissibility of such information in evidence, subject to limited exceptions. With the increasing crossover of laws regulating conduct that was previously exclusively in the security intelligence realm, there has been an increase in interoperability between ASIO and law enforcement. In particular, there has been an increase in the need for intelligence collected by ASIO to be used as evidence in the prosecution of these offences. An example of this, as evidenced in completed prosecutions for terrorism offences, is in relation to offences concerning acts which are preparatory to terrorist acts, such as collecting or making documents likely to facilitate a terrorist act under section 101.5 of the Criminal Code.

The committee notes this justification, however the committee requests further advice from the Attorney-General as to whether this approach is consistent with that taken in relation to the controlled operations scheme in Part IAB of the *Crimes Act 1914* and, if it is not, a rationale as to why a different approach is required for special intelligence operations.

Pending the Attorney-General's reply the committee draws Senators' attention to the provision as it may be considered to trespass unduly on personal rights and liberties in breach of principle 1(a)(i) of the committee's terms of reference.

Attorney-General's response - extract

Proposed s 35A is consistent with s 15GA of the *Crimes Act 1914.* Subsection (2) of each provision ensures that information obtained, respectively, through a special intelligence operation (SIO) or a controlled operation can be admitted in evidence in proceedings without being subject to challenge, or excluded, merely because it was obtained through authorised conduct that would, but for the authorisation, have constituted an offence.

Importantly, neither proposed s 35A(2) nor s 15GA(2) require a court to admit such evidence. Rather, and in response to *Ridgeway v The Queen* (1995) 184 CLR 19, These

provisions operate only to remove the risk that a court might exercise its discretion to exclude such evidence by mere reason of its connection with a special intelligence operation or a controlled operation. They otherwise preserve the general judicial discretion to admit or exclude evidence, and to accord an appropriate degree of weight to evidence admitted.

I note that s 15GA(2) of the Crimes Act has been in force since 2010, following its enactment in the *Crimes Legislation Amendment (Serious and Organised Crime) Act 2010* (Bill of 2009). I am advised that no practical issues have arisen in its use to date. I am also aware that a similar explanation to that at page 100 of the Explanatory Memorandum to the present Bill is provided at page 51 of the Explanatory Memorandum to the 2009 Bill, which did not attract comment from this Committee as constituted in 2009.[10]

Committee Response

The committee thanks the Attorney-General for this response and notes that proposed s 35A is consistent with s 15GA of the *Crimes Act 1914*. **The committee requests that the key information above be included in the explanatory memorandum.**

Alert Digest No. 11 of 2014 - extract

Undue trespass on personal rights and liberties—immunity from civil and criminal liability
Schedule 3, item 3, proposed sections 35D and 35H

Proposed section 35H describes the effect of a special intelligence operation (SIO) authority. The provision provides that an SIO authority has the effect of authorising 'each person who is identified…to engage in the special intelligence conduct specified in the special intelligence operation authority in respect of that person'. As stated in the explanatory memorandum, proposed section 35H is 'material to the application of the protection from criminal or civil liability in section 35K, which is strictly limited to conduct authorised under an SIO authority' (p. 107).

From a scrutiny perspective, it is a matter of concern that it is quite possible that the limits of conduct authorised by an SIO authority may not be clear. The result is that the extent of the trespass on personal rights occasioned by the immunity from liability will also not be clear. Proposed section 35D sets out the required content of a special intelligence operation authority. Paragraph 35D(1)(c) provides that the authority must 'state a general description

[10] Alert Digests No 9 and No 15 of 2009, and Report No 10 of 2009.

of the nature of the special intelligence conduct that the persons referred to' in the authority 'may engage in'.

Under the provisions of the bill in its current form the limits of authorised conduct under an SIO may be unclear because an SIO authority is only required to state authorised conduct in general terms. The committee therefore seeks the Attorney-General's advice as to whether it is possible to require authorised conduct to be particularised with more clarity.

> *Pending the Attorney-General's reply the committee draws Senators' attention to the provision as it may be considered to trespass unduly on personal rights and liberties in breach of principle 1(a)(i) of the committee's terms of reference.*

Attorney-General's response - extract

Proposed s 35D(1)(c) requires an SIO authority to provide a general description of the nature of the special intelligence conduct in which the persons referred to in paragraph (b) are authorised to engage. Proposed s 35H has the effect of authorising each person listed in the SIO authority to engage in the conduct set out therein. The immunity from legal liability in proposed s 35K applies to persons and conduct duly authorised.

A requirement for a general description of the nature of authorised conduct reflects a need for operational flexibility over the 12-month duration of an SIO, consistent with the purpose of such operations to gain close access to persons or organisations of security concern and to build a picture of them, which generally requires these operations to be undertaken over a sustained period of time. As such, it would not be practicable to require an SIO authority to include a significantly higher degree of particularisation of conduct in advance of the commencement of an operation.

For example, while it would be feasible to identify the general nature of conduct to be engaged in as part of an SIO (such as associating or participating in training with members of a terrorist organisation) it is unlikely to be possible to identify individual actions for the purpose of providing prior authorisation (such as authorising specified times or places of association with an organisation, particular training activities, or potentially individual members or affiliates of that organisation with whom participants in an SIO can associate).

Accordingly, the requirement in proposed s 35D(1)(c) that the SIO authority must "state a general description of the nature of the special intelligence conduct" is intended to remove any risk that the immunity in proposed s 35K may be found not to apply because an authorisation did not particularise an individual action, notwithstanding conduct of that general nature was authorised. This is consistent with the purpose of the proposed SIO scheme, to ensure that there is adequate certainty in relation to the legal status of

participants in such operations, in preference to relying solely on prosecutorial and investigative discretion after they have engaged in the relevant conduct as part of an intelligence operation.

Additionally, given the possible application of various State and Commonwealth criminal laws in relation to any particular authorised conduct, it will not be practicable to specifically define and detail with absolute precision such conduct without an exhaustive comparison of all possible criminal laws that might apply. Criminal offences can often broadly overlap and have application in relation to certain general conduct. Yet the specific elements of such applicable offences will vary from jurisdiction to jurisdiction or from offence to offence. For example, a specific authorisation in relation to being a member of a terrorist organisation, without more, may render the person liable to other related offences, such as 'association', 'training' and 'possession' offences, as well as the offence of 'other acts done in relation to planning or preparing for terrorist acts' as found in the Criminal Code. More broadly, the person may also be liable for offences applicable State offences in some instances. Accordingly, to provide certainty to persons participating in an SIO in relation to the application of the immunity provisions, the authorised conduct can only described in general terms rather than any attempt to meet the elements of particular offences.

The latitude provided for in proposed s 35D(l)(c) is caveated by a number of significant safeguards. Under proposed s 35C(2), an authorising officer may only grant an SIO authority if he or she is satisfied, among other things, that any unlawful conduct will be limited to the maximum extent consistent with conducting an SIO. The authorising officer must also be satisfied that the operation will assist the Organisation in performing one or more of its special intelligence functions, and the circumstances are such as to justify the conduct of an SIO. The degree to which conduct is particularised in an application, or is capable of being particularised, will be relevant to an assessment of these matters. Decisions about the authorisation and conduct of an SIO - including the degree of conduct particularised – are subject to independent oversight by the IGIS, who is empowered to inquire into the legality and propriety of ASIO's actions.

In addition, authorisations granted under proposed s 35C, and the immunity under proposed s 35K, cannot extend to conduct that causes death or serious injury, involves the commission of a sexual offence, results in significant loss of or damage to property, or which involves conduct in the nature of 'entrapment'. Proposed s 35L further provides that an SIO authority cannot authorise conduct that requires authorisation in accordance with a warrant issued under the ASIO Act or Part 2-2 of the *Telecommunications (Interception and Access) Act 1979,* or an authorisation made under Part 4-1 of the latter Act. An SIO authority can also be granted on any conditions the authorising officer may decide to apply under proposed s 35C(3), which could include further limitations on authorised conduct *as* appropriate. Further, as I have noted above, the Attorney-General may issue written guidelines under s 8A of the ASIO Act regarding the performance by ASIO of its functions or the exercise of its powers in relation to SIOs.

Given that the intention of the SIO scheme is to provide legal certainty to ASIO and individual participants in respect of the conduct of an SIO, it is in ASIO's operational interests to ensure that there is clarity, in advance, as to the conduct that is authorised as part of such an operation. If doubt arose as to whether a participant was authorised to undertake a particular activity as part of an SIO, it would be open to an authorising officer to vary the authority (on application or on his or her own motion) to authorise or exclude the relevant activity as appropriate. In the event there was doubt that a participant's action was authorised under an SIO authority, the matter may be referred to the Australian Federal Police for investigation, and if appropriate subsequently referred to the Commonwealth Director of Public Prosecutions, in accordance with normal law enforcement processes.

As indicated in the joint submission of my Department and ASIO to the PJCIS of 29 August 2014, the Government is giving further consideration to additional reporting and notification requirements to the IGIS, to enhance opportunities for oversight. This includes consideration of a requirement to notify the IGIS when an authority is issued, and when certain kinds of authorised conduct are engaged in.[11]

Recognising the Committee's concerns, however, I have also asked my Department to give consideration to whether the policy intent could be achieved by removing the word 'general' from the s 35D(l)(c) so that an SIO authority is required to include a statement of the nature of the authorised conduct, combined with an explanation of the intended meaning in the Explanatory Memorandum.

I note that the word 'general' is not used in the corresponding provisions of the Crimes Act in relation to controlled operations, ss 15GK(l)(f)(i) and 15GK(2)(f)(i). It has been included in proposed s 35D(l)(c) due to concerns to remove any ambiguity as to the requisite degree of particularisation in a description of the nature of the relevant conduct under an SIO authority.

Such ambiguity may arise because, unlike the controlled operations scheme, the proposed SIO scheme does not distinguish between civilian and non-civilian participation.[12] The controlled operations scheme distinguishes between the degree of particularisation required in controlled operations authorities for the authorised conduct of civilian and law enforcement participants respectively. Subparagraph (i) of ss 15GK(l)(f) and 15GK(2)(f) require an authority to specify "the nature of the controlled conduct" in which a law enforcement participant may engage. Subparagraph (ii) of the above provisions requires an authority to set out "the particular controlled conduct" in which a civilian participant may engage. As such, an interpretation of the degree of particularisation required by subparagraph (i) of ss 15GK(l)(f) and 15GK(2)(f) can be informed by reference to the comparatively higher degree of specificity required in subparagraph (ii).

---

[11] AGD and ASIO joint supplementary submission to the PJCIS, 29 August 2014, pp. 29-30.

[12] The reasons for this approach have been mentioned in response to question 11 above, and are further explained in Enclosure 2 (pp. 34-35).

As this interpretive approach is necessarily unavailable in relation to proposed s 35D(l)(c), since the SIO scheme does not distinguish between civilian and non-civilian participation, the inclusion of the word 'general' in the provision was considered appropriate to evince an intention that particular actions do not, as a matter of law, need to be specified in an SIO authority (and ensuring that an authorising officer may exercise his or her discretion in an individual case to limit an authority to specific actions, if considered appropriate).

Committee Response

The committee thanks the Attorney-General for this detailed response and notes the rationale provided for not requiring authorised conduct under an SIO to be particularised with more clarity. **The committee welcomes the fact that the government is giving further consideration to providing for additional reporting and notification requirements to the IGIS in relation to the proposed SIO scheme. The committee also welcomes the introduction by the Attorney-General of a proposed amendment to s 35D(1)(c) to remove the word 'general' so that an SIO authority is required to state a description of the nature of the authorised conduct (rather than just a 'general description' of the nature of that conduct). The committee considers that these proposed amendments will reduce, though not eliminate, the potential for this provision to constitute an undue trespass on personal rights and liberties.**

The committee draws these provisions to the attention of Senators and leaves the question of whether the proposed approach is appropriate to the Senate as a whole.

Alert Digest No. 11 of 2014 - extract

Undue trespass on personal rights and liberties—immunity from civil and criminal liability
Schedule 3, item 3, proposed section 35J

Proposed section 35J provides that special intelligence operation (SIO) applications and authorities are not invalidated by defects unless the defect affects the application, authority or variation in a ‘material particular’. The explanatory memorandum states that this ‘provision is designed to ensure that minor matters relating to form or process do not invalidate an application, authority or variation’ (p. 107). However, there is little guidance in the provision as to how to distinguish between minor and material matters. Given that the authorised conduct is apt to trespass on the rights of persons affected in significant ways, the committee’s general expectation is that legality of the authorisation or

application should be clearly established and that it is incumbent on the ASIO to implement appropriate procedures to obviate the risk of defects.

The committee therefore seeks the Attorney-General's further advice as to the justification for the necessity of this provision. Further, if the provision is considered necessary, the committee seeks advice as to the sort of defects that would not invalidate applications and authorisations (and whether more detailed guidance on this may be included in the provision).

> *Pending the Attorney-General's reply, the committee draws Senators' attention to the provision as it may be considered to trespass unduly on personal rights and liberties in breach of principle 1(a)(i) of the committee's terms of reference.*

Attorney-General's response - extract

I acknowledge and support the Committee's concern to ensure that ASIO implements appropriate procedures to obviate the risk of defects in SIO authorities. I consider that appropriate provision is made for this important matter in the thresholds required by the authorisation criteria in proposed s 35C, the requirements for the making of applications in proposed s 35B and for the issuing of authorisations in proposed s 35C, all of which are subject to the general oversight of the IGIS. I note that successive Governments and Parliaments have, justifiably, placed significant trust and confidence in the professional judgment and performance of ASIO. The high quality of its documentation in relation to warrants issued under Division 2 of Part 3 of the ASIO Act was also recently observed by the IGIS in her submission to the PJCIS inquiry into this Bill.[13]

However, proposed s 35J is necessary because special intelligence operations are major undertakings which can involve a significant investment of ASIO's resources over a sustained period of time, and will yield a significant benefit in enabling the collection of intelligence presently unable to be collected. As such, it would be inefficient and unreasonable if authorities were invalidated - and any intelligence collected potentially unable to be used - as a result of minor matters that pertain to form or process. Proposed s 35J is directed to avoiding this outcome. Without a provision of this kind, significant and resource-intensive operations could be invalidated on the basis of minor defects that do not in any way affect the basis on which an authority was granted. This outcome would, in my view, be disproportionate to the minor nature of the defect in an authority.

As noted at page 107 of the Explanatory Memorandum, the materiality (or otherwise) of a defect in relation to a particular in an SIO authority is capable of determination in the circumstances of individual applications, in accordance with the ordinary meaning of the

[13] Inspector-General of Intelligence and Security, Submission No 4 to the PJCIS inquiry into the National Security Legislation Amendment Bill (No 1) 2014, 4 August 2014, p. 14.

term 'material'. The Explanatory Memorandum further includes a guiding principle, that a defect affecting a material particular is intended to include one that vitiates the basis on which an application was made, or an authority granted, or a variation requested or granted.

In other words, a defect will relate to a material particular if it pertains to a detail that affected the decision of a person that was made in reliance on that detail. This may include, for example, an inaccuracy in the factual details relevant to the granting of an authority, on which a decision to make an application or grant an authorisation was based. In contrast, a defect in relation to a non-material particular may include, for example, a typographical error in an application or an authority.

There is considerable precedent in relation to the judicial interpretation of the term 'material particular', particularly as an element of criminal offences concerning the making of false or misleading statements under oath.[14] The term is also used in a wide range of Commonwealth legislation, generally creating such offences. These matters, in my view, support a conclusion that the meaning of the term 'material particular' is sufficiently clear without a requirement for express statutory guidance in proposed s 35J.

I further note that an identical provision applies in relation to the controlled operations scheme in s 15H of the Crimes Act, as inserted by the Crimes *Legislation Amendment (Serious and Organised Crime) Act 2010* (Bill of 2009). This provision was accompanied by a similar explanation at page 73 of the Explanatory Memorandum to the 2009 Bill, which was not the subject of specific comment by this Committee as constituted in 2009.[15]

Committee Response

The committee thanks the Attorney-General for this response.

The committee notes that the Attorney-General considers that there is considerable precedent in relation to the judicial interpretation of the term 'material particular' and that therefore the meaning of the term 'material particular' is sufficiently clear without a requirement for express statutory guidance in proposed s 35J.

(continued)

[14] See, for example, R v Millward [1985] QB 519 at 525. (A statement was determined to be material to judicial proceedings if it influenced or may have influenced a judicial officer "in believing or disbelieving" a statement given in evidence, or "affected the determination of guilt or innocence" by a trier of fact.) See further, *R v Traino* (1987) 27 A Crim R 271. (A statement was determined to be material "if it is of such significance and importance, having regard to the whole of the evidence, that it is capable of affecting the decision of the appropriate tribunal of fact on the factual issue or issues" or "to a fact relevant to a fact in issue" or "to the credit of a witness".)

[15] Alert Digest No 9 of 2009 and Report No 10 of 2009.

The committee requests that the key information above be included in the explanatory memorandum and leaves the question of whether the proposed approach is appropriate to the Senate as a whole.

Alert Digest No. 11 of 2014 - extract

Undue trespass on personal rights and liberties—immunity from civil and criminal liability
Schedule 3, item 3, proposed section 35K

This provision protects a person from civil and criminal liability as a result of their 'participation' in a special intelligence operation if specified conditions are met. The explanatory memorandum (p. 108) explains that:

> The application of the immunity is subject to satisfaction of the conditions specified in subsections 35K(1) and (2), which ensure that it is limited strictly to authorised conduct under an SIO, and that the immunity is proportionate to the purpose of an SIO by excluding from its scope several serious offences including those in the nature of entrapment.

The explanatory memorandum includes a detailed outline of the scope of the provision and justification for it. In addition to detailing the specific requirements that will need to be met, the explanatory memorandum (pp 108–109) notes that:

> A number of safeguards apply to the immunity conferred by section 35K. These safeguards [described further in the EM], ensure that its application is duly limited and is subject to independent oversight, and that there remains scope for the payment of compensation to aggrieved individuals in appropriate cases.

The committee notes this justification, however the committee requests further advice from the Attorney-General as to whether this approach (including in relation to payment of compensation in respect of damage to property and personal injury and the status of civilian participants in operations) is consistent with that taken in relation to the controlled operations scheme in Part IAB of the *Crimes Act 1914* and, if it is not, a rationale as to why a different approach is required for special intelligence operations.

Pending the Attorney-General's reply, the committee draws Senators' attention to the provision, as it may be considered to trespass unduly on personal rights and liberties, in breach of principle 1(a)(i) of the committee's terms of reference.

Attorney-General's response - extract

As noted in my response to question 11 above, a detailed explanation is provided at pages 38-40 of the Department and ASIO's joint supplementary submission to the PJCIS of 29 August 2014, a copy of which is provided at **Enclosure 2** to this response.

Committee Response

The committee thanks the Attorney-General for this response.

The committee notes that the submission referred to by the Attorney-General indicates that both proposed section 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, the submission indicates that there are some differences in these protections (relating to civil liability, conditions of protection from liability for civilian participants, and compensation and notification requirements. **The committee draws Senators attention to these differences as outlined at pages 38–40 of the Attorney-General's Department/ASIO joint supplementary submission to the PJCIS.**

In relation to proposed section 35K, the committee also takes this opportunity to **request further advice from the Attorney-General as to the definitions of 'serious injury', 'serious loss of, or damage to, property' and 'conduct in the nature of 'entrapment'' for the purposes of the limited protection from legal liability proposed in section 35K. The committee is interested in examples of conduct that would not be necessary or proportionate to the effective performance by ASIO of its special intelligence functions, or the effective operation of the SIO scheme (explanatory memorandum, pp 108–109).**

(continued)

The committee also notes that paragraphs 15HA(2)(d) and 15HB(d) of the Crimes Act provide protection from criminal responsibility and indemnification against civil liability if the relevant conduct 'does not involve the participant engaging in any conduct that is likely to (i) cause the death of, or serious injury to, any person; or (ii) involve the commission of a sexual offence against any person. **The committee notes that equivalent paragraph in this bill (proposed paragraph 35K(1)(e)) does not include the words 'is likely to' and seeks the Attorney-General's advice as to the impact of, and rationale for, this difference between the two schemes.**

Alert Digest No. 11 of 2014 - extract

Undue trespass on personal rights and liberties—offences
Schedule 3, item 3, proposed section 35P

Proposed section 35P creates two new offences in relation to the unauthorised disclosure of information relating to an SIO.

Subsection 35P(1) creates an offence if 'a person' discloses information and the information relates to a special intelligence operation. The penalty is imprisonment for 5 years. Subsection 35P(2) creates an aggravated version of this offence. It applies where the disclosure is (i) intended to endanger the health or safety of any person or prejudice the effective conduct of an SIO, or (ii) will endanger the health or safety of any person or prejudice the effective conduct of an SIO. The penalty is imprisonment for 10 years. The offences may be committed by any person, including participants in an SIO.

The explanatory memorandum suggests these 'offences are necessary to protect persons participating in an SIO and to ensure the integrity of operations, by creating a deterrent to unauthorised disclosures, which may place at risk the safety of participants or the effective conduct of the operation' (at p. 111). The explanatory memorandum also explains that the offences may be committed by any 'persons to whom information has been about an SIO has been communicated in an official capacity, and persons who are the recipients of an unauthorised disclosure on information, should they engage in subsequent disclosure'.

Although the purposes of protecting the integrity of operations and the safety of participants in operations can be readily understood, it must also be noted that these offences are drafted so as to have broad application. First, they are not limited to initial disclosures of information relating to an SIO but cover all subsequent disclosures (even, it would seem, if the information is in the public domain). In addition, these new offences as

currently drafted may apply to a wide range of people including whistleblowers and journalists.

Second, the primary offence (unlike the aggravated version) is not tied to the underlying purposes of the criminalisation of disclosure. This means that the offence (under subsection 35P(1)) could be committed even if unlawful conduct in no way jeopardises the integrity of operations or operatives. The concern about the breadth of application of these offences, in light of their purposes, is arguably heightened given that whether or not the disclosure of information will be caught by the provisions depends on whether or not the information relates to an SIO, a question which depends on an authorisation process which is internal to the Organisation.

As the justification for the breadth of application of these provisions is not directly addressed in the explanatory memorandum the committee seeks a more detailed justification from the Attorney-General in this regard. The committee emphasises that its interest is not only in the underlying purposes served by the provisions, but whether these purposes could be achieved by offences that are more directly connected and proportionate to the achievement of those purposes.

A further reason why these offences may be considered to be too broad in their application is that it is possible they may apply to the disclosure of information even if the person who discloses the information is not aware that it relates to an SIO. Given the nature of an SIO it is likely that only persons within the Organisation will know whether information relates to an SIO. It is also relevant to note that the boundaries of an SIO, and therefore what information 'relates' to such an operation, may be unclear to the extent that an SIO authority need only state 'a general description of the nature of the special intelligence conduct that the persons' authorised to engage in conduct for the purposes of the SIO 'may engage in' (paragraph 35D(1)(c)). **The committee therefore also seeks clarification about (and a justification for) the applicable fault requirement in relation to the element that 'the information relates to a special intelligence operation' (paragraph 35P(1)(b) and paragraph 35P(2)(b)).**

> *Pending the Attorney-General's reply the committee draws Senators' attention to the provision, as it may be considered to trespass unduly on personal rights and liberties, in breach of principle 1(a)(i) of the committee's terms of reference.*

Attorney-General's response - extract

The Government has, in developing the disclosure offences in proposed s 35P, given careful consideration to their scope of application, including whether more limited formulations could adequately achieve the legitimate objective of protecting sensitive operational information in relation to SIOs. The Government is of the view that proposed

ss 35P(l) and (2) are necessary and proportionate to the legitimate objective to which they are directed, and that the alternatives considered would not provide adequate protection for the relevant information. These matters have also been addressed in considerable detail in the evidence of my Department and ASIO to the PJCIS.[16] I address each of the Committee's main areas of interest below, with a focus on the basic offence in s 35P(1) given that its application is broader than the aggravated offence in proposed s 35P(2), which requires proof of a person's intention to cause certain harm in communicating the information, or that the communication of the information will cause harm.

Purpose served by proposed s 35P

The wrongdoing to which the offences are directed is the harm inherent in the disclosure of highly sensitive intelligence-related information. The disclosure of the very existence of an SIO - which is intended to remain covert - is, by its very nature, likely to cause harm to security interests. Given the necessarily covert nature of an SIO, disclosure of the existence of such an operation automatically creates a significant risk that the operation may be frustrated or compromised and that the safety of its participants, or persons associated with them such as family members, may be jeopardised. It may also jeopardise other investigations where there is some connection between the two - for example, if there is some relationship between the persons being investigated or an authorised participant, whose identity is disclosed, is known to associate with other persons who are also performing investigative roles. Once such information is disclosed, there is limited recourse available to address these significant risks. This harm is not contingent on a person's malicious intention in making a disclosure, except that it may be aggravated by persons who act with a malicious intention since this may further increase the prospects that these risks may eventuate. As such, there is a need for a strong deterrent to such behaviour.

A number of independent reviews of intelligence and secrecy legislation have found that it is appropriate to criminalise the disclosure of intelligence-related information on the basis that harm is inherent or implicit in the very act of disclosure, thereby obviating a need to prove any specific malicious intention on the part of the disclosure, or an adverse outcome of the disclosure. These have included the Hope Royal Commission on Intelligence and Security in its 1976 report on ASIO, and the Australian Law Reform Commission's 2009 Report on Secrecy Laws and Open Government in Australia, which specifically examined secrecy offences in respect of the Australian Intelligence Community.

Offences with largely identical elements have been enacted in relation to the controlled operations scheme in ss 15HK and 15HL of the Crimes Act. I am advised that no matters have been investigated, referred for prosecution, or prosecuted in relation to ss 15HK and 15HL of the Crimes Act, which have been in force since 2010. This, in my view, supports a conclusion that these offences have not operated to unduly infringe individual rights and

[16] See especially: AGD, responses to matters taken on notice on 15 August (18 August 2014), pp. 17-22; AGD and ASIO, joint supplementary submission (29 August 2014), pp. 41-42, 47-48 (see also pp. 77-79 in relation to the proposed secrecy offences in Schedule 6 to the Bill); AGD and ASIO, second joint supplementary submission (9 September 2014), pp. 6-7.

libe1ties, particularly in respect of freedom of expression. I am further aware that the scope of the offences in ss 15HK and 15HL of the Crimes Act was not identified as a source of concern by this Committee, as constituted in 2009, in its examination of the Crimes Amendment (Serious and Organised Crime) Bill 2009 (Act of 2010).[17]

I acknowledge that the Committee has raised a number of specific concerns about the following matters, which are addressed in the subheading below:

- coverage of subsequent disclosures, including of information in the public domain;
- coverage of persons including journalists and whistleblowers;
- absence of a requirement to prove harm or damage as a result of disclosures; and
- application of the offences on the basis of an internal authorisation process.

Consideration of alternatives

Coverage of information in the public domain

The offences are intentionally capable of covering information already in the public domain. This reflects the fact that the significant risks associated with the disclosure of information about an SIO (including its existence, methodology or participants) arc just as significant in relation to a subsequent disclosure as they arc in relation to an initial disclosure. Limiting the offences to initial disclosures would create an arbitrary distinction between culpable and non-culpable conduct, on the basis of a technical question of the order in which multiple disclosures were made.

Consideration was given to the inclusion of a specific defence for the communication of information in the public domain by reason of the authority of the Commonwealth. However, given that it is highly unlikely information about an SIO would ever be authorised, or capable of authorisation, for public release, it was considered that appropriate provision for such circumstances was made via the general defence of lawful authority under s 10.5 of the Criminal Code, together with general prosecutorial and investigative discretion. Further, I note that there is no equivalent exception in the offences in ss 15HK and 15HL of the Crimes Act for information already in the public domain.

Proposed s 35P(3) does, however, contain a number of exceptions for permitted disclosures. These include, in paragraph (b), disclosures for the purposes of legal proceedings arising out of, or otherwise related to the SIO scheme, or any report of such proceedings. This exception could therefore apply to a journalist who reported on legal proceedings in which the existence of an SIO was disclosed (however, disclosure may further be subject to any protective orders the Court may make in relation to such evidence).

[17] Alert Digests No 9 and No 15 of 2009, and Report No 10 of 2009.

Application to journalists and whistleblowers

The offences intentionally apply to all persons, consistent with the intention to avoid the significant risks arising from the very fact of disclosure of information about an SIO. I am aware that some stakeholders, including participants in the PJCIS inquiry into the Bill, have advocated for either a specific exception to the offences in favour of journalists, or a general public interest exception, where the trier of fact is of the view that the public interest in making a disclosure outweighed the detriment to security. I have strong reservations about either of these options, for the reasons outlined in the submissions of my Department and ASIO to the PJCIS inquiry into the Bill.[18]

In short, these reasons are, first, that it is contrary to the criminal law policy of the Commonwealth to create specific exceptions of this kind from the legal obligations of non-disclosure to which all other Australian persons and bodies are subject. It is appropriate that all members of the community are expected to adhere to non-disclosure obligations, which should apply equally to all persons - whether they are intelligence or law enforcement professionals or journalists reporting on national security matters. The absence of exceptions in favour of specific classes of persons is also consistent with the policy intention that the offences are directed to the risks posed to security as a result of the disclosure of sensitive information, which arise irrespective of the motives of the discloser.

Secondly, a general public interest defence is not considered necessary or appropriate for two reasons. Provision is already made for the disclosure of suspected wrongdoing to the Director-General of Security or the Inspector-General of Intelligence and Security under the *Public Interest Disclosure Act 2013*, which overrides secrecy laws of general application. The *Inspector-General of Intelligence and Security Act 1986* further overrides secrecy laws of general application in relation to persons who comply with notices for the production of documents or the provision of information issued under that Act.

In addition, a dedicated public interest defence is not, in my view, appropriate in relation to the offences in proposed ss 35P(l) or (2). This is because, even if a jury or a trial judge as the final arbiter of fact held that a disclosure was not in the public interest, the disclosure would have already occurred and the potential for harm actualised. Prejudice to security, and consequently harm to the public interest from a disclosure relating to an SIO can evolve quickly, such as in reprisals from persons being investigated. Harm could also evolve so slowly as to be difficult to detect - for example, the disclosure of a person's identity as an ASIO employee or an ASIO affiliate could be used by foreign intelligence services to target and infiltrate ASIO and its operations, or compromise its staff, over a significant period of time.

---

[18] See especially: AGD, responses to questions on notice 15 August 2014 (18 August 20 I 4), p. 23; and AGD and ASIO, joint supplementary submission (29 August 2014), pp.82-83. See further AGD and ASIO, second joint supplementary submission (9 September 2014), pp. 12-13. (The comments in the latter submission were made specifically in relation to the proposed offences in Schedule 6 to the Bill, but apply equally to proposed s 35P.)

Further, a public interest defence would inappropriately designate a jury or a trial judge as the final arbiter of whether a particular disclosure caused harm to the public interest in the context of adjudicating criminal guilt. There is a risk that such individuals may not have an appropriate understanding or an appreciation of the possible impact of releasing that information, and will necessarily not be in a position to adequately asses how the disclosure of a particular piece of information may, when taken together with other information, cause prejudice or risk causing prejudice to security interests. Such a defence would further be inconsistent with the general policy intention I have outlined above.

I have, however, asked my Department to consider whether some additional exceptions to proposed ss 35P(l) and (2) could feasibly be included in proposed s 35P(3), in respect of legal advice, and pro-active disclosures to the IGIS by persons to whom the *Public Interest Disclosure Act 2013* does not apply. (That is, complaints to the IGIS by persons other than 'public officials' as defined under that Act, and disclosures to the IGIS in response to requests or as part of inspections rather than pursuant to the Public Interest Disclosure Act or statutory notices to produce issued under the IGIS Act.)

Resultant harm

I consider it appropriate that an intention to cause harm is limited to an element of the aggravated offence in proposed s 35P(2), and that the basic offence in proposed s 35P(l) does not include such an element. This is consistent with the policy intention outlined above. I note that the ALRC, in its 2009 report on secrecy laws and open government in Australia, considered that secrecy offences in respect of intelligence-related information did not need to include an element requiring proof of harm or intent to cause harm in making a disclosure, on the basis that the harm is implicit.[19]

Internal authorisation process

I acknowledge that the Committee is concerned that proposed s 35P may result in the exposure of persons to criminal liability who may not know that the information related to an SIO, recognising that the authorisation process is internal to ASIO. This matter is addressed in my response to question 17 below, in relation to the applicable fault element applying to this physical element of the offence. In short, the offences apply to persons who disclose information, and are reckless as to the circumstances that it relates to an SIO. This means that they must be aware of a substantial risk that the information related to an SIO, and acted unjustifiably in the circumstances by taking the risk of making the disclosure. As discussed further below, this is a high threshold for the prosecution to prove to the criminal standard.

In summary, for the reasons set out above, the Government's view that the offences in proposed s 35P represent a proportionate means of achieving the legitimate objective to which they are directed, being the protection of sensitive operational information

[19] Australian Law Reform Commission, Report 112, p. 289 at [8.65] and recommendation 8-2 at p. 307.

(including information concerning the existence of an operation together with details of its methodology and participants).

The physical element in (b) of each of ss 35P(l) and (2) is a circumstance in which conduct occurs, within the meaning of s 4.1.(l)(c) of the *Criminal Code 1995*. As the provision does not specify a fault element, s 5.6(2) of the Criminal Code operates to provide that the fault element of recklessness applies. Recklessness is defined in s 5.4(1) of the Criminal Code to mean that the person was aware of a substantial risk that the information disclosed related to a special intelligence operation, and unjustifiably, in the circumstances known to him or her at the time, took the risk of making the disclosure.[20]

Accordingly, it is not necessary for the prosecution to establish that a person had knowledge that the information related to an SIO, in the sense of a conscious awareness of the existence of an SIO and that the relevant information related to that operation. However, the prosecution must establish, beyond reasonable doubt, that a person was aware of a real and not remote possibility that the information was so related. As such, the offences will not apply to a person who disclosed information entirely unaware that it could relate to an SIO, since there would be no evidence of an advertence to a risk of any kind.

In addition, proof of a person's awareness of a substantial risk will depend on the availability of evidence of a person's awareness of relevant information about an operation or a suspected operation, which must suggest more than mere advertence to a nominal or speculative possibility that an SIO might have been declared, and that the information proposed to be communicated related to that operation. Rather, the prosecution would need to prove, beyond reasonable doubt, that the person was aware of a real and not remote possibility that the information related not just to an intelligence or national security related operation of some general description, but specifically to an SIO.

As the Committee has observed, SIO authorisations are an entirely internal matter. This means that the burden on the prosecution to prove, to the criminal standard, that a person was advertent to a risk that a specific circumstance existed, and that that risk was significant, is an onerous one.

In addition to providing a person was aware of a substantial risk that the relevant circumstance existed, the prosecution must further prove that, having regard to the circumstances known to the person at the time of making the disclosure, it was unjustifiable to have taken that risk. The actions of a person in attempting to manage risk are directly relevant to an assessment of whether a person's actions were justifiable. For example, the actions of a journalist in attempting to check facts and consult with ASIO about any possible concerns in reporting on a matter would tend very strongly against a finding that such a person had acted unjustifiably in the circumstances. As such, adherence to the usual practices of responsible journalism in the reporting of operational matters

[20] See further, AGD response to questions on notice at a public hearing of the PJClS, 15 August 2014 (18 August 2014), pp. 17-22.

relating to national security is directly relevant to the question of whether a communication was justified in the circumstances.

The policy justification for adopting recklessness, rather than knowledge, as the applicable fault element is - as noted above - that the wrongdoing targeted by proposed s 35P is that the disclosure of information about an SIO will, by its very nature, create a significant risk to the integrity of that operation and the safety of its participants. The fault element of recklessness gives expression to the policy imperative to deter such conduct by clearly placing an onus on persons contemplating making a public disclosure of such information to consider whether or not their actions would be capable of justification to the criminal standard. In the event that there is doubt, and the proposed disclosure relates to suspected wrongdoing by ASIO, consideration should be given to making an appropriate internal disclosure, such as to the Inspector-General of Intelligence and Security, or to the Australian Federal Police if the commission of a criminal offence is suspected.

Committee Response

The committee thanks the Attorney-General for this detailed response and **requests that the key information above be included in the explanatory memorandum**.

The committee notes the detailed rationale for the provision provided by the Attorney-General and that the government considers that the offences in proposed s 35P represent a proportionate means of protecting sensitive operational information. The committee further notes that it will not be necessary for the prosecution to establish that a person had knowledge that the information disclosed related to an SIO, however, the prosecution will be required to establish, beyond reasonable doubt, that a person was aware of a real and not remote possibility that the information was so related. As such, the Attorney-General suggests that the offences would not apply to a person who disclosed information entirely unaware that it could relate to an SIO, since there would be no evidence of an advertence to a risk of any kind.

The committee also takes this opportunity to note recommendation 11 of the Parliamentary Joint Committee on Intelligence and Security's report into the bill. In particular, the committee considers that it would be appropriate to provide for additional exemptions relating to the disclosure of information to the IGIS and for the purposes of obtaining legal advice.

The committee draws this provision to the attention of Senators and leaves the question of whether the proposed approach is appropriate to the Senate as a whole.

Alert Digest No. 11 of 2014 - extract

Undue trespass on personal rights and liberties—penalties
Schedule 3, item 3, proposed subsection 35P(1)

The explanatory memorandum (at p. 113) and statement of compatibility (at p. 19) explicitly deal with the appropriateness of the penalties imposed for the offences detailed above. It is suggested that the penalties are consistent with the principles set out in the *Guide to Framing Commonwealth Offences, Infringement Notices and Enforcement Powers*. The consequences of the prohibited conduct is said to be 'particularly dangerous or damaging'.

The committee notes that the breadth of application of the offence in subsection 35P(1), which applies to any person and is not limited to intended or actual consequences of the offence, means that the offence may be proved even though the conduct did not in fact compromise the integrity of operations or place at risk the safety of any participants in an SIO. **In light of this, the committee seeks a fuller justification from the Attorney-General as to why the penalty of imprisonment for 5 years is considered appropriate given that the breadth of application of the offence provision.**

> *Pending the Attorney-General's reply the committee draws Senators' attention to the provision, as it may be considered to trespass unduly on personal rights and liberties, in breach of principle 1(a)(i) of the committee's terms of reference.*

Attorney-General's response - extract

A maximum penalty of five years' imprisonment is considered appropriate to reflect the wrongdoing inherent in the reckless disclosure of information relating to a special intelligence operation. As mentioned above, information about the existence and conduct of a special intelligence operation is inherently sensitive due to the necessarily covert nature of these operations. The disclosure of such information, by its very nature, places at risk the conduct of the operation to which it relates. This risk arises in respect of both the potential frustration of the effective conduct of an operation (and therefore the ability of ASIO to collect vital intelligence) and in potentially jeopardising the lives and safety of participants.

The proposed maximum penalty further reflects that the person disclosing the information was reckless as to the circumstance of its relationship with a special intelligence operation. That is to say, the person was aware of a substantial risk that the information was so

related, but nonetheless, and unjustifiably in the circumstances, took the risk of making the disclosure. A person who was unaware of a substantial risk, or whose conduct is considered by a trier of fact to be justifiable would not be criminally responsible. It is a matter for a sentencing court to determine an appropriate penalty within the maximum, in accordance with general sentencing rules and having regard to the circumstances of individual cases. A person who, for example, disclosed information knowing that it related to a special intelligence operation would reasonably be expected to be subject to a higher penalty than a person who was aware of a substantial risk of this connection.

I further note that the proposed maximum penalty would maintain parity with the penalties applying to the secrecy offences in s 34ZS of the ASIO Act, concerning the unauthorised disclosure of information relating to ASIO's questioning and questioning and detention warrants. These offences, which were enacted in the *ASIO Legislation Amendment Act 2006* (Bill of 2006), similarly do not require proof of harm or intention to cause harm in the making of a disclosure, in recognition that such harm is implicit. This approach was found acceptable to the Parliament in 2006 and was not the subject of comment by this Committee as constituted at that time.[21]

I consider that an internally consistent penalty structure within the ASIO Act is necessary to adequately reflect the harm implicit in the disclosure of information about a covert intelligence activity, namely the creation of, at least, a risk that a sensitive operation may be compromised.

Committee Response

The committee thanks the Attorney-General for this response and **requests that the key information above be included in the explanatory memorandum**.

The committee draws this provision to the attention of Senators and leaves the question of whether the proposed maximum penalty of 5 years imprisonment is appropriate to the Senate as a whole.

Alert Digest No. 11 of 2014 - extract

Undue trespass on personal rights and liberties—evidentiary certificates

[21] See Alert Digest No 4 of 2006 and Report No 3 of 2006. See also Alert Digest No 4 of 2003 and Report 12 of 2002, in which the Committee similarly did not comment on disclosure offences in s 34VA concerning the unauthorised communication of information by a subject's lawyer, which also carry a maximum penalty of five years' imprisonment.

Schedule 3, item 3, proposed section 35R

This provision seeks to permit an authorising officer to issue a written certificate setting out facts relevant to the granting of a special intelligence operation authority and the certificate will constitute prima facie evidence of these facts. The explanatory memorandum notes that this 'creates a rebuttable presumption as to the existence of the factual basis on which the authorising officer was satisfied the relevant issuing criteria for an SIO authority were met.' (p. 114)

The explanatory memorandum argues (p. 114) that this is appropriate:

> …to minimise the time that authorising officers (who are senior position-holders within the Organisation, being the Director-General and Deputy Directors-General) must spend away from their duties providing evidence in proceedings as to the factual basis for the granting of an authority. The prima facie nature of evidentiary certificates issued under section 35R is consistent with Commonwealth policy that a party to proceedings should generally be accorded an opportunity to adduce evidence to the contrary, and that a court should adjudicate on the respective weight to be placed on the evidence before it in proceedings.

While the committee appreciates the importance of ensuring that senior officers are able to spend their time efficiently, whether or not the proposed reversal of onus is appropriate depends significantly on the types of facts likely to be included in an evidentiary certificate. **The committee therefore seeks the Attorney-General's further advice as to the justification for this provision, including possible general examples of the content of these evidentiary certificates.**

> *The committee draws Senators' attention to the provision as it may be considered to trespass unduly on personal rights and liberties, in breach of principle 1(a)(i) of the committee's terms of reference.*

Attorney-General's response - extract

The scheme of evidentiary certificates in proposed s 35R is necessary to ensure that sensitive operational details of decision-making in relation to SIOs are adequately protected in legal proceedings, and that such protection is applied in a way that is both procedurally fair and operationally efficient.

Proposed s 35R(l) is expressly limited to matters with respect to the granting of an SIO authority - namely, the authorising criteria in proposed s 35C. As such, certificates apply to the factual basis on which SIO authorisations are made. They could include such matters as:

- the particular special intelligence functions in respect of which the SIO will assist the Organisation, including details of how the SIO will do so;

- why the circumstances in a particular case are such as to justify the conduct of an SIO;

- what conduct is authorised or was sought to be authorised, including details of any otherwise unlawful conduct and how it is to be limited to the maximum extent consistent with an effective operation; and

- why any additional conditions or limitations are imposed.

Accordingly, a certificate issued under proposed s 35R could, in general terms, include details about a particular entity or activity of security concern, including why it is of security concern and why it is necessary to collect intelligence in relation to it, and why a special intelligence operation is needed, and details of the methodology of and participants in an SIO.

Importantly, proposed s 35R is limited to matters in respect of the authorisation of an SIO and not the intelligence collected in an SIO. As such these certificates would not include matters that could be used as prima facie evidence of the elements of an offence. 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 a respondent nonetheless had concern as to the breadth or scope of the facts covered by a certificate, because it appeared to include material facts that could address or prove the ultimate facts in the case, the prima facie nature of a certificate means it could be challenged in court and both parties given an opportunity to test its limits. If a certificate purported to cover such facts, it would be struck out to the extent it exceeded the permissible matters in proposed s 35R.

Committee Response

The committee thanks the Attorney-General for this detailed response.

The committee requests that the key information above be included in the explanatory memorandum and leaves the question of whether the proposed scheme of evidentiary certificates to be created by this provision is appropriate to the Senate as a whole.

Tax and Superannuation Laws Amendment (2014 Measures No. 4) Bill 2014

Introduced into the House of Representatives on 17 July 2014
Portfolio: Treasury

Introduction

The committee dealt with this bill in *Alert Digest No. 10 of 2014*. The Acting Assistant Treasurer responded to the committee's comments in a letter dated 4 September 2014. A copy of the letter is attached to this report.

Alert Digest No. 10 of 2014 - extract

Background

This bill amends various laws relating to taxation, superannuation and excise.

Schedule 1 in the bill:

- amends the debt limit settings in the thin capitalisation rules to ensure that multinationals do not allocate a disproportionate amount of debt to their Australian operations;
- increases the *de minimis* threshold to minimise compliance costs for small businesses; and
- introduces a new worldwide gearing debt test for inbound investors.

Schedule 2 amends the exemption for foreign non-portfolio dividends.

Schedule 3 amends the *Income Tax Assessment Act 1997* (ITAA 1997) to ensure that the foreign residents capital gains tax (CGT) regime operates as intended by preventing the double counting of certain assets under the Principal Asset Test. A technical correction is also made to the meaning of 'permanent establishment' in section 855-15 of the ITAA 1997.

Schedule 4 requires the Commissioner of Taxation to issue a tax receipt to individuals for the income tax assessed to them.

Schedule 5 makes a number of miscellaneous amendments to the taxation and superannuation laws.

Retrospective commencement
Schedule 3, item 10

Part 2 of schedule 3 seeks to make a 'technical correction' to the meaning of 'permanent establishment' in section 855-15 of the *Income Tax Assessment Act 1997*. The correction is to ensure that foreign residents are subject to capital gains tax (CGT) in relation to CGT assets that they have used in carrying on a business through a permanent establishment located in Australia.

Item 10 is an application provision which provides that the amendments made in Part 2 of schedule 3 apply from the commencement of Division 855 (i.e. the amendments will apply to CGT events that happen on or after 12 December 2006). The explanatory memorandum (p. 57) states that:

> These changes are of a technical nature and do not affect any other aspect of the definition of taxable Australian property. They do not negatively affect any taxpayer because the scope of the definition of taxable Australian property aligns with the intention of the original provisions.

While the committee notes this explanation, it is unclear whether the proposed amendment will in fact give rise to detriment to any person who has relied on the definition in its current form. **The committee therefore seeks the Minister's advice about this matter.**

> *Pending the Minister's reply, the committee draws Senators' attention to the provision as it may be considered to trespass unduly on personal rights and liberties in breach of principle 1(a)(i) of the committee's terms of reference.*

Assistant Treasurer's response - extract

The amendment made by Schedule 3 is purely of a technical nature as the clear intention of Division 855 is to tax foreign residents on their Australian taxable property assets (either Australian real property assets or assets that are used in their Australian permanent establishment (branches)).

> The explanatory material that accompanied the introduction of Division 855 into the Parliament in 2006 makes this point clear by stating that *"the changes narrow the range of assets on which a foreign resident will be liable to Australian capital gains tax (CGT) to Australian real property and the business assets (other than Australian real property) of a* ***foreign resident's Australian permanent establishment'*** [emphasis added].

In determining the assets **of permanent establishments located in Australia,** the table in section 855-15 of the *Income Tax Assessment Act 1997* includes as 'taxable Australian property':

> A CGT asset that you have used in carrying on a business through a **permanent establishment** (within the meaning of s23AH of the ITAA 1936) **in Australia.**

In relation to the technical amendment made by Schedule 3, the reference to the section 23 definition of permanent establishment in Division 855 (the foreign resident CGT regime) is a reference to a definition that only applies to outbound investments: that is, the permanent establishments of Australian residents operating overseas. A technical amendment is therefore required to Division 855 to ensure that it can correctly apply where assets are used in carrying on a business through a permanent establishment in Australia.

> The change replaces the reference to a permanent establishment within the meaning of section 23AH of the ITAA 1936 with specific tests. Consistent with section 23AH, these tests take into account an entity's status as a resident of a country with which Australia has an international tax agreement in determining whether it has a permanent establishment in Australia. Where there is no international agreement the general definition defined in subsection 6(1) of the ITAA 1936 is used.

The proposed amendment does not negatively affect any taxpayer because the scope of the definition of taxable Australian property will now align with the intention of the original provisions to only tax the Australian assets of foreign residents.

My Department undertook targeted consultation with several tax practitioners on this issue prior to its introduction into Parliament. Those contacted were supportive of the change applying retrospectively. Further, they advised Treasury that they were unaware that this technical issue existed as the measure was clearly intended to cover Australian assets only.

Committee Response

The committee thanks the Assistant Treasurer for this detailed response and **requests that the key information above be included in the explanatory memorandum to the bill**. The committee notes that generally it will have concerns where a bill seeks to apply a legislative change retrospectively where that change may give rise to a detriment to any person who had relied on the legislative provision as originally enacted. The fact that a retrospective change may ensure that the provisions aligns with the original intention of the provision would generally not, in itself, alleviate the committee's concerns.

(continued)

The committee therefore draws this provision to the attention of Senators and leaves the question of whether the proposed approach is appropriate to the Senate as a whole.

Senator Helen Polley
Chair

Minister for Small Business

Senator Helen Polley
Chair
Senate Scrutiny of Bills Committee
Suite 1.111
Parliament House
CANBERRA ACT 2600

1 SEP 2014

Dear Senator Polley

I refer to the letter of 28 August 2014, from Ms Toni Dawes, Secretary of the Standing Committee for the Scrutiny of Bills, in relation to the Competition and Consumer (Industry Code Penalties) Bill 2014.

As noted by Ms Dawes, the Bill will amend the *Competition and Consumer Act 2010* (the Act) to make pecuniary penalties issued by a Court and infringement notices issued by the Australian Competition and Consumer Commission (ACCC) available as remedies for breaches of a civil penalty provision of a prescribed industry code.

The reasons for the Government's decision to introduce the Bill are set out in its policy statement, *The Future of Franchising*, which addresses the implementation of recommendations of the 2013 review of the Franchising Code by Mr Alan Wein. The policy statement identifies that:

> Consultation during the review presented consistent anecdotal evidence of questionable behaviours in franchising. As franchisors are usually in a more powerful economic and contractual position than the franchisee, poor conduct by franchisors can have a disproportionate effect on franchisees. On the other hand, due to the network nature of franchising, poor conduct by isolated franchisees can affect the reputation of the system as a whole. To address this, the Government proposes to:
>
> – Improve compliance and enforcement outcomes through a range of flexible tools for use by the regulator, the Australian Competition and Consumer Commission ('ACCC'). The Government will introduce penalties of up to $51,000 for serious breaches of the Code. This will mean stronger consequences for breaching the Code and will further deter parties from breaching the Code. The ACCC will also be given powers to issue infringement notices.

Parliament House CANBERRA ACT 2600
Telephone: 02 6277 7930 Facsimile: 02 6273 0434
Email: sbminister@treasury.gov.au

In response to the specific issues raised in Ms Dawes letter:

The rationale why the content of a civil penalty offence is not provided for in primary legislation:
Introducing a general power to allow penalties to be applied for a breach of an industry code made under the Act was considered the simplest and most efficient means of providing a flexible tool that can be adopted, where required, in different industry codes.

Providing for pecuniary penalties and infringement notices in primary legislation would require the reproduction in the Act of the proposed pecuniary penalty provisions for each individual industry code. Further, there could be less flexibility and less clarity for industry participants around which specific clauses of each industry code would have an associated pecuniary penalty or an infringement notice. This option was considered unwieldy in practical terms.

The justification for the penalty of up to 300 penalty units being prescribed for the breach of a civil penalty provision in an industry code:
Mr Wein's recommendation, after considering all the evidence, was for a pecuniary penalty of $50,000 for a breach of the Franchising Code. The Government agreed with Mr Wein that this amount would act as a deterrent to a breach of the Franchising Code, without punishing the breaching party excessively. The court may order a lower penalty if it believes one is warranted and one of the factors a court may take into account is the financial capacity of the breaching company.

It was considered preferable to express the penalty in penalty units, as expressed in the *Crimes Act 1914*. At present, 300 penalty units is $51,000.

On 27 August 2014, the Shadow Minister Assisting the Leader for Small Business, the Hon Bernie Ripoll MP, spoke in relation to the Bill, stating:

> The Bill will allow for a pecuniary penalty of up to $51,000, which is equal to 300 penalty units. From what I can tell, it is very, very similar to the former Labor government supported changes to the code which would have allowed for pecuniary penalties of up to $50,000. So if that is the only change then, of course, I welcome the bill that we had introduced in those terms.

The type of industry codes that may be prescribed by regulations under this provision (including whether it is intended that this provision will only apply to the Franchising Code):
The provisions may be applied to any industry code prescribed under section 51AC of the Act.

A new Franchising Code is expected to be introduced later in 2014 and be in place by 1 January 2015. It is the only Code that has currently made the case for the introduction of pecuniary penalties, to date. The case for the introduction of penalties for breach of a civil penalty provision will have to be made for each code separately.

Whether industry codes, including but not limited to the Franchising Code of Conduct, will be available for scrutiny and disallowance by the Parliament:
Section 51ACA of the Act provides that an industry code prescribed under section 51AC must be declared by a regulation. Any new industry code or amendment to existing industry codes will be subject to scrutiny and disallowance by the Parliament.

Measures in place to ensure that industry civil code penalty provisions will be readily accessible to regulated persons:

The inclusion of penalty provisions in the industry code itself, and not the Act, makes them more readily accessible to participants in the industry. The Government has consulted widely and is working with the industry codes regulator, the ACCC, to ensure guidance material is made available to participants and potential participants in the sector.

I hope you find this information useful.

Yours sincerely

BRUCE BILLSON

Minister for Finance
Acting Assistant Treasurer

Senate Helen Polley
Chair
Senate Scrutiny of Bills Committee
Suite 1.111
Parliament House
CANBERRA ACT 2600

Dear Senator Polley

On 4 September 2014, Ms Toni Dawes, Committee Secretary, wrote on behalf of the Senate Scrutiny of Bills Committee in relation to the Corporations Amendment (Streamlining of Future of Financial Advice) Bill 2014 (the Bill). Your letter has been referred to me as I have portfolio responsibility for this matter in my capacity as Acting Assistant Treasurer.

In its Scrutiny of Bills Alert Digest *No. 11 of 2014*, the Committee sought advice in relation to amendments 4, 5 and 6 to the Bill: these amendments extend the regulation-making powers in the Bill to allow regulations to prescribe circumstances when a benefit is to be treated as conflicted remuneration (amendment 4 relates to section 963B, amendment 5 to subsection 963C(1) and amendment 6 to subsection 963C(1)).

In addition to the regulation-making powers, amendment 4 inserts a new targeted general advice provision that is comprised of five limbs: all five limbs must be satisfied for the benefit to not be considered conflicted remuneration. There is also a specific limb that clarifies — beyond doubt — that payments known as commissions cannot be paid.

Whilst I believe the Future of Financial Advice amendments have been well tested, there is always the possibility – given the complexity of arrangements in the financial services sector – that unintended consequences may arise. As such, the enhanced regulation-making powers would permit the Government to address any unintended consequences should they arise.

The Government has endeavoured to ensure that there is adequate flexibility in the new amendments to address the concerns of industry and consumers at a time of legislative change. I believe that the Bill achieves the appropriate regulatory balance. Any regulations would be subject to consultation with stakeholders, as well as subject to the disallowance procedure under the *Legislative Instruments Act 2003*, providing Parliament with the opportunity to scrutinise the application of new regulations.

Parliament House Canberra ACT 2600
Australia
Telephone: 02 6277 7360 Facsimile: 02 6273 4125

I also note that the Bill – including the amendments – is currently being reviewed by the Senate Economics Legislation Committee. The Committee is due to report later this month and the Government will carefully consider any amendments recommended by the Committee.

I hope this answers your inquiries.

Kind regards

MATHIAS CORMANN

13 September 2014

The Hon Scott Morrison MP
Minister for Immigration and Border Protection

Senator Helen Polley
Chair
Senate Scrutiny of Bills Committee
Suite 1.111
Parliament House
CANBERRA ACT 2600

Dear Senator Polley

Migration Amendment (Protection and Other Measures) Bill 2014

Thank you for the Committee Secretary's letter dated 28 August 2014 in relation to advice provided to the Senate Scrutiny of Bills Committee (the Committee) by the Assistant Minister for Immigration and Border Protection, Senator the Honourable Michaelia Cash, and about which the Committee is seeking further information.

I note that, while the Committee's views are outlined in full in its *Tenth Report of 2014* (27 August 2014), additionally the Committee is seeking to know why the general exemption from the *Legislative Instruments Act 2003* (LI Act) is appropriate to guidance decisions. Further information in response to this request is provided below.

Undefined scope of administrative power
Delegation of legislative power
Schedule 4, Part 1, item 7, proposed section 353B
Schedule 4, Part 1, item 22, proposed section 420B

The committee seeks further advice from the Minister as to why the general exemption from the LI Act for practice directions is appropriate in relation to 'guidance decisions'. The committee would also be interested to know whether there are other examples of practice directions, covered by the exemption form the LI Act, which relate to questions of substance falling for determination by a Court of Tribunal.

A practice direction is not just confined to matters of procedure, but encompasses matters of practice and procedure. The application of a guidance decision in a direction of the Principal Member of the Migration Review Tribunal or Refugee Review Tribunal depends on if the facts or circumstances in the guidance decision can be distinguished from the current matter before the relevant tribunal. Once those matters of substance are determined, it becomes clear whether or not the tribunal must follow the direction and apply a decision (the guidance decision) of the Tribunal as a matter of practice. That is, the question of whether a guidance decision must, as a matter of practice, be applied is resolved. The application of guidance decisions will align and reduce inconsistencies in decision-making and increase efficiency of the review process. However, there will be no derogation of the responsibility of the tribunal to investigate the individual circumstances of an applicant.

As noted in the response to the Committee dated 11 August 2014, the guidance decision is an exercise of legislative power, but is not subject to disallowance under the LI Act. Regulation 7 of the *Legislative Instruments Regulations 2004* (LIR) provides that for item 24 of the table in subsection 7(1) of the LI Act, and, subject to section 6 and 7 of the LI Act, instruments mentioned in Schedule 1 of the LIR are prescribed. Item 6 of Part 1 of Schedule 1 provides that practice directions made by a court or tribunal are not legislative instruments.

As the concept of a guidance decision is a specific concept in respect of a practice direction of a tribunal, I am unable to provide another similar example of a practice direction.

To make it clear that 'guidance decisions' are not subject to disallowance, it is my intention to provide an Addendum to the Explanatory Memorandum.

I note that the Committee has also recommended that a number of other amendments be made to the Explanatory Memorandum for this Bill. I will make such amendments by way of an addendum to the Explanatory Memorandum, based on the further information already provided to the Committee, at an appropriate time.

Thank you for considering this advice. The contact officer in my Department is Ms Karen Visser, Director, Protection and Humanitarian Policy Section, who can be contacted on (02) 6264 4124.

Yours sincerely

The Hon Scott Morrison MP
Minister for Immigration and Border Protection
19/9/2014

ATTORNEY-GENERAL

CANBERRA

Senator Helen Polley
Chair
Senate Standing Committee for the Scrutiny of Bills
PO Box 6100
Parliament House
CANBERRA ACT 2600

16 SEP 2014

scrutiny.sen@aph.gov.au

Dear Chair

National Security Legislation Amendment Bill (No. 1) 2014

Thank you for your letter of 4 September 2014 regarding your Committee's consideration of the above Bill in Alert Digest No. 11 of 2014, tabled in the Senate on 3 September.

I now provide responses to each of the 19 matters in respect of which your Committee has sought further information from me. (**Enclosure 1**.)

I have also taken the liberty of providing three additional documents at **Enclosure 2**, which may be of assistance to the Committee in completing its examination of the Bill. These are unclassified submissions from my Department (AGD) and the Australian Security Intelligence Organisation (ASIO) to the Parliamentary Joint Committee on Intelligence and Security (PJCIS) inquiry into the Bill, which is due to provide its report in the week commencing 22 September 2014. A number of issues raised in Alert Digest No. 11 were also the subject of evidence before the PJCIS. My responses to your Committee's questions refer to relevant passages in these additional materials.

I trust that this information is of assistance to your Committee. I would be pleased to provide any further assistance that may be required, and look forward to considering your Committee's report on the Bill in due course.

Thank you again for writing to me on this matter.

Yours faithfully

(George Brandis)

Encl:

(1) Responses to Alert Digest No. 11 of 2014.
(2) Copies of three AGD and ASIO submissions to the PJCIS, August-September 2014.

Enclosure 1

National Security Legislation Amendment Bill (No. 1) 2014
Responses to Senate Standing Committee for the Scrutiny of Bills: Alert Digest No. 11 of 2014

Outline

Schedule 1 – ASIO Employment (questions 1-4)

(1) Director-General's power of delegation, s 16 (item 5)

Committee question (p. 8)

The committee therefore seeks more detailed advice from the Attorney-General as to why departure from this well established principle as proposed in the bill is appropriate in the circumstances. In this respect it is noted that the existing provision already casts the power to delegate in very broad terms, that is, to 'an officer of the Organisation'. The committee's consideration of the new provision would likely be assisted by examples of the sorts of delegations that would be appropriately authorised by the proposed new power of delegation, but are not possible under the terms of the existing provision.

Attorney-General's response

Amending item 5 of Schedule 1 to the Bill replaces the phrase "officer of the Organisation" in s 16 with "a person". It is consequential to the updated terminology proposed to be included in s 4 of the ASIO Act of 'ASIO employee' and 'ASIO affiliate' (per amending item 1 of Schedule 1 to the Bill). The adoption of these terms will mean that the term 'an officer of the Organisation' (which is undefined) is no longer used in Part V of the ASIO Act. As such, another term is required in s 16(1) to describe those to whom the Director-General of Security may delegate powers, functions or duties under the ASIO Act in respect of the management of ASIO employees and ASIO affiliates, and the financial management of the Organisation.

The term 'a person' has been used in proposed new s 16(1) to ensure that the Director-General can exercise his or her power of delegation in favour of persons who, for a range of reasons, may not be within the definition of an 'ASIO employee' or an 'ASIO affiliate',[1] in addition to persons within the Organisation who may fall within the definition of those terms (for example, a Chief Financial Officer or a Deputy Director-General). I acknowledge the Committee's comments on the breadth of the existing delegation under s 16 and that proposed to be included by amending item 5. Consideration was given to limiting the provision to an identified class or classes of persons. However, it was determined that the balance of interests in ensuring necessary flexibility and placing appropriate limitations on the power of delegation is best achieved through the limited nature of the powers, functions and duties of the Director-General which are subject to delegation under proposed new s 16(1). Further safeguards are contained in new s 16(2) and the independent oversight of the Inspector-General of Intelligence and Security (IGIS) in relation to the activities of ASIO, which could include the activities of delegates under proposed s 16(1).

---

1 The contingency that certain persons may not be ASIO employees or ASIO affiliates (or within the meaning of the former term 'officers of the Organisation') is presently recognised in other provisions of the ASIO Act. For example, the Minister is empowered under s 14 to appoint 'a person' to act as Director-General of Security.

In particular, the functions and powers of the Director-General that may be the subject of a delegation under proposed new s 16(1) are very limited. The provision does not extend to any or all of the Director-General's functions and powers under the ASIO Act. It is only those powers relating to management of ASIO employees or ASIO affiliates, and the financial management powers provided for in the ASIO Act. Almost all financial management within ASIO is carried out under the *Public Governance Performance and Accountability Act 2013*, and delegations of those powers are made in accordance with that Act. The power of delegation in proposed new s 16(1) is consistent with the scope of other such powers of delegation invested in agency heads under Commonwealth legislation. For example, s 78(7) of the *Public Service Act 1999* allows an Agency Head to delegate to "another person any of the Agency Head's powers or functions under that Act", which includes various staff management powers.[2]

In addition, the delegation power in proposed new s 16(1) must be exercised subject to any written directions given by the Director-General under proposed new s 16(2). The exercise of the power of delegation under proposed s 16(1), the issuing of any directions under s 16(2), and the activities of a delegate would also be subject to the independent oversight of IGIS under the *Inspector-General of Intelligence and Security Act 1986* (IGIS Act). The IGIS is empowered under s 8 of the IGIS Act to examine both the legality and the propriety of the activities of ASIO. The IGIS also has power under s 8(1)(b) of the IGIS Act to examine, at the request of the Attorney-General, the procedures of ASIO relating to redress of grievances of employees of ASIO (which is proposed to be amended by item 43 of Schedule 1 to cover ASIO employees and ASIO affiliates). The IGIS further has power under s 8(6) to inquire into complaints made by ASIO employees about certain staff management issues. (A similar power is proposed to be inserted in relation to ASIO affiliates by amending item 45 in Schedule 1 to the Bill in proposed ss 8(8) and 8(8A).) These powers would be exercisable in relation to the activities of delegates under proposed s 16(1).

To take account of the Committee's comments on this proposed provision, I have asked my Department to revise the Explanatory Memorandum to the Bill to include an explanation of these matters.

---

2 It is acknowledged, however that an additional limitation is applied under s 78(8) of the *Public Service Act 1999*. An Agency Head cannot delegate powers or functions to a non-APS employee or a person who does not hold an executive or statutory office (referred to as an 'outsider') without the prior written consent of the Public Service Commissioner. An additional approval requirement was not considered necessary for inclusion in the ASIO Act, given the limited scope of delegation within s 16(1), and nor appropriate within the context of an intelligence agency where vulnerabilities may be created if the identities of those performing work for ASIO are revealed unnecessarily. Instead, adequate provision is made for oversight under proposed new s 16(2) (in which the delegate must comply with any written direction given by the Director-General) and the general oversight jurisdiction of the IGIS in respect of the activities of ASIO.

(2) Director-General's power of authorisation, s 18(2) (item 6)

Committee question (p. 9)

The committee therefore seeks more detailed advice from the Attorney-General as to the justification for this proposed approach, including whether consideration has been given to limitations being placed on the category of persons whom may be authorised to communicate information.

Attorney-General's response

The Bill retains the existing ability of the Director-General under s 18(1) to authorise a person to communicate intelligence on behalf of the Organisation, within the limits of that person's authority as conferred by the Director-General. Amending item 6 updates the unauthorised communication offence in s 18(2) to apply the new terminology of 'ASIO employee' and 'ASIO affiliate' proposed to be included by amending item 1 of Schedule 1, which will replace the terms presently used in that provision, consistent with other employment-related amendments proposed in the Bill.

As a result, the framework within which the Director-General communicates or authorises a person to communicate information held by ASIO is not significantly changed by the Bill. Proposed ss 18(2)(e) and 18(2)(f) reflect the existing provisions in ss 18(2)(b) and 18(2)(c) of the ASIO Act. There is no proposal to amend s 18(1), which allows the Director-General to authorise a person to communicate intelligence. Subsection 18(1) was inserted, in its present form, by the *Australian Security Intelligence Organisation Legislation Amendment (Terrorism) Act 2003* (Bills of 2002 and 2003). I note that this provision was not the subject of comment by this Committee as constituted in 2002 and 2003.[3]

I acknowledge the Committee's comment that the ability of the Director-General to approve 'a person' to communicate information may potentially impact on personal privacy. This matter is addressed in the Attorney-General's Guidelines to ASIO, issued under s 8A of the ASIO Act. Paragraph 13 of the Guidelines place obligations on ASIO in relation to the treatment of personal information. This includes an obligation to collect, use, handle or disclose personal information only for purposes connected with ASIO's statutory functions. The Guidelines also require the Director-General to take reasonable steps to ensure that personal information shall not be collected, used, handled or disclosed by ASIO unless necessary for the performance of its statutory functions (or as otherwise authorised or required by law). The communication of intelligence, and the authorisation by the Director-General of persons under s 18(1), is subject to the independent oversight of the IGIS.

The damage to Australia's national security interests that can be posed by the unauthorised communication of intelligence-related information should not be underestimated. The Bill, in relation to s 18(2), contains measures to reflect the culpability inherent in such wrongful conduct. However, the seriousness of such conduct must be balanced against the need to

3 Alert Digest No 4 of 2002, Report No 12 of 2002, Alert Digest No 4 of 2003.

ensure that the intelligence community is able to appropriately share information with those who have associated responsibilities for protecting Australian interests. Careful consideration is given to the sharing of intelligence-related information and who is authorised to do so, in accordance with the Attorney-General's Guidelines.

(3) Authorisation of classes of persons, s 23(6) (items 9, 34, 35)

Committee question (p. 11)

It is a matter of concern to the committee that the legislation appears to contain no criteria or limitations on the class of persons who may be authorised to exercise these coercive powers. The committee therefore seeks more detailed advice from the Attorney-General as to the justification for the proposed approach, including a more detailed elaboration of the above arguments.

Attorney-General's response

Amending items 9, 34 and 35 replace references in the relevant provisions to officers and employees of ASIO, consequential to the updating of employment-related terminology in amending item 1 of Schedule 1 to the Bill.

Amending item 8 replaces the reference in s 23(1) of the ASIO Act to "an authorised officer or employee" with a reference to "an authorised person". Amending item 9 similarly amends the Director-General's power of authorisation under s 23(6) to authorise persons for the purpose of s 23(1).

Consideration was given to limiting the persons able to be authorised under s 23(6) for the purpose of s 23(1) to ASIO employees and ASIO affiliates (as proposed to be defined in s 4 by amending item 1 of Schedule 1). However, such a limitation was not considered appropriate from an operational perspective. It may not always be possible to locate an ASIO employee or ASIO affiliate at the same location as an aircraft or vessel operator in order to ask questions, or make a request for information. It would be unnecessarily restrictive to operational realities for the legislation to require an ASIO employee or ASIO affiliate to be physically at a particular, and often unplanned, location of the aircraft or vessel (noting that such aircraft and vessels may also depart from that location at short notice). It was considered an operational and administrative necessity that, for the purposes of carrying out ASIO's functions, another person (or class of persons) may need to be authorised to undertake that activity on ASIO's behalf. For example, it would not be unreasonable to authorise such persons as, but not limited to, Customs officers, or law enforcement officers to undertake this activity on behalf of ASIO.

The proposed amendments to ss 90F(1) and 90F(2)(b) of the *Australian Postal Corporation Act 1989* (amending items 34 and 35 of Schedule 1) are in a similar category, noting that information or documents relating to articles carried by post, or articles in the course of post, may also be available at unplanned locations that may rapidly change.

While the Committee has observed that s 23 is a "significant powers to request information or documents from operators of aircraft or vessels", the amendments proposed to s 23 are consistent with other powers for the collection of information across the ASIO Act. For example, s 24 of the ASIO Act, as currently enacted, provides for an officer, employee, or other people, to be authorised to exercise the authority of a warrant issued under the ASIO Act. (I acknowledge, however, that the Committee has also commented on the proposed amendments to s 24. My response to those comments is provided below.)

To take account of the Committee's comments on amending item 6 of Schedule 1, I have asked my Department to revise the Explanatory Memorandum to elaborate on the justification for these items, in line with my remarks above.

(4) Authorisation of ASIO affiliates, (item 61)

Committee question (p. 12)

A key question for each of these instances is why is it appropriate to extend a range of powers, authorisations and exemptions to ASIO affiliates. This does not appear to be addressed in the explanatory memorandum other than to say it is 'consistent with operational requirements'. It seems to the committee that there is a real issue about what powers etc. might be appropriately be held by different classes of decision makers, how appropriate qualifications will be determined and assessed and what safeguards will apply given that ASIO affiliates are not employees of the organisation.

The committee seeks more detailed advice from the Attorney-General as to the appropriateness of extending these exceptions to this broad class of persons associated with ASIO.

Attorney-General's response

Rationale for the term 'ASIO affiliate', and limitations on the scope of its coverage

I acknowledge the perception that the proposed new term 'ASIO affiliate' is an expansion of the range of persons who can be authorised to exercise the Organisation's powers and functions. My Department and ASIO recently provided a submission to the Parliamentary Joint Committee on Intelligence and Security (PJCIS) inquiry into the Bill, which responded to submissions to that inquiry on this point.[4] A copy of this submission is provided at **Enclosure 2** to this correspondence. The commentary at pages 53-58 of the enclosed submission, and in particular at pages 57-58, may be of interest to the Committee.

As noted in the abovementioned submission, the proposed new term 'ASIO affiliate' is a label which describes a range of persons, who are not employees, who perform functions or services for ASIO. It is a label which reflects the variety of mechanisms, including

4 AGD and ASIO, joint supplementary submission to the PJCIS inquiry into the National Security Legislation Amendment Bill (No 1) (unclassified), 29 August 2014, pp. 53-58.

secondment and consultancy arrangements, that are used to appropriately resource agencies, including an intelligence agency, to undertake their functions.

The proposed definition of the term 'ASIO affiliate' in amending item 1 of Schedule 1 to the Bill contains a mechanism for ensuring that an ASIO affiliate is an appropriate person to exercise powers for, or perform functions of, the Organisation. An ASIO affiliate is defined as a person who performs functions or services for ASIO pursuant to a contract, agreement or arrangement. An assessment of whether an individual holds the requisite or necessary qualifications to fulfil the requirements of that contract, agreement or arrangement would be an essential criterion taken into account by the Organisation before entering into any contract, agreement or arrangement with that person.

Decisions by the Director-General about the engagement of a person as an ASIO affiliate are consistent with the Director-General's overall control of, and responsibility for the Organisation in s 8, and are subject to the obligation on the Director-General in s 20 to take reasonable steps to ensure that the work of the Organisation is limited to what is necessary for purposes of the discharge of its functions, and to ensure that the Organisation is kept free from any influences or considerations not relevant to its functions, and nothing is done that might lend colour to any suggestion that it is concerned to further or protect the interests of any particular section of the community, or with any matters other than the discharge of its functions. The activities of ASIO in entering into a contract, agreement or arrangement for the performance of functions or services for that Organisation are also subject to the oversight of the IGIS.

In addition, the validity of any activities or actions undertaken by an ASIO affiliate depends on the person acting in accordance with the relevant contract, agreement or arrangement. If an ASIO affiliate exceeds his or her authorisation under the relevant contract, agreement or arrangement, he or she would not be acting as an affiliate, and may also be subject to criminal liability in respect of any unauthorised actions.

Further, as the term 'ASIO affiliate' identifies the pool of persons who might be able to do certain things under legislation, the relevant 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.

Explanation of the consequential amendments in Part 2 of Schedule 1 to the Bill

As the Committee has identified, Part 2 of Schedule 1 to the Bill proposes a number of consequential amendments to provisions of Commonwealth legislation which confers upon ASIO personnel various powers, authorities, duties, obligations, immunities and liabilities. Such personnel are generally referred to '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 generally substitute the phrase "officer or employee' of ASIO" with the phrase "ASIO employee or ASIO affiliate" (or in some instances, use the term 'ASIO employee' or 'ASIO affiliate' alone). In the development of these consequential amendments, consideration was given to consistency with the overarching policy intention of the relevant legislation being amended.

For example, the Committee has specifically referred to amending item 61, which inserts a new s 7(2)(ad) in the *Telecommunications (Interception and Access) Act 1979* (TIA Act). Presently, s 7(2)(ac) of the TIA Act provides that the general prohibition on interceptions in s 7(1) of that Act does not apply to an activity undertaken by an "officer of the Organisation" for the purpose of determining if a listening device is being used, or to determine the location of such a device. Amending item 60 updates this provision to refer to an 'ASIO employee', consequential to amending item 1 of Schedule 1. Amending item 61 applies a corresponding exception from s 7(1) in relation to the actions of ASIO affiliates. It is appropriate that the exception to s 7(1) applies to all persons who have been engaged to perform a role within ASIO that may include undertaking these activities. The exception in s 7(2)(ac) is directed to conduct rather than the technical nature of a person's relationship with ASIO. Limiting the exception in s 7(2) of the TIA Act to 'ASIO employees' would result in an arbitrary distinction in relation to the application (or otherwise) of s 7(1).

In recognition of the Committee's comments, I have asked my Department to revise the Explanatory Memorandum to the Bill to include a statement outlining the oversight and control mechanisms in relation to ASIO affiliates, and an elaboration of the need to apply the term, and its legal effect, in relation to each consequential amendment in Part 2 of Schedule 1 to the Bill.

Schedule 2 – Powers of the Organisation (questions 5-10)

(5) Approval of classes of persons, s 24(2) (item 8)

Committee question (p. 13)

The committee is mindful of these difficulties, [in relation to maintaining lists of authorised persons] *however the committee also notes that there are accountability benefits associated with a requirement that persons able to exercise extensive coercive powers be identified with exactness, and that the responsibility for the appointment of such persons be clear. There is a danger that specification of persons able to exercise these extensive powers by reference to a class of persons (1) may be over-inclusive in the sense that particular persons covered may not be appropriately qualified to exercise the powers, and (2) that situations may arise in which it is uncertain whether a particular person is covered by an authorisation of a class of persons. Both of these problems may be thought to lessen the level of accountability associated with the exercise of authority under warrants.*

Noting these concerns, the committee seeks the Attorney General's advice as to whether consideration has been given to these matters and whether there are ways in which to address them. The committee is also interested in whether it would be appropriate to provide legislative guidance as to any parameters on the class/es of persons to whom authorisation can be granted and whether the option to authorise classes of persons could be limited to emergency situations (those involving 'very short notice').

Attorney-General's response

I confirm that consideration has been given to the matters raised by the Committee. Outlined below is further context to the use by ASIO of authorisation lists in relation to the exercise of special powers under warrant.

Context – ASIO's use of authorisation lists

In practice, to ensure compliance with the legislation and provide sufficient operational flexibility, ASIO may need to list a large number of persons as being authorised to carry out warranted activities – though they may not all be required to exercise authority under the warrant.

As a result, an authorisation list is not a record of who carried out authorised activity. Both the existing provision, and the proposed amendment, rely upon ASIO maintaining effective records in relation to the actual execution of the warrant for accountability and oversight purposes. This is an area that the IGIS will continue to inspect and monitor.

It is common that an authorisation list includes a range of persons with the range of skill-sets required. Each person authorised will possess a relevant qualification or a skill; however, not all authorised persons will possess all of the skills and qualifications required to carry out all activities authorised by the warrant. Each person who is authorised will generally perform a particular role within a team. For example, in the case of a search warrant it may be necessary to authorise:

- persons who will facilitate entry to target premises;
- persons who inspect data on a computer at the premises; and
- law enforcement officers who can provide protection to persons carrying out the warranted activities.

Members of a specified class of authorisation can be ascertained by internal records demonstrating who is occupying a certain position or role in ASIO. ASIO has a number of mechanisms and safeguards that are directed at ensuring that ASIO officers have the necessary qualifications, skills and expertise for their position or role including recruitment, training, supervision and performance management regimes.

The ability to authorise classes of persons is consistent with s 55 of the TIA Act which allows classes of officers or employees of ASIO to be authorised to exercise the authority conferred by a Part 2-5 warrant.

The need for operational flexibility means that the current practice, which requires specific officers to be authorised to exercise the authority of a warrant, has led to the authorisation lists including up to 50 names (including, for example, linguists, technical officers, case officers and analysts). The specification of a large number of names to provide operational flexibility does not provide additional meaningful accountability.

Whether legislative guidance as to any parameters on the class or classes of persons to whom authorisation can be granted

Any parameters on the classes of persons to whom authorisations can be granted would need to be sufficiently flexible so as not to defeat the purpose of enabling ASIO to achieve the required operational flexibility. In particular, the amendment seeks to provide ASIO with flexibility to encompass a broad range of appropriate persons to exercise powers under a warrant or request information or documents from operators of aircraft or vessels. I consider it is preferable that existing oversight and accountability mechanisms (including the role of the IGIS in reporting on the propriety with which ASIO carries out its functions) be the means by which ASIO's exercise of special powers, including authorisations of classes of persons, is monitored.

Whether the option to authorise classes of persons could be limited to emergency situations

As noted in the Explanatory Memorandum to the Bill, the execution of a warrant sometimes take place in unpredictable and volatile environments requiring ASIO to expand the list of individually authorised persons at very short notice. An operational opportunity to exercise the authority of a warrant may be lost before an authorisation list can be updated. For this reason, it would be impracticable to provide statutory authority for the Director-General to authorise classes of persons only in emergency situations.

(6) Entry to third party premises, ss 25(4)(aa), 25A(4)(aaa) (items 10, 19)

Committee question (p. 14)

Noting the above comments [at p. 14 about the exceptional nature of the power], *the committee seeks the Attorney-General's advice as to whether it would be possible to constrain the power to enter third-party premises. If it is thought that it would not be possible to further constrain this power in the legislation, a detailed rationale as to why that is the case (and details of any internal safeguards or procedures in place to constrain this power) would assist the committee in assessing the appropriateness of this provision.*

Attorney-General's response

In my view it would unduly limit the ability of ASIO to carry out its functions if further constraints were placed on the proposed power to enter third party premises. Consideration has been given to submissions made to the PJCIS inquiry into the Bill suggesting that the power to enter third party premises be authorised subject to a 'necessity' test.

Rationale

The purpose of the amendment is to enable ASIO to enter or exit third-party premises where necessary, but also where such entry or exit serves an operational imperative. For example, where entry via adjoining premises allows ASIO to reduce a risk of detection, or where a person unexpectedly arrives at target premises and the safest means of exit is via third party premises. In such circumstances, a requirement to meet a 'necessity test' may preclude ASIO from acting in the most operationally effective and appropriate manner.

The power to enter third party premises does not provide any power to search or otherwise collect intelligence on the third party premises – it is limited to entry to the premises.

Safeguards and procedures that would constrain this power

The range of existing safeguards provide an appropriate and effective framework of checks and balances in respect of ASIO's use of its powers and ensures that ASIO's activities are necessary and proportionate.

The proposed power to enter third party premises can only be exercised under the authority of a warrant. Before I issue a warrant, I must be satisfied that certain thresholds are met. Before entry onto third party premises can be authorised in the warrant, I must consider it appropriate in the circumstances to authorise such entry. In addition, the Attorney-General's Guidelines to ASIO, issued under s 8A of the ASIO Act, require all activities to be done with as little intrusion into individual privacy as possible. Third-party premises would only be accessed in accordance with these Guidelines. Consistent with the Guidelines, ASIO's methodology and operating procedures place an emphasis on the principle of 'proportionality', and are designed to ensure an appropriate and proportionate response, having close regard to both individual privacy considerations and the potential gravity of the threat being investigated. All warrants are available to the IGIS for inspection pursuant to the IGIS Act.[5]

(7) Surveillance devices – interaction with State and Territory laws (item 29)

Committee question (p. 16)

The committee seeks advice from the Attorney-General as to whether there may be circumstances where use of surveillance devices by ASIO not authorised under Subdivision D may be lawful under State and Territory law and whether, therefore, the repeal of subsections 26(1) and 26A(1) will operate to enlarge the circumstances in which the use of surveillance devices is lawful. Further, if that is so, the committee seeks the Attorney-General's advice as to the rationale for not dealing comprehensively with the legality of the use of surveillance devices by ASIO in the ASIO Act.

Attorney-General's response

Circumstances in which the use of surveillance devices is lawful

The proposed removal of the general prohibitions in ss 26(1) and 26A(1) of the ASIO Act is consistent with the approach taken and the rationale for introducing a surveillance device framework under the *Surveillance Devices Act 2004*.

The general prohibition of ASIO officers' use of surveillance devices reflects the Commonwealth preference for legislating some 35 years ago, at a time when the regulation of the use of listening devices by the states and territories was in its infancy. Today, a selective

5 See further, AGD and ASIO, joint supplementary submission to the PJCIS (unclassified) 29 August 2014, p. 60; and AGD, supplementary submission (8 September 2014), p. 6. (Copies provided at **Enclosure 2**.)

prohibition of this nature stands alone among Australian jurisdictions. Rather than prohibiting the use of surveillance devices, the Bill establishes a structured process for the use of surveillance devices that is clear and transparent. The draft provisions set out when an ASIO officer 'may' use a particular surveillance device without a warrant. This approach is similar to the regime applicable to Commonwealth law enforcement officers set out in the Surveillance Devices Act.

A blanket prohibition is enduring and removes the ability for the use of surveillance devices to be regulated by States and Territories. For example, an amendment in 1986 to s 22 of the ASIO Act incorporated in the definition of a 'listening device' a device that can record images. The effect of the prohibition in s 26(1) is to make it unlawful for an ASIO officer to record images that are being communicated. Although the content of this prohibition is unclear, no other jurisdiction in the country would outlaw the covert photography of images being communicated by ASIO in and of itself. Nonetheless, the confusion and the possibility that an ASIO officer may inadvertently act unlawfully in recording an image being communicated is solely the result of the general prohibition in s 26(1).

The use of surveillance devices is normally regulated by State and Territory law and these regimes are generally more permissive than the ASIO Act – for example, some State regimes do not regulate the use of particular devices at all. The starting point for the use of surveillance devices under the ASIO Act is to prohibit all such use by ASIO officers (ss 26(1) and 26A(1) of the ASIO Act) and then to authorise particular use in certain circumstances. For this reason, the proposal to remove the general prohibition on the use of surveillance devices that currently appears in the ASIO Act will generally result in the enlargement of circumstances in which ASIO's use of surveillance devices without warrant is permitted. Examples of the practical effect of the repeal include:

- In some states, such as Queensland and South Australia, there is no general prohibition on the use of optical surveillance devices. In these jurisdictions, ASIO officers would be free to use such devices were it not for s 26(1) of the ASIO Act. The latter provision prohibits an ASIO officer from using a hand-held camera in certain circumstances except pursuant to a warrant or the specific circumstances listed in the ASIO Act. No such prohibition is imposed on other parts of the community such as private investigators, foreign intelligence officers or law enforcement officers. The removal of s 26(1) will align the permissible activities of ASIO officers with other members of the community.
- In some states, (for example, South Australia, Queensland, Tasmania and the Australian Capital Territory), it is not otherwise unlawful for persons to use a tracking device. The repeal of s 26A(1) will make uniform the application of tracking device laws in those States or Territories, irrespective of whether the person is an ASIO officer.
- The removal of the prohibition will also expand the circumstances in which the use of listening devices without warrant is lawful in certain jurisdictions. This is because the Acts relating to surveillance devices in those jurisdictions exempt ASIO from the operation of those provisions. For example, s 5(b) of the *Surveillance Devices Act 1999* (Vic) provides that nothing in that Act applies to anything done in the course of duty by the Director-General or an officer or employee of ASIO. A similar provision exists in the

Western Australian and Tasmanian legislation. (I note, however, that where the installation, use, maintenance or recovery of surveillance devices contravenes any other law – for example, because it amounts to a trespass – such use of surveillance devices will not be permitted without a warrant.)

- The ASIO Act has not kept pace with developments in other Australian jurisdictions. For example, s 26(1) comprehensively states the circumstances in which ASIO may use a listening device. The removal of s 26(1) will bring ASIO's use of listening devices in line with State and Territory surveillance device legislation by permitting the use of a listening device for the purpose of protecting the lawful interests of the ASIO officer, which is permitted in most other jurisdictions.

Rationale for "not dealing comprehensively with the legality of the use of surveillance devices by ASIO in the ASIO Act"

As the Committee has identified, Division 2 of Part III of the ASIO Act is not an exhaustive or comprehensive statutory 'code' in relation to the legality of the use of surveillance devices by ASIO, and is not intended to serve such a purpose. No comprehensive statute exists under Australian law in relation to the use of surveillance devices by any other entity, whether a law enforcement agency, an intelligence agency, or any other person or organisation. Legislative responsibility with respect to the use of surveillance devices is divided between the Commonwealth and the States and Territories, and regulation is subject to both statute and common law.

The measures proposed in item 29 of Schedule 2 to the Bill reflect the recommendation of the PJCIS in its 2013 *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation* that the ASIO Act be amended "to modernise the warrant provisions to align the surveillance device provisions with the *Surveillance Devices Act 2004*, in particular by optical devices" (recommendation 30). The PJCIS was motivated by a desire to align, to the extent possible, ASIO's surveillance powers for intelligence purposes with those in the Surveillance Devices Act, the main purpose of which is to regulate surveillance device operations by law enforcement agencies (per s 3 of the Surveillance Devices Act).

Consistent with my comments above, the Surveillance Devices Act does not purport to deal comprehensively with the legality of the use of surveillance devices by law enforcement agencies and, accordingly, this approach has been replicated in the ASIO Act. The Surveillance Devices Act was developed in consultation with the States and Territories, and was intended to serve as a model for the enactment of surveillance legislation in States and Territories to regulate matters within their jurisdictions (recognising that the Commonwealth does not have a general power to legislate with respect to criminal law or law enforcement).

As the Government intends to limit the proposed amendments to ASIO's surveillance powers in the Bill to the implementation of recommendation 30 of the PJCIS's 2013 inquiry, I do not propose that the Bill should make broader amendments to cause the ASIO Act to deal comprehensively with the legality of the use of surveillance devices by ASIO.

(8) ASIO affiliates – exercise of powers under Division 2, s 26F (item 29)

Committee question (p. 19)

Given the importance of this objective, that is, ensuring that the use of surveillance devices without warrant is used by appropriately qualified ASIO staff, the committee seeks further advice from the Attorney-General as to whether consideration has been given to excluding 'ASIO affiliates' from the exercise of these powers unless they are positively determined to be appropriate persons to exercise such powers. The committee notes that this approach would provide a more robust safeguard than the current proposed approach. It is not clear from the explanatory memorandum whether this alternative has been considered.

Attorney-General's response

The existing provisions of Division 2 of Part III of the ASIO Act already provide that ASIO may use surveillance devices without a warrant, including by agents of ASIO, albeit, in limited circumstances (especially when compared to law enforcement). The inclusion of agents in the relevant provisions recognises that, in some circumstances, it may be appropriate for persons who are not employees of ASIO to use a surveillance device, for a purpose relating to security – for example, a person seconded to ASIO may be required to use a listening device to conduct a security interview with a person with that person's consent. The concept of an 'ASIO affiliate' replaces the term 'agent of the Organisation' as used in the existing provisions, and offers greater transparency as to who may use surveillance devices without warrant as its scope is defined in the Bill.

As I have mentioned above, the practical effect of the definition of the term 'ASIO affiliate', and the circumstances in which it is used across legislative provisions, is that such persons are 'positively determined' to be appropriate persons to exercise powers such as the use of surveillance devices without warrant. The validity of any activities or actions undertaken by an ASIO affiliate depends on the person acting in accordance with the relevant contract, agreement or arrangement. If it was envisioned that an ASIO affiliate would be in a position to exercise such a power, the suitability of that individual would be a relevant criteria taken into account before entering into a contract, agreement or arrangement with the individual to perform that particular role.

Further, the proposed framework for ASIO's use of surveillance devices without a warrant draws from Commonwealth, State and Territory surveillance device legislation. Such frameworks do not make unlawful, the use of surveillance devices in certain circumstances. For example, the use of tracking devices with consent is not prohibited in any State or Territory. Where there is no such prohibition, I do not consider there to be a justification for requiring an ASIO affiliate to be separately authorised to engage in activities that an ordinary member of the public is not prohibited from engaging in. I remain of the view that the inclusion of proposed s 26F provides an additional, and robust, safeguard consistent with that envisioned by the Committee in Alert Digest No. 11 of 2014.

(9) Use of reasonable force against persons, s 27A(2)(a) (item 36)

Committee question (p. 19)

In general the committee expects that the necessity of authorising force against persons in the execution of warrants to be examined and justified in explanatory memoranda. The committee therefore seeks the Attorney-General's advice as to the justification for the authorisation of force against persons in this context.

Attorney-General's response

My Department and ASIO recently provided detailed evidence to the PJCIS in relation to this matter. The submissions provided at **Enclosure 2** to this correspondence may be of assistance to the Committee.[6]

In summary, 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.

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. This could occur, for example, through a person preventing access to a room or an item or preventing a person authorised to execute the warrant from leaving the premises by blocking the exit. In the absence of the ability to use reasonable force against a person, any person seeking to obstruct the execution of the warrant could do so by standing in a doorway so that anyone seeking to go through that doorway would come into physical contact with them. If, in pushing past a person obstructing a doorway, the person executing the warrant came into physical contact with the person obstructing their access, the person executing the warrant may have committed an assault. In the absence of a power to use reasonable force in the execution of a warrant, this would not be authorised and could potentially lead to civil action or criminal charges.

Additionally, where police assist in the execution of an ASIO search warrant, they rely on the powers available to them under the warrant, rather than any generic police power. This means that they would rely on the ability in the ASIO Act to use force, the absence of such a power would hamper police. Further, while ASIO will often request law enforcement attendance at the execution of warrants, police will not be present in all instances.

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

6 AGD, responses to questions taken on notice on 15 August 2014 (18 August 2014), pp. 10-12; AGD and ASIO, joint supplementary submission (unclassified) (29 August 2014), pp. 61-62.

circumstances, it cannot constitute grievous bodily harm or lethal force. Any use of unauthorised force against a person may attract civil and criminal liability.

(10) Evidentiary certificates, s 34AA (item 47)

Committee question (pp. 21-22)

These subsections, [subsections 62(5)-(8) of the Surveillance Devices Act 2004] *especially (5) and (6) appear to provide further safeguards, and the committee is interested in whether analogous provisions would be appropriate in this context. The Guide to Framing Commonwealth Offences, Infringement Notices and Enforcement Powers states (p. 55) that 'procedural safeguards have generally been included with provisions for evidentiary certificates directed to a technical/scientific context', but does not specify examples. The explanatory memorandum explains how this provision works but it is not clear why it has been considered necessary to include it. The committee therefore seeks the Attorney-General's advice as to the justification for the proposed approach, including whether the additional provisions outlined above would be appropriate in this context.*

Attorney-General's response

While ASIO's role is to gather intelligence in accordance with its statutory functions set out in s 17 of the ASIO Act, there are occasions on which intelligence gathered by ASIO may be used in evidence in court to support criminal prosecutions or in civil proceedings. Most of the major counter-terrorism prosecutions conducted to date have made use of intelligence in evidence.

In adducing such evidence, it is important that ASIO's sensitive capabilities, including the identity of ASIO employees and others giving evidence, are not exposed in open court. In its 2013 *Report on Potential Reforms to National Security Legislation*, the PJCIS recognised the "legitimate need to protect the technological capabilities of ASIO where information under warrant is eventually led in evidence as part of the prosecution" (at pages 132-133).

Consistent with the recommendation of the PJCIS in that inquiry, proposed s 34AA will provide a mechanism to minimise the risk of revealing technical capabilities and the identity of ASIO employees or sources in evidence in proceedings. The proposed provision will also reduce the need for senior ASIO officers and other expert technical witnesses to be diverted from their duties to attend court and give evidence concerning the execution of warrants and the use of the information obtained from the warrants.

Proposed s 34AA is intended to operate in a manner that will ensure the veracity of the information gathered can be tested by the court, as certificates are of a prima facie rather than conclusive nature. An accused person in criminal proceedings, or a party to civil proceedings, could therefore lead evidence to challenge the matters set out in a certificate.

In addition, the proposed provision is not intended to authorise the issuing of certificates to facilitate proof of any ultimate fact, or any fact so closely connected with an ultimate fact as to be indistinguishable from it, or facts that go to elements of the offence. Rather, certificates must relate to the technical matters set out in proposed s 34AA(3). Evidence adduced in

support of an ultimate fact, or an element of an offence, will continue to be capable of protection under existing mechanisms such as those available under the *National Security Information (Criminal and Civil Proceedings) Act 2004.* In the event that a party to proceedings, or a presiding judge on his or her own initiative, was concerned that a certificate purported to apply to material facts or facts that would address or prove the ultimate facts in the case (or elements of an offence), the certificate could be struck out on the basis it has exceeded the limits of s 34AA.[7]

On this basis, I am of the view that proposed s 34AA strikes an effective balance between the protection of sensitive information pertaining to operational capability and the identity of sources, procedural fairness and operational efficiency.

Consideration of possible additional provisions

As the Committee has observed, proposed s 34AA is based upon similar regimes operating under the TIA Act and the Surveillance Devices Act. Due to the nature of the information associated with the execution of computer access and surveillance device warrants, it is not possible for the provision to exhaustively list the specific facts or matters that may be covered by a certificate issued under this section without putting at risk the very capabilities the regime is designed to protect.

Consideration was given to the possible inclusion in proposed s 34AA of provisions similar to those set out in ss 62(5)-(8) of the Surveillance Devices Act. On balance, it was considered it would not be appropriate to include these provisions. In some instances they would not be feasible in light of the classified nature of evidence to which they relate, and in others would unnecessarily duplicate powers already available to the court.

In particular, s 62(5) of the Surveillance Devices Act limits the court from admitting a certificate in evidence if the person charged or solicitor engaged by them has not had at least 14 days' notice as well as a copy of the certificate and reasonable evidence of the intention to produce the certificate. Certificates issued by ASIO under the TIA Act have generally borne a national security classification, as they contain facts and information that would damage national security were it to be publicly released. Noting the certificates to be issued under proposed s 34AA are designed to protect ASIO's capabilities and the identity of sources or staff, they too would likely be highly classified and therefore unable to be released to a person charged, or their lawyer in an unamended form. This would make compliance with a similar provision difficult.

In addition, ss 62(6)-(8) of the Surveillance Devices Act are statements of powers that are already available to the court in a criminal prosecution when dealing with evidentiary certificates. The court's inherent powers already allow it to order that specific witnesses are called in respect of certain evidence, and the court must also consider the evidence on its merits, with no weighting or credibility to be taken from the section establishing the ability to issue evidentiary certificates. It is, in my view, appropriate to leave these matters to the domain of the court in those proceedings in which a certificate is relevant.

---

7 See further, AGD and ASIO joint supplementary submission to the PJCIS inquiry into the National Security Legislation Amendment Bill (No 1) 2014 (unclassified) 29 August 2014, p. 62. See also: pp. 13-14 of the Explanatory Memorandum to the Bill (Human Rights Statement of Compatibility).

Schedule 3 – Special Intelligence Operations (questions 11-19)

(11) Differences to controlled operations scheme (general comment)

Committee question (pp. 22-23)

The committee notes that it would assist the committee's scrutiny of this schedule if it were aware (in a systematic manner) of the differences between the proposed SIO scheme and the controlled operations scheme. The committee therefore requests advice from the Attorney-General as to the differences between the proposed SIO scheme in schedule 3 of the bill and the controlled operations scheme in Part IAB of the Crimes Act 1914. In particular, the committee is interested in information as to:

- *any differences in the authorisation process (including matters on which authorising officers must be satisfied);*
- *any differences in the immunities (civil and criminal) provided in the two schemes;*
- *any differences in reporting and oversight mechanisms; and*
- *any other safeguards which are present in the controlled operations scheme that are not replicated in the proposed SIO scheme.*

Attorney-General's response

This issue has been the subject of extensive consideration by the Parliamentary Joint Committee on Intelligence and Security (PJCIS). On 29 August 2014, my Department and ASIO provided a detailed submission to that Committee, which included a systematic identification and explanation of differences between the two schemes.

A copy of this submission is provided at **Enclosure 2**. Pages 27-30 of that submission address the authorisation process (specifically the authorising officer, including responses to suggestions that an external or Ministerial authorisation model could be adopted in relation to SIOs). Pages 31-48 address all other areas of differences, including the authorisation process, protections from legal liability, reporting and oversight mechanisms, and other safeguards. A table summarising the key areas of difference is also provided at attachment 1 to that submission (pages 86-96).[8]

By way of general observation, and as noted at page 31 of the abovementioned submission, the proposed SIO regime is based upon, and largely analogous to, controlled operations in Part 1AB of the Crimes Act. These include 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.

---

8 The Committee may also be interested in the commentary at pages 67-69, addressing two further matters raised by some submitters to the PJCIS inquiry, concerning the policy and operational justification for the scheme, and whether it should be subject to a sunset provision and a statutory review requirement after five years of operation.

However, it is important that these elements are implemented in a way that is adapted to the specific purposes of each scheme – namely, the collection of intelligence in the case of SIOs, and obtaining evidence that may lead to a prosecution in relation to serious criminal offences in the case of controlled operations.

In particular, SIOs are directed to covert operations for the purpose of collecting intelligence relevant to security, consistent with ASIO's statutory functions. As such, SIOs will be directed to obtaining intelligence, typically over an extended 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. 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, it is important that the guiding principle in designing the SIO scheme – and in assessing its individual provisions – is that of suitability for the 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 more perfunctory exercise in identifying technical 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.

As outlined in the relevant passages of Enclosure 2, key areas of difference include: the definition of an SIO compared to the definition of a 'controlled operation'; the duration of authorisations; relevant authorising officers; aspects of 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 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.

(12) Use of evidence, s 35A (item 3)

Committee question (p. 24)

The committee notes this justification [at p. 100 of the EM], *however the committee requests further advice from the Attorney-General as to whether this approach is consistent with that taken in relation to the controlled operations scheme in Part IAB of the Crimes Act 1914 and, if it is not, a rationale as to why a different approach is required for special intelligence operations.*

Attorney-General's response

Proposed s 35A is consistent with s 15GA of the *Crimes Act 1914*. Subsection (2) of each provision ensures that information obtained, respectively, through a special intelligence operation (SIO) or a controlled operation can be admitted in evidence in proceedings without being subject to challenge, or excluded, merely because it was obtained through authorised conduct that would, but for the authorisation, have constituted an offence.

Importantly, neither proposed s 35A(2) nor s 15GA(2) require a court to admit such evidence. Rather, and in response to *Ridgeway v The Queen* (1995) 184 CLR 19, These provisions operate only to remove the risk that a court might exercise its discretion to exclude such evidence by mere reason of its connection with a special intelligence operation or a controlled operation. They otherwise preserve the general judicial discretion to admit or exclude evidence, and to accord an appropriate degree of weight to evidence admitted.

I note that s 15GA(2) of the Crimes Act has been in force since 2010, following its enactment in the *Crimes Legislation Amendment (Serious and Organised Crime) Act 2010* (Bill of 2009). I am advised that no practical issues have arisen in its use to date. I am also aware that a similar explanation to that at page 100 of the Explanatory Memorandum to the present Bill is provided at page 51 of the Explanatory Memorandum to the 2009 Bill, which did not attract comment from this Committee as constituted in 2009.[9]

(13) Description of conduct authorised, s 35H (item 3)

Committee question (p. 27)

Under the provisions of the bill in its current form the limits of authorised conduct under an SIO may be unclear because an SIO authority is only required to state authorised conduct in general terms. The committee therefore seeks the Attorney-General's advice as to whether it is possible to require authorised conduct to be particularised with more clarity.

Attorney-General's response

Proposed s 35D(1)(c) requires an SIO authority to provide a general description of the nature of the special intelligence conduct in which the persons referred to in paragraph (b) are authorised to engage. Proposed s 35H has the effect of authorising each person listed in the

9 Alert Digests No 9 and No 15 of 2009, and Report No 10 of 2009.

SIO authority to engage in the conduct set out therein. The immunity from legal liability in proposed s 35K applies to persons and conduct duly authorised.

A requirement for a general description of the nature of authorised conduct reflects a need for operational flexibility over the 12-month duration of an SIO, consistent with the purpose of such operations to gain close access to persons or organisations of security concern and to build a picture of them, which generally requires these operations to be undertaken over a sustained period of time. As such, it would not be practicable to require an SIO authority to include a significantly higher degree of particularisation of conduct in advance of the commencement of an operation.

For example, while it would be feasible to identify the general nature of conduct to be engaged in as part of an SIO (such as associating or participating in training with members of a terrorist organisation) it is unlikely to be possible to identify individual actions for the purpose of providing prior authorisation (such as authorising specified times or places of association with an organisation, particular training activities, or potentially individual members or affiliates of that organisation with whom participants in an SIO can associate).

Accordingly, the requirement in proposed s 35D(1)(c) that the SIO authority must "state a general description of the nature of the special intelligence conduct" is intended to remove any risk that the immunity in proposed s 35K may be found not to apply because an authorisation did not particularise an individual action, notwithstanding conduct of that general nature was authorised. This is consistent with the purpose of the proposed SIO scheme, to ensure that there is adequate certainty in relation to the legal status of participants in such operations, in preference to relying solely on prosecutorial and investigative discretion after they have engaged in the relevant conduct as part of an intelligence operation.

Additionally, given the possible application of various State and Commonwealth criminal laws in relation to any particular authorised conduct, it will not be practicable to specifically define and detail with absolute precision such conduct without an exhaustive comparison of all possible criminal laws that might apply. Criminal offences can often broadly overlap and have application in relation to certain general conduct. Yet the specific elements of such applicable offences will vary from jurisdiction to jurisdiction or from offence to offence. For example, a specific authorisation in relation to being a member of a terrorist organisation, without more, may render the person liable to other related offences, such as 'association', 'training' and 'possession' offences, as well as the offence of 'other acts done in relation to planning or preparing for terrorist acts' as found in the Criminal Code. More broadly, the person may also be liable for offences applicable State offences in some instances. Accordingly, to provide certainty to persons participating in an SIO in relation to the application of the immunity provisions, the authorised conduct can only described in general terms rather than any attempt to meet the elements of particular offences.

The latitude provided for in proposed s 35D(1)(c) is caveated by a number of significant safeguards. Under proposed s 35C(2), an authorising officer may only grant an SIO authority if he or she is satisfied, among other things, that any unlawful conduct will be limited to the maximum extent consistent with conducting an SIO. The authorising officer must also be satisfied that the operation will assist the Organisation in performing one or more of its

special intelligence functions, and the circumstances are such as to justify the conduct of an SIO. The degree to which conduct is particularised in an application, or is capable of being particularised, will be relevant to an assessment of these matters. Decisions about the authorisation and conduct of an SIO – including the degree of conduct particularised – are subject to independent oversight by the IGIS, who is empowered to inquire into the legality and propriety of ASIO's actions.

In addition, authorisations granted under proposed s 35C, and the immunity under proposed s 35K, cannot extend to conduct that causes death or serious injury, involves the commission of a sexual offence, results in significant loss of or damage to property, or which involves conduct in the nature of 'entrapment'. Proposed s 35L further provides that an SIO authority cannot authorise conduct that requires authorisation in accordance with a warrant issued under the ASIO Act or Part 2-2 of the *Telecommunications (Interception and Access) Act 1979*, or an authorisation made under Part 4-1 of the latter Act. An SIO authority can also be granted on any conditions the authorising officer may decide to apply under proposed s 35C(3), which could include further limitations on authorised conduct as appropriate. Further, as I have noted above, the Attorney-General may issue written guidelines under s 8A of the ASIO Act regarding the performance by ASIO of its functions or the exercise of its powers in relation to SIOs.

Given that the intention of the SIO scheme is to provide legal certainty to ASIO and individual participants in respect of the conduct of an SIO, it is in ASIO's operational interests to ensure that there is clarity, in advance, as to the conduct that is authorised as part of such an operation. If doubt arose as to whether a participant was authorised to undertake a particular activity as part of an SIO, it would be open to an authorising officer to vary the authority (on application or on his or her own motion) to authorise or exclude the relevant activity as appropriate. In the event there was doubt that a participant's action was authorised under an SIO authority, the matter may be referred to the Australian Federal Police for investigation, and if appropriate subsequently referred to the Commonwealth Director of Public Prosecutions, in accordance with normal law enforcement processes.

As indicated in the joint submission of my Department and ASIO to the PJCIS of 29 August 2014, the Government is giving further consideration to additional reporting and notification requirements to the IGIS, to enhance opportunities for oversight. This includes consideration of a requirement to notify the IGIS when an authority is issued, and when certain kinds of authorised conduct are engaged in.[10]

Recognising the Committee's concerns, however, I have also asked my Department to give consideration to whether the policy intent could be achieved by removing the word 'general' from the s 35D(1)(c) so that an SIO authority is required to include a statement of the nature of the authorised conduct, combined with an explanation of the intended meaning in the Explanatory Memorandum.

I note that the word 'general' is not used in the corresponding provisions of the Crimes Act in relation to controlled operations, ss 15GK(1)(f)(i) and 15GK(2)(f)(i). It has been included in

---

10 AGD and ASIO, joint supplementary submission to the PJCIS, 29 August 2014, pp. 29-30

proposed s 35D(1)(c) due to concerns to remove any ambiguity as to the requisite degree of particularisation in a description of the nature of the relevant conduct under an SIO authority.

Such ambiguity may arise because, unlike the controlled operations scheme, the proposed SIO scheme does not distinguish between civilian and non-civilian participation.[11] The controlled operations scheme distinguishes between the degree of particularisation required in controlled operations authorities for the authorised conduct of civilian and law enforcement participants respectively. Subparagraph (i) of ss 15GK(1)(f) and 15GK(2)(f) require an authority to specify "the nature of the controlled conduct" in which a law enforcement participant may engage. Subparagraph (ii) of the above provisions requires an authority to set out "the particular controlled conduct" in which a civilian participant may engage. As such, an interpretation of the degree of particularisation required by subparagraph (i) of ss 15GK(1)(f) and 15GK(2)(f) can be informed by reference to the comparatively higher degree of specificity required in subparagraph (ii).

As this interpretive approach is necessarily unavailable in relation to proposed s 35D(1)(c), since the SIO scheme does not distinguish between civilian and non-civilian participation, the inclusion of the word 'general' in the provision was considered appropriate to evince an intention that particular actions do not, as a matter of law, need to be specified in an SIO authority (and ensuring that an authorising officer may exercise his or her discretion in an individual case to limit an authority to specific actions, if considered appropriate).

(14) Defects in authorisations – material v immaterial particulars, s 35J (item 3)

Committee question (pp. 27-28)

The committee therefore seeks the Attorney-General's further advice as to the justification for the necessity of this provision. Further, if the provision is considered necessary, the committee seeks advice as to the sort of defects that would not invalidate applications and authorisations (and whether more detailed guidance on this may be included in the provision).

Attorney-General's response

I acknowledge and support the Committee's concern to ensure that ASIO implements appropriate procedures to obviate the risk of defects in SIO authorities. I consider that appropriate provision is made for this important matter in the thresholds required by the authorisation criteria in proposed s 35C, the requirements for the making of applications in proposed s 35B and for the issuing of authorisations in proposed s 35C, all of which are subject to the general oversight of the IGIS. I note that successive Governments and Parliaments have, justifiably, placed significant trust and confidence in the professional judgment and performance of ASIO. The high quality of its documentation in relation to

11 The reasons for this approach have been mentioned in response to question 11 above, and are further explained in Enclosure 2 (pp. 34-35).

warrants issued under Division 2 of Part 3 of the ASIO Act was also recently observed by the IGIS in her submission to the PJCIS inquiry into this Bill.[12]

However, proposed s 35J is necessary because special intelligence operations are major undertakings which can involve a significant investment of ASIO's resources over a sustained period of time, and will yield a significant benefit in enabling the collection of intelligence presently unable to be collected. As such, it would be inefficient and unreasonable if authorities were invalidated – and any intelligence collected potentially unable to be used – as a result of minor matters that pertain to form or process. Proposed s 35J is directed to avoiding this outcome. Without a provision of this kind, significant and resource-intensive operations could be invalidated on the basis of minor defects that do not in any way affect the basis on which an authority was granted. This outcome would, in my view, be disproportionate to the minor nature of the defect in an authority.

As noted at page 107 of the Explanatory Memorandum, the materiality (or otherwise) of a defect in relation to a particular in an SIO authority is capable of determination in the circumstances of individual applications, in accordance with the ordinary meaning of the term 'material'. The Explanatory Memorandum further includes a guiding principle, that a defect affecting a material particular is intended to include one that vitiates the basis on which an application was made, or an authority granted, or a variation requested or granted.

In other words, a defect will relate to a material particular if it pertains to a detail that affected the decision of a person that was made in reliance on that detail. This may include, for example, an inaccuracy in the factual details relevant to the granting of an authority, on which a decision to make an application or grant an authorisation was based. In contrast, a defect in relation to a non-material particular may include, for example, a typographical error in an application or an authority.

There is considerable precedent in relation to the judicial interpretation of the term 'material particular', particularly as an element of criminal offences concerning the making of false or misleading statements under oath.[13] The term is also used in a wide range of Commonwealth legislation, generally creating such offences. These matters, in my view, support a conclusion that the meaning of the term 'material particular' is sufficiently clear without a requirement for express statutory guidance in proposed s 35J.

I further note that an identical provision applies in relation to the controlled operations scheme in s 15H of the Crimes Act, as inserted by the Crim*es Legislation Amendment (Serious and Organised Crime) Act 2010* (Bill of 2009). This provision was accompanied by

---

12 Inspector-General of Intelligence and Security, Submission No 4 to the PJCIS inquiry into the National Security Legislation Amendment Bill (No 1) 2014, 4 August 2014, p. 14.

13 See, for example, *R v Millward* [1985] QB 519 at 525. (A statement was determined to be material to judicial proceedings if it influenced or may have influenced a judicial officer "in believing or disbelieving" a statement given in evidence, or "affected the determination of guilt or innocence" by a trier of fact.) See further, *R v Traino* (1987) 27 A Crim R 271. (A statement was determined to be material "if it is of such significance and importance, having regard to the whole of the evidence, that it is capable of affecting the decision of the appropriate tribunal of fact on the factual issue or issues" or "to a fact relevant to a fact in issue" or "to the credit of a witness".)

a similar explanation at page 73 of the Explanatory Memorandum to the 2009 Bill, which was not the subject of specific comment by this Committee as constituted in 2009.[14]

(15) Immunity from liability – comparison with controlled operations, s 35K (item 3)

Committee question (p. 28)

The committee notes this justification [at pp. 108-109 of the EM], *however the committee requests further advice from the Attorney-General as to whether this approach (including in relation to payment of compensation in respect of damage to property and personal injury and the status of civilian participants in operations) is consistent with that taken in relation to the controlled operations scheme in Part IAB of the Crimes Act 1914 and, if it is not, a rationale as to why a different approach is required for special intelligence operations.*

Attorney-General's response

As noted in my response to question 11 above, a detailed explanation is provided at pages 38-40 of the Department and ASIO's joint supplementary submission to the PJCIS of 29 August 2014, a copy of which is provided at **Enclosure 2** to this response.

(16) Disclosure offences – application, s 35P (item 3)

Committee question (p. 30)

As the justification for the breadth of application of these provisions is not directly addressed in the explanatory memorandum the committee seeks a more detailed justification from the Attorney-General in this regard. The committee emphasises that its interest is not only in the underlying purposes served by the provisions, but whether these purposes could be achieved by offences that are more directly connected and proportionate to the achievement of those purposes.

Attorney-General's response

The Government has, in developing the disclosure offences in proposed s 35P, given careful consideration to their scope of application, including whether more limited formulations could adequately achieve the legitimate objective of protecting sensitive operational information in relation to SIOs. The Government is of the view that proposed ss 35P(1) and (2) are necessary and proportionate to the legitimate objective to which they are directed, and that the alternatives considered would not provide adequate protection for the relevant information. These matters have also been addressed in considerable detail in the evidence of my Department and ASIO to the PJCIS, provided at **Enclosure 2.**[15] I address each of the

---

14 Alert Digest No 9 of 2009 and Report No 10 of 2009.

15 See especially: AGD, responses to matters taken on notice on 15 August (18 August 2014), pp. 17-22; AGD and ASIO, joint supplementary submission (29 August 2014), pp. 41-42, 47-48 (see also pp. 77-79 in relation to the proposed secrecy offences in Schedule 6 to the Bill); AGD and ASIO, second joint supplementary submission (9 September 2014), pp. 6-7.

Committee's main areas of interest below, with a focus on the basic offence in s 35P(1) given that its application is broader than the aggravated offence in proposed s 35P(2), which requires proof of a person's intention to cause certain harm in communicating the information, or that the communication of the information will cause harm.

Purpose served by proposed s 35P

The wrongdoing to which the offences are directed is the harm inherent in the disclosure of highly sensitive intelligence-related information. The disclosure of the very existence of an SIO – which is intended to remain covert – is, by its very nature, likely to cause harm to security interests. Given the necessarily covert nature of an SIO, disclosure of the existence of such an operation automatically creates a significant risk that the operation may be frustrated or compromised and that the safety of its participants, or persons associated with them such as family members, may be jeopardised. It may also jeopardise other investigations where there is some connection between the two – for example, if there is some relationship between the persons being investigated or an authorised participant, whose identity is disclosed, is known to associate with other persons who are also performing investigative roles. Once such information is disclosed, there is limited recourse available to address these significant risks. This harm is not contingent on a person's malicious intention in making a disclosure, except that it may be aggravated by persons who act with a malicious intention since this may further increase the prospects that these risks may eventuate. As such, there is a need for a strong deterrent to such behaviour.

A number of independent reviews of intelligence and secrecy legislation have found that it is appropriate to criminalise the disclosure of intelligence-related information on the basis that harm is inherent or implicit in the very act of disclosure, thereby obviating a need to prove any specific malicious intention on the part of the disclosure, or an adverse outcome of the disclosure. These have included the Hope Royal Commission on Intelligence and Security in its 1976 report on ASIO, and the Australian Law Reform Commission's 2009 Report on Secrecy Laws and Open Government in Australia, which specifically examined secrecy offences in respect of the Australian Intelligence Community.

Offences with largely identical elements have been enacted in relation to the controlled operations scheme in ss 15HK and 15HL of the Crimes Act. I am advised that no matters have been investigated, referred for prosecution, or prosecuted in relation to ss 15HK and 15HL of the Crimes Act, which have been in force since 2010. This, in my view, supports a conclusion that these offences have not operated to unduly infringe individual rights and liberties, particularly in respect of freedom of expression. I am further aware that the scope of the offences in ss 15HK and 15HL of the Crimes Act was not identified as a source of concern by this Committee, as constituted in 2009, in its examination of the Crimes Amendment (Serious and Organised Crime) Bill 2009 (Act of 2010).[16]

I acknowledge that the Committee has raised a number of specific concerns about the following matters, which are addressed in the subheading below.

- coverage of subsequent disclosures, including of information in the public domain;

16 Alert Digests No 9 and No 15 of 2009, and Report No 10 of 2009.

- coverage of persons including journalists and whistleblowers;
- absence of a requirement to prove harm or damage as a result of disclosures; and
- application of the offences on the basis of an internal authorisation process.

Consideration of alternatives

Coverage of information in the public domain

The offences are intentionally capable of covering information already in the public domain. This reflects the fact that the significant risks associated with the disclosure of information about an SIO (including its existence, methodology or participants) are just as significant in relation to a subsequent disclosure as they are in relation to an initial disclosure. Limiting the offences to initial disclosures would create an arbitrary distinction between culpable and non-culpable conduct, on the basis of a technical question of the order in which multiple disclosures were made.

Consideration was given to the inclusion of a specific defence for the communication of information in the public domain by reason of the authority of the Commonwealth. However, given that it is highly unlikely information about an SIO would ever be authorised, or capable of authorisation, for public release, it was considered that appropriate provision for such circumstances was made via the general defence of lawful authority under s 10.5 of the Criminal Code, together with general prosecutorial and investigative discretion. Further, I note that there is no equivalent exception in the offences in ss 15HK and 15HL of the Crimes Act for information already in the public domain.

Proposed s 35P(3) does, however, contain a number of exceptions for permitted disclosures. These include, in paragraph (b), disclosures for the purposes of legal proceedings arising out of, or otherwise related to the SIO scheme, or any report of such proceedings. This exception could therefore apply to a journalist who reported on legal proceedings in which the existence of an SIO was disclosed (however, disclosure may further be subject to any protective orders the Court may make in relation to such evidence).

Application to journalists and whistleblowers

The offences intentionally apply to all persons, consistent with the intention to avoid the significant risks arising from the very fact of disclosure of information about an SIO. I am aware that some stakeholders, including participants in the PJCIS inquiry into the Bill, have advocated for either a specific exception to the offences in favour of journalists, or a general public interest exception, where the trier of fact is of the view that the public interest in making a disclosure outweighed the detriment to security. I have strong reservations about either of these options, for the reasons outlined in the submissions of my Department and ASIO to the PJCIS inquiry into the Bill as provided at **Enclosure 2** to this correspondence.[17]

---

17 See especially: AGD, responses to questions on notice 15 August 2014 (18 August 2014), p. 23; and AGD and ASIO, joint supplementary submission (29 August 2014), pp.82-83. See further AGD and ASIO, second joint supplementary submission (9 September 2014), pp. 12-13. (The comments in the

In short, these reasons are, first, that it is contrary to the criminal law policy of the Commonwealth to create specific exceptions of this kind from the legal obligations of non-disclosure to which all other Australian persons and bodies are subject. It is appropriate that all members of the community are expected to adhere to non-disclosure obligations, which should apply equally to all persons – whether they are intelligence or law enforcement professionals or journalists reporting on national security matters. The absence of exceptions in favour of specific classes of persons is also consistent with the policy intention that the offences are directed to the risks posed to security as a result of the disclosure of sensitive information, which arise irrespective of the motives of the discloser.

Secondly, a general public interest defence is not considered necessary or appropriate for two reasons. Provision is already made for the disclosure of suspected wrongdoing to the Director-General of Security or the Inspector-General of Intelligence and Security under the *Public Interest Disclosure Act 2013*, which overrides secrecy laws of general application. The *Inspector-General of Intelligence and Security Act 1986* further overrides secrecy laws of general application in relation to persons who comply with notices for the production of documents or the provision of information issued under that Act.

In addition, a dedicated public interest defence is not, in my view, appropriate in relation to the offences in proposed ss 35P(1) or (2). This is because, even if a jury or a trial judge as the final arbiter of fact held that a disclosure was not in the public interest, the disclosure would have already occurred and the potential for harm actualised. Prejudice to security, and consequently harm to the public interest from a disclosure relating to an SIO can evolve quickly, such as in reprisals from persons being investigated. Harm could also evolve so slowly as to be difficult to detect – for example, the disclosure of a person's identity as an ASIO employee or an ASIO affiliate could be used by foreign intelligence services to target and infiltrate ASIO and its operations, or compromise its staff, over a significant period of time.

Further, a public interest defence would inappropriately designate a jury or a trial judge as the final arbiter of whether a particular disclosure caused harm to the public interest in the context of adjudicating criminal guilt. There is a risk that such individuals may not have an appropriate understanding or an appreciation of the possible impact of releasing that information, and will necessarily not be in a position to adequately asses how the disclosure of a particular piece of information may, when taken together with other information, cause prejudice or risk causing prejudice to security interests. Such a defence would further be inconsistent with the general policy intention I have outlined above.

I have, however, asked my Department to consider whether some additional exceptions to proposed ss 35P(1) and (2) could feasibly be included in proposed s 35P(3), in respect of legal advice, and pro-active disclosures to the IGIS by persons to whom the *Public Interest Disclosure Act 2013* does not apply. (That is, complaints to the IGIS by persons other than 'public officials' as defined under that Act, and disclosures to the IGIS in response to

---

latter submission were made specifically in relation to the proposed offences in Schedule 6 to the Bill, but apply equally to proposed s 35P.)

requests or as part of inspections rather than pursuant to the Public Interest Disclosure Act or statutory notices to produce issued under the IGIS Act.)

Resultant harm

I consider it appropriate that an intention to cause harm is limited to an element of the aggravated offence in proposed s 35P(2), and that the basic offence in proposed s 35P(1) does not include such an element. This is consistent with the policy intention outlined above. I note that the ALRC, in its 2009 report on secrecy laws and open government in Australia, considered that secrecy offences in respect of intelligence-related information did not need to include an element requiring proof of harm or intent to cause harm in making a disclosure, on the basis that the harm is implicit.[18]

Internal authorisation process

I acknowledge that the Committee is concerned that proposed s 35P may result in the exposure of persons to criminal liability who may not know that the information related to an SIO, recognising that the authorisation process is internal to ASIO. This matter is addressed in my response to question 17 below, in relation to the applicable fault element applying to this physical element of the offence. In short, the offences apply to persons who disclose information, and are reckless as to the circumstances that it relates to an SIO. This means that they must be aware of a substantial risk that the information related to an SIO, and acted unjustifiably in the circumstances by taking the risk of making the disclosure. As discussed further below, this is a high threshold for the prosecution to prove to the criminal standard.

In summary, for the reasons set out above, the Government's view that the offences in proposed s 35P represent a proportionate means of achieving the legitimate objective to which they are directed, being the protection of sensitive operational information (including information concerning the existence of an operation together with details of its methodology and participants).

18 Australian Law Reform Commission, Report 112, p. 289 at [8.65] and recommendation 8-2 at p. 307.

(17) Disclosure offences – fault elements ss 35P(1)(b) and 35P(2)(b) (item 3)

Committee question (p. 30)

A further reason why these offences may be considered to be too broad in their application is that it is possible they may apply to the disclosure of information even if the person who discloses the information is not aware that it relates to an SIO. Given the nature of an SIO it is likely that only persons within the Organisation will know whether information relates to an SIO. It is also relevant to note that the boundaries of an SIO, and therefore what information 'relates' to such an operation, may be unclear to the extent that an SIO authority need only state 'a general description of the nature of the special intelligence conduct that the persons' authorised to engage in conduct for the purposes of the SIO 'may engage in' (paragraph 35D(1)(c)).

The committee therefore also seeks clarification about (and a justification for) the applicable fault requirement in relation to the element that 'the information relates to a special intelligence operation' (paragraph 35P(1)(b) and paragraph 35P(2)(b)).

Attorney-General's response

The physical element in (b) of each of ss 35P(1) and (2) is a circumstance in which conduct occurs, within the meaning of s 4.1.(1)(c) of the *Criminal Code 1995.* As the provision does not specify a fault element, s 5.6(2) of the Criminal Code operates to provide that the fault element of recklessness applies. Recklessness is defined in s 5.4(1) of the Criminal Code to mean that the person was aware of a substantial risk that the information disclosed related to a special intelligence operation, and unjustifiably, in the circumstances known to him or her at the time, took the risk of making the disclosure.[19]

Accordingly, it is not necessary for the prosecution to establish that a person had knowledge that the information related to an SIO, in the sense of a conscious awareness of the existence of an SIO and that the relevant information related to that operation. However, the prosecution must establish, beyond reasonable doubt, that a person was aware of a real and not remote possibility that the information was so related. As such, the offences will not apply to a person who disclosed information entirely unaware that it could relate to an SIO, since there would be no evidence of an advertence to a risk of any kind.

In addition, proof of a person's awareness of a substantial risk will depend on the availability of evidence of a person's awareness of relevant information about an operation or a suspected operation, which must suggest more than mere advertence to a nominal or speculative possibility that an SIO might have been declared, and that the information proposed to be communicated related to that operation. Rather, the prosecution would need to prove, beyond reasonable doubt, that the person was aware of a real and not remote possibility that the information related not just to an intelligence or national security related operation of some general description, but specifically to an SIO.

---

19 See further, AGD response to questions on notice at a public hearing of the PJCIS, 15 August 2015 (18 August 2014), pp. 17-22.

As the Committee has observed, SIO authorisations are an entirely internal matter. This means that the burden on the prosecution to prove, to the criminal standard, that a person was advertent to a risk that a specific circumstance existed, and that that risk was significant, is an onerous one.

In addition to providing a person was aware of a substantial risk that the relevant circumstance existed, the prosecution must further prove that, having regard to the circumstances known to the person at the time of making the disclosure, it was unjustifiable to have taken that risk. The actions of a person in attempting to manage risk are directly relevant to an assessment of whether a person's actions were justifiable. For example, the actions of a journalist in attempting to check facts and consult with ASIO about any possible concerns in reporting on a matter would tend very strongly against a finding that such a person had acted unjustifiably in the circumstances. As such, adherence to the usual practices of responsible journalism in the reporting of operational matters relating to national security is directly relevant to the question of whether a communication was justified in the circumstances.

The policy justification for adopting recklessness, rather than knowledge, as the applicable fault element is – as noted above – that the wrongdoing targeted by proposed s 35P is that the disclosure of information about an SIO will, by its very nature, create a significant risk to the integrity of that operation and the safety of its participants. The fault element of recklessness gives expression to the policy imperative to deter such conduct by clearly placing an onus on persons contemplating making a public disclosure of such information to consider whether or not their actions would be capable of justification to the criminal standard. In the event that there is doubt, and the proposed disclosure relates to suspected wrongdoing by ASIO, consideration should be given to making an appropriate internal disclosure, such as to the Inspector-General of Intelligence and Security, or to the Australian Federal Police if the commission of a criminal offence is suspected.

(18) Disclosure offence – penalty, s 35P(1) (item 3)

Committee question (p. 31)

The committee notes that the breadth of application of the offence in subsection 35P(1), which applies to any person and is not limited to intended or actual consequences of the offence, means that the offence may be proved even though the conduct did not in fact compromise the integrity of operations or place at risk the safety of any participants in an SIO.

In light of this, the committee seeks a fuller justification from the Attorney-General as to why the penalty of imprisonment for 5 years is considered appropriate given that the breadth of application of the offence provision.

Attorney-General's response

A maximum penalty of five years' imprisonment is considered appropriate to reflect the wrongdoing inherent in the reckless disclosure of information relating to a special intelligence operation. As mentioned above, information about the existence and conduct of a special intelligence operation is inherently sensitive due to the necessarily covert nature of these operations. The disclosure of such information, by its very nature, places at risk the conduct of the operation to which it relates. This risk arises in respect of both the potential frustration of the effective conduct of an operation (and therefore the ability of ASIO to collect vital intelligence) and in potentially jeopardising the lives and safety of participants.

The proposed maximum penalty further reflects that the person disclosing the information was reckless as to the circumstance of its relationship with a special intelligence operation. That is to say, the person was aware of a substantial risk that the information was so related, but nonetheless, and unjustifiably in the circumstances, took the risk of making the disclosure. A person who was unaware of a substantial risk, or whose conduct is considered by a trier of fact to be justifiable would not be criminally responsible. It is a matter for a sentencing court to determine an appropriate penalty within the maximum, in accordance with general sentencing rules and having regard to the circumstances of individual cases. A person who, for example, disclosed information knowing that it related to a special intelligence operation would reasonably be expected to be subject to a higher penalty than a person who was aware of a substantial risk of this connection.

I further note that the proposed maximum penalty would maintain parity with the penalties applying to the secrecy offences in s 34ZS of the ASIO Act, concerning the unauthorised disclosure of information relating to ASIO's questioning and questioning and detention warrants. These offences, which were enacted in the *ASIO Legislation Amendment Act 2006* (Bill of 2006), similarly do not require proof of harm or intention to cause harm in the making of a disclosure, in recognition that such harm is implicit. This approach was found acceptable to the Parliament in 2006 and was not the subject of comment by this Committee as constituted at that time.[20]

I consider that an internally consistent penalty structure within the ASIO Act is necessary to adequately reflect the harm implicit in the disclosure of information about a covert intelligence activity, namely the creation of, at least, a risk that a sensitive operation may be compromised.

---

20 See Alert Digest No 4 of 2006 and Report No 3 of 2006. See also Alert Digest No 4 of 2003 and Report 12 of 2002, in which the Committee similarly did not comment on disclosure offences in s 34VA concerning the unauthorised communication of information by a subject's lawyer, which also carry a maximum penalty of five years' imprisonment.

(19) Evidentiary certificates, s 35R (item 3)

Committee question (p. 32)

While the committee appreciates the importance of ensuring that senior officers are able to spend their time efficiently, whether or not the proposed reversal of onus is appropriate depends significantly on the types of facts likely to be included in an evidentiary certificate. The committee therefore seeks the Attorney General's further advice as to the justification for this provision, including possible general examples of the content of these evidentiary certificates.

Attorney-General's response

The scheme of evidentiary certificates in proposed s 35R is necessary to ensure that sensitive operational details of decision-making in relation to SIOs are adequately protected in legal proceedings, and that such protection is applied in a way that is both procedurally fair and operationally efficient.

Proposed s 35R(1) is expressly limited to matters with respect to the granting of an SIO authority – namely, the authorising criteria in proposed s 35C. As such, certificates apply to the factual basis on which SIO authorisations are made. They could include such matters as:

- the particular special intelligence functions in respect of which the SIO will assist the Organisation, including details of how the SIO will do so;
- why the circumstances in a particular case are such as to justify the conduct of an SIO;
- what conduct is authorised or was sought to be authorised, including details of any otherwise unlawful conduct and how it is to be limited to the maximum extent consistent with an effective operation; and
- why any additional conditions or limitations are imposed.

Accordingly, a certificate issued under proposed s 35R could, in general terms, include details about a particular entity or activity of security concern, including why it is of security concern and why it is necessary to collect intelligence in relation to it, and why a special intelligence operation is needed, and details of the methodology of and participants in an SIO.

Importantly, proposed s 35R is limited to matters in respect of the authorisation of an SIO and not the intelligence collected in an SIO. As such these certificates would not include matters that could be used as prima facie evidence of the elements of an offence. 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 a respondent nonetheless had concern as to the breadth or scope of the facts covered by a certificate, because it appeared to include material facts that could address or prove the ultimate facts in the case, the prima facie nature of a certificate means it could be challenged in court and both parties given an opportunity to test its limits. If a certificate purported to cover such facts, it would be struck out to the extent it exceeded the permissible matters in proposed s 35R.

Minister for Finance
Acting Assistant Treasurer

Senator Helen Polley
Chair
Senate Scrutiny of Bills Committee
Suite 1.111
Parliament House
CANBERRA ACT 2600

Dear Senator

I refer to the letter of 28 August 2014 from the Secretary of the Standing Committee for the Scrutiny of Bills to the Assistant Treasurer's office concerning *Tax and Superannuation Laws Amendment (2014 Measures No.4) Bill 2014*.

The Committee has requested further advice about whether the retrospective application of the 'technical correction' to the 'permanent establishment' definition set out in Schedule 3 of the Bill will have a detrimental effect on any persons who have relied on the definition in its current form. In relation to this, please find attached my response to the Committee.

I trust that this information addresses the concerns raised by the Committee.

Kind regards

MATHIAS CORMANN

4 September 2014

Parliament House Canberra ACT 2600
Australia
Telephone: 02 6277 7360 Facsimile: 02 6273 4125

Tax and Superannuation Laws Amendment (2014 Measures No.4) Bill 2014

Schedule 3

Issue

The Committee seeks further advice from the Acting Assistant Treasurer given that it is unclear whether the retrospective application of the proposed amendment set out in Schedule 3 of the Bill to the 'permanent establishment' definition will have a detrimental effect on any persons who have relied on the definition in its current form.

Response

The amendment made by Schedule 3 is purely of a technical nature as the clear intention of Division 855 is to tax foreign residents on their Australian taxable property assets (either Australian real property assets or assets that are used in their Australian permanent establishment (branches)).

- The explanatory material that accompanied the introduction of Division 855 into the Parliament in 2006 makes this point clear by stating that "*the changes narrow the range of assets on which a foreign resident will be liable to Australian capital gains tax (CGT) to Australian real property and the business assets (other than Australian real property) of a* ***foreign resident's Australian permanent establishment***" [emphasis added].

In determining the assets **of permanent establishments located in Australia,** the table in section 855-15 of the *Income Tax Assessment Act 1997* includes as 'taxable Australian property':

- A CGT asset that you have used in carrying on a business through a **permanent establishment** (within the meaning of s23AH of the ITAA 1936) **in Australia.**

In relation to the technical amendment made by Schedule 3, the reference to the section 23 definition of permanent establishment in Division 855 (the foreign resident CGT regime) is a reference to a definition that only applies to outbound investments: that is, the permanent establishments of Australian residents operating overseas. A technical amendment is therefore required to Division 855 to ensure that it can correctly apply where assets are used in carrying on a business through a permanent establishment in Australia.

- The change replaces the reference to a permanent establishment within the meaning of section 23AH of the ITAA 1936 with specific tests. Consistent with section 23AH, these tests take into account an entity's status as a resident of a country with which Australia has an international tax agreement in determining whether it has a permanent establishment in Australia. Where there is no international agreement the general definition defined in subsection 6(1) of the ITAA 1936 is used.

The proposed amendment does not negatively affect any taxpayer because the scope of the definition of taxable Australian property will now align with the intention of the original provisions to only tax the Australian assets of foreign residents.

My Department undertook targeted consultation with several tax practitioners on this issue prior to its introduction into Parliament. Those contacted were supportive of the change applying retrospectively. Further, they advised Treasury that they were unaware that this technical issue existed as the measure was clearly intended to cover Australian assets only.