SENATE STANDING COMMITTEE

FOR THE

SCRUTINY OF BILLS

THIRD REPORT

OF

2016

2 March 2016

ISSN 0729-6258 (Print)

ISSN 2204-3985 (Online)

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 Joseph Ludwig	ALP, Queensland
Senator Rachel Siewert	AG, Western Australia

Secretariat

Ms Toni Dawes, 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

THIRD REPORT OF 2016

The committee presents its *Third Report of 2016* 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:

Aged Care Legislation Amendment (Increasing Consumer Choice) Bill 2016

Introduced into the House of Representatives on 11 February 2016
Portfolio: Health

Introduction

The committee dealt with this bill in *Alert Digest No. 2 of 2016*. The Minister responded to the committee's comments in a letter dated 29 February 2016. A copy of the letter is attached to this report.

Alert Digest No. 2 of 2016 - extract

Background

This bill amends the *Aged Care (Transitional Provisions) Act 1997* (the Transitional Provisions Act) to:

- enable funding for home care packages to 'follow' the care recipient;
- provide a consistent national process for prioritising access to subsidised home care; and
- simplify the approval process for approved providers.

The bill also amends the *Aged Care Act 1997* contingent on the commencement of the *Aged Care Amendment (Red Tape Reduction in Places Management) Act 2016*.

Merits review
Schedule 1, item 44, proposed subsection 23B-1(1)

Proposed subsection 23B-1(1) states that the Secretary may determine that a person is a prioritised home care recipient and the person's level of care as such a recipient. A person must be determined to be a prioritised home care recipient before an approved provider can be paid home care subsidy for providing home care to the person. The exercise of subsection 23B-1(1) in effect is necessary for the provision of subsidised care to a person.

As explained in the explanatory memorandum, a decision made under subsection 23B-1(1) is not subject to merits review. The justification provided is as follows:

> This [i.e. the absence of merits review] is appropriate in light of the factors the Secretary must take into account under the proposed subsection (4) when making a determination. In particular:

- in deciding whether a person is a prioritised home care recipient under section 23B-1, the Secretary must consider the priority for home care services assigned to the person under section 22-2A. Decisions relating to the priority for home care services made under section 22-2A are reviewable under section 85-1;
- the other key factor the Secretary must consider is the time a person has waited to receive subsidised home care. Merits review is not appropriate in this case, as waiting time is objectively determined and does not require the exercise of discretion by the Secretary; and
- the decision to prioritise a care recipient is a decision to allocate a finite resource (home care packages) between competing applicants (eligible care recipients) for which merits review is generally considered inappropriate. Given the limited number of home care packages available, the overturning of a decision not to prioritise an individual on merits review would naturally affect the rights of a person in respect of whom a determination has been made under Division 23B.

Subsection 23B-1(4) also provides that in addition to a consideration of the two matters outlined above, the Secretary may also consider any other matters specified in the Prioritised Home Care Recipients Principles. Subsection 23B-1(5) provides that the Secretary may also consider whether there are exceptional circumstances. Thus, determinations about whether to make a determination may involve a significant element of discretionary judgment.

Although the committee accepts that decisions allocating finite resources between competing applicants may be a basis for the exclusion of merits review, it need not be the case that in a large or moderately large program distributing benefits that a limited number of successful appeals would necessarily directly affect the rights of another person who has been awarded such a benefit. For example, some flexibility may be introduced into program funding estimates. **For this reason the committee seeks the Minister's more detailed explanation as to why merits review is impractical in the circumstances of the program and exercise of this particular power.**

The committee also seeks the Minister's advice as to whether any measures, such as alternatives to merits review, have been considered in relation to determinations made under subsection 23B-1(1). The committee is interested in measures to promote administrative accountability to ensure that processes for allocating funds are fair and to ensure the underlying policy applied to make the decisions is made clear. In this context, a requirement to give reasons and a reporting requirement are possible examples.

Pending the Minister's reply, the committee draws Senators' attention to the provisions, as they may be considered to make rights, liberties or obligations unduly dependent upon non-reviewable decisions, in breach of principle 1(a)(iii) of the committee's terms of reference.

Minister's response – extract

Schedule 1, item 44, proposed subsection 23B-l(l)

The Committee is seeking further information as to why merits review is impractical in the circumstances of the programme and in the exercise of this particular power.

Subject to passage of the Bill, new Part 2.3A of the *Aged Care Act 1997* (the Act) sets out the process for the prioritisation of home care recipients (consumers). The introduction of a consistent national system for prioritising access to subsidised home care will allow for a more equitable and flexible distribution of packages to consumers based on individual needs and circumstances.

This is important because the number of home care packages will continue to be capped or limited at each of the four package levels. In determining the number of consumers who can be prioritised for packages, the Secretary of the Department of Health will continue to work within the Government's policy parameters of the aged care planning ratio and the forward estimates. The Secretary does not have flexibility to adjust these parameters. At present, demand for packages substantially exceeds number of packages available, particularly for higher level packages.

The proposed subsection 23B-1(1) provides that the Secretary may, by written notice, determine that a person is a 'prioritised home care recipient' for the purposes of the programme. This is one of the criteria that must be satisfied in order for home care subsidy to be paid to an approved provider under section 46-1 of the Act for the provision of care to that person.

In making a determination under subsection 23B-1 (1), the Secretary must consider the factors set out in subsection 23B-1(4). These factors are: (a) the time that a person has been waiting for care; (b) a person's 'priority for home care services' determined under section 22-2A; and (c) any other matters specified in the Prioritised Home Care Recipient Principles.

The time that a person has been waiting for home care (from the date of the person's approval under Part 2.3 of the Act) is an objective criterion that does not allow discretion in decision-making by the Secretary and is therefore not suitable for merits review.

The determination of a person's priority for home care services under section 22-2A is a decision of the Secretary, based on information about a person's clinical and care needs (collected as part of the comprehensive assessment undertaken by an Aged Care Assessment Team). Decisions regarding a person's priority will be subject to merits review under Part 6.1 of the Act. In addition, the Act provides for written notice, including reasons for these decisions, to be provided to the consumer. The outcome of a decision under section 22-2A will directly impact on a decision made under subsection 23B-1(1).

It is not intended that any additional matters would be specified in the Prioritised Home Care Recipient Principles at this time. However, if any other matters are specified in the future, these would relate to objective factors because, as indicated in new section 23B-4, it is anticipated that the issuing of a notice under subsection 23B-1(1) will be an automatic process through the My Aged Care computer system.

Subsection 23B-1(5) allows the Secretary to consider any other exceptional circumstances in addition to the criteria set out in subsection (4). This provision would only be used in limited circumstances and to the benefit of consumers requiring priority access to care. The kinds of exceptional circumstances envisaged under subsection (5) include emergency care situations or instances of market failure (e.g. where individuals or groups of people are not able to access care in an appropriate and timely manner). Decisions would be made by the Secretary, or a delegate at the SES officer level within the Department.

Generally only individuals who are the subject of a decision can seek a review. It is therefore considered impractical for merits review because the individual will have been prioritised for a home care package.

The Committee is also seeking advice as to whether any measures, such as alternatives to merits review, have been considered in relation to determinations made under subsection 23B-1(1).

The legislation will provide transparency regarding the factors to be considered in the prioritisation process. To assist stakeholders to understand how decisions will be made, the prioritisation process, including review rights available to consumers under section 22-2A, will be clearly explained in public materials. Information resources will be developed specifically for consumers, carers, assessors and providers. The My Aged Care Gateway and advocacy services will also support consumers and carers. The prioritisation process will be closely monitored to ensure that the factors are applied correctly and consistently.

To further support accountability in the programme, the Department will make available information about expected waiting times, i.e. the time that a person would typically wait for a package after their approval by an Aged Care Assessment Team. The outcomes of the prioritisation process will be closely monitored to ensure that consumers, including people with special needs and those living in rural and regional areas, are able to access care in a fair and equitable manner. There will be regular public reporting on the operation of the prioritisation process and access to care though the programme.

Thank you for bringing these issues to my attention and I trust the information will address the concerns of the Committee.

Committee response

The committee thanks the Minister for this detailed response and requests that the key points be included in the explanatory memorandum, noting the importance of these documents as a point of access to understanding the law and, if needed, as extrinsic material to assist with interpretation e.g. section 15AB of the *Acts Interpretation Act 1901*.

The committee leaves the question of whether the proposed approach is appropriate to the consideration of the Senate as a whole.

Australian Crime Commission Amendment (National Policing Information) Bill 2015

Introduced into the House of Representatives on 3 December 2015
Portfolio: Justice

Introduction

The committee dealt with this bill in *Alert Digest No. 2 of 2016*. The Minister responded to the committee's comments in a letter dated 29 February 2016. A copy of the letter is attached to this report.

Alert Digest No. 1 of 2016 - extract

Background

This bill merges the functions of the CrimTrac Agency into the Australian Crime Commission (ACC) by amending the *Australian Crime Commission Act 2002* to enable the ACC to perform CrimTrac's functions, including providing national coordinated criminal history checks.

The bill also amends the *Crimes Act 1914*, the *Law Enforcement Integrity Commissioner Act 2006* and *Privacy Act 1988* to make consequential amendments.

Trespass on personal rights and liberties—privacy
Schedule 1, items 17 and 30

The purpose of this bill is to merge the CrimTrac Agency into the Australian Crime Commission (ACC). As a consequence the merged agency will be empowered to continue to carry out all of CrimTrac's functions. The explanatory materials note that it is necessary to modify the information disclosure regime in the ACC Act in two broad ways, seemingly with the intention to continue similar arrangements for the disclosure of national policing information that currently are in place for CrimTrac.

First, the ACC Act is to be amended so that the Board of the merged body has a role in the disclosure of 'national policing information' (which may include personal information). Secondly, a new disclosure regime will be inserted to enable the merged body (i.e. ACC) to disclose national criminal history check information to accredited bodies and individuals that are subject to the check.

Item 17 inserts new subsections 46A(5), (6), and (7) which confer on the ACC CEO the function of approving bodies that may access nationally coordinated criminal history checks through the ACC. As explained in the explanatory memorandum (at p. 20) these

'provisions are intended to enable the ACC Board to set limits or conditions on the types of bodies that can access a nationally coordinated criminal history check through the ACC, which the ACC CEO must comply with'. By this mechanism, the Board 'may control or limit the release of this specific type of national policing information, if it so wishes'.

Given that the accreditation means that particular bodies may apply for and receive what may be sensitive personal information, questions arise as to:

- whether it would be preferable for the legislation to contain more guidance in relation to the types of bodies that may access nationally coordinated criminal history checks (proposed subsection 46A(5) is very broad and provides that the CEO may approve a body of the Commonwealth, a State or a Territory or any other body or organisation however described, including bodies or organisations outside Australia); and
- whether the policy and directions issued by the ACC Board in relation to accreditation should be subject to Parliamentary oversight and disallowance.

The committee therefore seeks the Minister's further advice in relation to these issues.

Item 30 inserts a new section 59AAA to enable the merged agency to disclose nationally coordinated criminal history checks to accredited bodies and/or to the person to whom the check relates. Again, the intention is give the ACC Board control over disclosures. More particularly, the amendments will 'enable the ACC Board to set limits or conditions on the level of access an accredited body and/or an individual can have to nationally coordinated criminal history checks' (explanatory memorandum, p. 25). **The committee therefore seeks the Minister's advice as to whether guidance concerning the setting of such limits and conditions could be contained in the primary legislation and, if not, whether it is appropriate for the setting of such limits and controls to at least be subject to disallowance.**

> *Pending the Minister's advice, 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.*

Minister's response - extract

The Committee has sought additional information about Schedule 1, items 17 and 30 - proposed subsections 46A(5), (6) and (7) and section 59AAA- on the basis that they may unduly trespass on the right to privacy.

Specifically, the Committee has asked for further advice on:

1. whether the legislation should contain more guidance in relation to the types of bodies that may access nationally coordinated criminal history checks under subsections 46A(5), (6) and (7)
2. whether directions issued by the ACC Board in relation to accreditation under subsections 46A(5), (6) and (7) should be subject to Parliamentary oversight and disallowance, and
3. whether the legislation should contain guidance about the setting of limits and conditions for s5 9 AAA disclosures and, if not, whether the setting of such limits should be, at least, subject to disallowance.

For the reasons outlined in the Statement of Compatibility with Human Rights for the Bill and further detailed below, I am satisfied that the further measures suggested by the Committee are not necessary to protect the right to privacy.

Current arrangements for nationally coordinated criminal history checks

CrimTrac currently conducts nationally coordinated criminal history checks through the National Police Checking Service (NPCS). The NPCS provides accredited organisations with timely and accurate police history information, helping the organisation make informed decisions about potential employment of the individual subject to the check. Police history information may include charges, court convictions, good behaviour bonds or other court orders, matters awaiting court hearing, or traffic offences. The service enables controlled access to disclosable police history information from all Australian police agencies. A police check can be used for a number of purposes, including to screen employees applying for employment that involves working with children and vulnerable groups. Police agencies may also seek criminal history checks directly from CrimTrac for the purpose of the administration of justice, such as screening potential jurors. These checks do not require the subject's consent.

Except in the cases of checks for police for the administration of justice, CrimTrac can only disclose police checks to accredited organisations. The NPCS Terms of Service **(Attachment** A), which are available on the CrimTrac website, provide that an accredited organisation must not request a police check unless the individual subject to the check has provided inf01med consent. An accredited organisation is also required to provide the police history check result to the individual subject to the check. This gives the individual an opportunity to verify the check result and submit a dispute if necessary.

The CrimTrac CEO has the role of approving accredited organisations on the advice of the CrimTrac Board (comprised of the Police Commissioner from each state and territory, the Chief Police Officer of the·ACT, the AFP Commissioner and a nominated representative from the Commonwealth Attorney-General's Department). When an application to become an accredited agency is submitted, the CrimTrac CEO consults with state and territory police agencies.

Extensive guidance on the types of bodies that may be eligible to become accredited organisations is publically available on the CrimTrac website. It provides that an accredited organisation must:

- be an Australian registered business
- commit to submitting at least 500 nationally coordinated police checks over a three year period
- implement the required security management measures contained in the Information Technology- Security Management document (also publically available on the CrimTrac website).

CrimTrac currently has arrangements with in excess of 200 accredited organisations, which include Australian government agencies, private sector businesses, not-for-profit organisations and screening units for working with children or vulnerable people.

Arrangements following a merger

The Bill would amend the *Australian Crime Commission Act 2002* to merge the functions of CrimTrac into the Australian Crime Commission.

Item 17 of the Bill would insert new subsection 46A(5) to provide that the ACC CEO may approve a body of the Commonwealth, a state or territory, or any other body or body as an accredited body for the purposes of receiving nationally coordinated criminal history checks. Subsection 46A(6) provides that the ACC CEO must act in accordance with any policy or direction given by the ACC Board when deciding whether to approve a body or organisation under subsection 46A(5). Subsection 46A(7) provides that an instrument approving a body or organisation as an accredited body is not a legislative instrument.

These arrangements are designed to reflect the current CrimTrac arrangements.

Importantly, the provision of nationally coordinated criminal history checks will continue to occur on the basis that the individual to which the police information relates will have to consent to the provision of that information to an accredited agency. The current NPCS Terms of Service will continue to apply and the guidance available on the website will be transitioned to the website of the merged agency.

1. ***Should the legislation contain more guidance in relation to the types of bodies that may access nationally coordinated criminal history checks under subsections 46A(5), (6) and (7)?***

Information provided by a nationally coordinated criminal history check is collected from state and territory police. It is appropriate that the merged agency Board - which will include all current CrimTrac board members and six heads of Commonwealth agencies – maintains control of, and can limit the release of, the specific type of national policing information contained in nationally coordinated criminal history checks, by providing

guidance to the ACC CEO. The Board is very experienced in dealing with national policing information and has extensive knowledge about which bodies would or would not be suitable to access nationally coordinated criminal history checks under subsections 46A(5) and (6).

2 Should directions issued by the ACC Board in relation to accreditation under subsections 46A(5), (6) and (7) be subject to Parliamentary oversight and disallowance?

Given the large number of accredited agencies, Parliamentary oversight and disallowance of the Board's directions is likely to be onerous and would add uncertainty to the accreditation process.

Further, the ACC and its Board are already subject to a comprehensive oversight regime. The ACC Board reports to the Inter-Governmental Committee on the ACC, which comprises police ministers from all jurisdictions. The ACC is also subject to review and monitoring by the Parliamentary Joint Committee on Law Enforcement. These bodies have extensive expertise on the ACC, its functions, statutory regime and secrecy provisions, making them the most appropriate forums to monitor the ACC Board's directions about approving accredited bodies. Therefore, the Government does not consider that additional Parliamentary oversight of Board decisions is warranted.

3. Should the legislation contain guidance about the setting of limits and conditions for s59AAA disclosures and, if not, should the setting of such limits and conditions be, at least, subject to disallowance?

Item 30 would insert a new section 59AAA to enable the merged agency to disclose nationally coordinated criminal history checks to accredited bodies or to the person to whom the check relates, if:

a) disclosing the information would not be contrary to a Commonwealth, state or territory law that would otherwise apply, and

b) disclosing the information would not be contrary to any conditions or restrictions · determined by the Board in relation to providing nationally coordinated criminal history checks.

This provision is linked with new paragraph 7C(1)(gd), under which the Board may determine any conditions or restrictions that the merged agency must comply with in providing nationally coordinated criminal history checks. Together, the provisions are intended to enable the Board to play a role in limiting or restricting the disclosure of this specific type of national policing information, if it chooses to do so.

Information disclosed by a nationally coordinated criminal history check is currently sourced from state and territory police databases so it is appropriate that the Board, which includes all state and territory police representatives, has the power to issue a direction

about the disclosure of this information, if it wishes. This will maintain the Board's power to limit and restrict access to the specific type of national policing information.

The Government considers that the inclusion of detailed guidance about any limits and conditions in legislation would be unnecessary and inappropriate and would limit the Board's flexibility in dealing with national policing information.

Subjecting these limits and conditions to disallowance would be an unnecessary administrative burden that could delay the provision of nationally coordinated criminal history checks to accredited bodies and to individuals.

The Government considers that the ACC's existing and comprehensive oversight regime provides appropriate assurance that the ACC Board will issue reasonable and appropriate directions to the ACC CEO about the type of bodies that can receive nationally coordinated criminal history checks and the disclosure of this information.

I trust this information is of assistance to the Committee.

Committee response

The committee thanks the Minister for this detailed response and requests that the key points be included in the explanatory memorandum, noting the importance of these documents as a point of access to understanding the law and, if needed, as extrinsic material to assist with interpretation e.g. section 15AB of the *Acts Interpretation Act 1901*.

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

Counter-Terrorism Legislation Amendment Bill (No. 1) 2015

Introduced into the Senate on 12 November 2015
Portfolio: Attorney-General

Introduction

The committee dealt with this bill in *Alert Digest No. 13 of 2015*. The Attorney-General responded to the committee's comments in a letter dated 25 February 2016. A copy of the letter is attached to this report.

Alert Digest No. 13 of 2015 - extract

Background

The bill amends various legislation in relation to:

- receiving funds for legal assistance;
- extending control orders to children aged 14 or 15 years;
- control orders and tracking devices;
- issuing court for control orders;
- preventative detention orders;
- issuing authorities for preventative detention orders;
- application of amendments of the *Criminal Code*;
- monitoring of compliance with control orders;
- telecommunications interception;
- use of surveillance devices;
- a new offence of advocating genocide;
- security assessments;
- classification of publications;
- delayed notification search warrants;
- protecting national security information in control order proceedings;
- dealing with national security information in proceedings; and
- disclosures by taxation officers.

Trespass on personal rights and liberties—extension of control orders Schedule 2, general comment

Currently Division 104 of Part 5.3 of the *Criminal Code* specifies that control orders can only be made in relation to persons 16 years of age or older. Where control orders are imposed on persons aged 16 or 17 the maximum duration is three months, rather than the 12 month period applicable for adults.

This schedule will allow control orders to be imposed on a person who is 14 years of age or older. The Schedule provides that the maximum duration for children aged 14–17 is three months.

The schedule requires the issuing court to take into account the 'best interests' of the person when considering whether to impose each of the proposed obligations and requirements sought by the police in relation to children aged 14–17 years.

The Schedule also requires the issuing court to appoint an 'advocate' of the child in relation to any control order matter (proposed section 104.28AA). The court appointed advocate must be a lawyer. The advocate is given a number of functions:

- to ensure, as far as practicable, that the child understands the information provided in the proceedings;
- to form an independent view of what is in the best interests of the child;
- to act in what the advocate believes to be the best interests of the child and make submissions reflecting any course of action required by such a view;
- to ensure that the views expressed by the child are fully put before an issuing court; and
- to minimise any distress to the child associated with the control order matters.

The advocate is not the child's legal representative. The advocate is under no obligation to disclose to the court information the child communicates to him or her, but may do so if the advocate considers the disclosure to be in the best interests of the child (even if the child objects to such a disclosure of information).

The committee has previously noted that the control order regime established by Division 104 of Part 5.3 of the *Criminal Code* constitutes what is generally acknowledged to be a substantial departure from the traditional approach to restraining and detaining persons on the basis of a criminal conviction. That traditional approach involves a number of steps: investigation, arrest, charge, remand in custody or bail, and then sentence upon a conviction.

In contrast, control orders provide for restraint on personal liberty without there being any criminal conviction (or without even a charge being laid) on the basis of a court being satisfied on the balance of probabilities that the threshold requirements for the issue of the orders have been satisfied. Protections of individual liberty built into ordinary criminal

processes are necessarily compromised (at least, as a matter of degree). The extraordinary nature of the control order regime is recognised in the current legislation by the inclusion of a sunset period, due to expire on 7 September 2018 (section 104.32 of the *Criminal Code*).
In view of these general scrutiny concerns, any proposal to extend the operation of the control order regime to children aged 14 and 15 must also be subject to close scrutiny.

In this regard, the committee notes that questions in relation to the efficacy and appropriateness of the existing control order regime have been raised by the Independent National Security Legislation Monitor (INSLM) (see chapter II of second annual report, 20 December 2012, pp 6–44). For example, the INSLM noted that:

> The effectiveness, appropriateness and necessity of [control orders (COs)] is reduced by the ability of police to detect and prosecute at an early stage of offending. The UK CO regime (on which the Australian regime is modelled) was said to be necessary because of a lack of express terrorism offence provisions under UK criminal law at the time of introduction. This is now largely a historical problem for both the UK and Australia (INSLM, second annual report, p. 29).

In other words, the INSLM suggested that the appropriateness and necessity of control orders is reduced because it is now feasible a person may be charged with a terrorism offence comparatively early in the course of offending. That is, criminal responsibility arises in relation preparatory acts even where an offender has not decided precisely what he or she intends to do. In relation to this point, the INSLM noted that:

> Experience with Australia's terrorism offences shows that courts are prepared to hand down lengthy sentences of imprisonment to those convicted of preparatory terrorism offences even where "the enterprise was interrupted at a relatively early stage of its implementation" (INSLM, second annual report, p. 30).

In supporting a conclusion that the practical possibility of early prosecution for preparatory terrorism offences 'attenuates the policy justification…for the non-criminal power to make' control orders, the INSLM noted that:

> …the kind and cogency of evidence in support of an application for a CO converges very closely to the kind and cogency of evidence to justify the laying of charges so as to commence a prosecution. In particular, the availability, peculiar to terrorism, of precursor or inchoate offences earlier in the development of violent intentions and actions than ordinary conspiracy offences, renders this convergence practically complete (INSLM, second annual report, pp 30–31).

In addition, the committee notes that the INSLM has also raised questions in relation to the efficacy of control orders as a preventative mechanism (INSLM, second annual report, pp 37–38) and that the INSLM is currently inquiring into 'safeguards attaching to the control order regime'.

Noting the questions that have been raised in relation to the efficacy and appropriateness of the control order regime, the committee seeks the Attorney-

General's response to these concerns and, in particular, why it is not appropriate to wait for the INSLM to complete his current inquiry into control order safeguards before extending the regime to 14 and 15 year olds.

Pending the Attorney-General's reply, the committee draws Senators' attention to the schedule, 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

Schedule 2
Control orders for young people

Control orders play an important role in protecting the public from terrorist threats. They ensure that law enforcement has a legal basis on which to take action to prevent a terrorist threat from eventuating where an arrest or a prosecution is not open, but a person nonetheless presents a credible risk to public safety. In addition, these orders can be used as a less coercive tool than arrest and prosecution by facilitating the monitoring of individuals who pose a threat to the community through the imposition of certain controls on the person's behaviour.

Control orders can also be utilised in relation to individuals who continue to pose a threat to the public following charge, prosecution, conviction and release, to facilitate reintegration into society while also mitigating the risk that the person will engage again in risky behaviour (for example, associating with other people of security concern or accessing websites that advocate extremist views).

Control orders are not intended to replace investigations and prosecutions. They are a preventative mechanism which complements other law enforcement tools.

In 2012, the former INSLM recommended the control order regime be repealed and replaced with a new scheme of post-sentence orders. The Government, however, supports recommendation 26 of the COAG *Review of Counter-Terrorism Legislation*, which recommended the retention of control orders (with additional safeguards and protections). The proposed amendments to extend the regime to 14 to 15-year-olds include additional safeguards. These additional safeguards are being extended to 16 and 17-year-olds – who are already covered by the regime but without those additional safeguards. The Government will of course consider any further recommendations of the current INSLM concerning additional safeguards and protections to the regime to ensure it remains targeted and robust while not unnecessarily impacting on an individual's rights.

The former INSLM further noted in his 2012 report that the efficacy of a control order depends largely upon the subject's willingness to respect a court order, and that in the absence of the ability to effectively monitor a person's compliance with the terms of a control order, there is no guarantee that a person will not breach the order or go on to commit a terrorist offence.

This is a position shared by our law enforcement agencies. That is because existing Commonwealth coercive powers in relation to the conduct of physical searches, telecommunication interception and surveillance devices are only available for the purposes of investigating an offence that has already been committed or is about to be committed.

The proposed new monitoring powers seek to resolve this issue by adopting a threshold appropriate to the monitoring of a person in relation to whom a superior court has already decided the relevant threshold for issue of a control order has been met and who therefore, by definition, is of security concern. The new regimes will allow monitoring to mitigate the risk of breaches of control orders and, consequently, to mitigate the risk of the person engaging in preparatory acts, planning and terrorist acts.

As noted above, the PJCIS has completed its inquiry into the Bill, which included consideration of Part One of the INSLMS's report on control order safeguards. The Government is presently considering the reports of the INSLM and the PJCIS.

For additional information concerning the new monitoring powers which increase the efficacy of control orders, please see our response under that relevant heading below.

Committee response

The committee thanks the Attorney-General for this response. Pending the Government's response to recommendation 2 of the Parliamentary Joint Committee on Intelligence and Security (PJCIS) and the details of any alternative scheme, the committee is unable to finalise its comments on this matter at this stage.

In accordance with the committee's usual practice, the committee will consider (and, if appropriate, comment) on any amendments made to the bill by either House of the Parliament.

Alert Digest No. 13 of 2015 - extract

Trespass on personal rights and liberties—control orders: service of documents on a parent or guardian
Schedule 2, items 11, 13 and 14

These items insert notice requirements (requiring that a specified document be served) in relation to control order decisions made in relation to a child aged 14–17 years. The document must be served on the child's court appointed advocate and 'reasonable steps' must be taken to serve the document to at least one parent or guardian of the child. The explanatory memorandum characterises the service requirement on a parent or guardian as a 'slightly lower' requirement that 'reflects the fact that there will be instances where it is not possible to identify and/or locate a parent or guardian' (at p. 45).

While the committee notes this explanation, the committee seeks further information from the Attorney-General as to the options considered to deal with this potential problem with a view to ensuring that documents are served on a parent or guardian in all but the most exceptional circumstances. For example, the committee is interested whether consideration was given to including a provision in the bill that would have the effect of requiring that *all* reasonable steps are taken to notify a parent or guardian.

> *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

Service of documents on a parent or guardian (items 11, 13 and 14)

The requirement to take reasonable steps to serve the order on a young person's parent or guardian will ensure a parent or guardian is served whenever possible. Service on a parent or guardian will occur unless it is not reasonably possible to do so. There are a number of reasons the AFP may be unable to serve a parent or guardian. It may be that a parent or guardian cannot be located. It may also be that it would be inappropriate to serve a parent or guardian because, for example, the young person is estranged from the parent. Providing that the AFP 'must' serve the parent or guardian could potentially frustrate the process in circumstances where the AFP is unable to effect service or where service would actually

infringe on the young person's civil liberties and privacy, where they are estranged from the parent.

In considering how to formulate the obligation to serve the parent or guardian the Government adopted the term 'reasonable steps', a phrase that is commonly used in Australian laws and has been considered in case law, thus providing guidance to its interpretation.

The term bears its ordinary meaning, as being based upon or according to reason and capable of sound explanation. What is reasonable is a question of fact in each individual case. It is an objective test that has regard to how a reasonable person, who is properly informed, would be expected to act in the circumstances. What is reasonable can be influenced by current standards and practices. In a related context, the High Court has observed that whether there are 'reasonable grounds' to support a course of action 'requires the existence of facts which are sufficient to [persuade] a reasonable person';[1] it 'involves an evaluation of the known facts, circumstances and considerations which may bear rationally upon the issue in question'.[2]

It will be the responsibility of law enforcement to justify that reasonable steps were taken.

Amending the requirement to require that '*all* reasonable steps' are taken could be interpreted as requiring the AFP to take steps that another person contemplates, but that were not contemplated by the AFP at the time. In other words, it could bring an element of hindsight into the test, resulting in an AFP officer who acted in good faith and took reasonable steps to undertake service being found not to have taken a further step that another person identified after the fact.

Recommendation three of the PJCIS report considers the requirement to serve a parent or guardian. The Government is presently considering the PJCIS report.

Committee response

The committee thanks the Attorney-General for this response.

The committee notes the Attorney-General's comments in relation to the use of the term 'reasonable steps' in formulating the obligation to serve the parent or guardian with a control order issued for a young person. In particularly, the committee notes the view that a requirement to take *all* reasonable steps:

continued

1 *George v Rockett* {1990) 170 CLR 104 at 112 (Mason CJ, Brennan, Deane, Dawson, Toohey, Gaudron & McHugh JJ).

2 *McKinnon v Secretary, Department of Treasury* {2006) 228 CLR 423 at 430 (Gleeson CJ & Kirby J).

'could bring an element of hindsight into the test, resulting in an AFP officer who acted in good faith and took reasonable steps to undertake service being found not to have taken a further step that another person identified after the fact'.

The committee also notes that the Government is presently considering the PJCIS report into the bill, which includes a recommendation requiring the AFP to take reasonable steps, 'irrespective of whether the AFP member, having taken reasonable steps previously, has not been able to serve a copy of the interim control order personally on at least one parent or guardian of the young person.' (Recommendation 3)

The committee's view from a scrutiny perspective is that the issue of a control order for a young person is of such significance that it is appropriate to set the test for service at a level that includes a requirement to take 'all reasonable steps' so that, in taking such action, the AFP is required to think comprehensively about what might constitute the range of reasonable conduct. However, in the absence of a requirement to this effect, the committee supports the PJCIS suggestion to ensure that the obligation is continuing (contained in its recommendation 3). The committee draws this matter to the attention of Senators and leaves its consideration to the Senate as a whole.

In accordance with the committee's usual practice, the committee will consider (and, if appropriate, comment) on any amendments made to the bill by either House of the Parliament.

Alert Digest No. 13 of 2015 - extract

Trespass on personal rights and liberties—control orders: independence of court appointed advocate
Schedule 2, item 46, proposed subsection 104.28AA(1)

Under proposed subsection 104.28AA(1) the issuing court must make an order appointing a lawyer to be the court appointed advocate in relation to a child aged 14 to 17 years as soon as practicable after it has made an interim control order. Paragraph 104.28AA(1)(b) provides that the court may make other orders as appropriate to secure independent advocacy for the person in relation to the control order matter.

The independence of the court appointed advocate is considered to be an important safeguard in the application of the control order regime to children. However, the legislation is silent as to how that independence is to be achieved.

The explanatory memorandum does not explain what sort of orders may be made pursuant to paragraph 104.28AA(1)(b) nor how, in practical terms, independence is to be assured. The only requirement in the legislation is that the advocate be a lawyer, but the advocate once appointed is not the child's legal representative so it may be unclear what professional obligations, if any, are applicable in this context.

The committee therefore seeks the Attorney-General's advice as to:

- **how the independence of the court appointed advocate is to be secured in practice;**
- **more detail about the intended professional obligations applying to advocates; and**
- **the justification for not providing more guidance about the qualifications of advocates and mechanisms designed to ensure their independence in the legislation.**

> *Pending the Attorney-General's reply, the committee draws Senators' attention to this matter, 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.*

Trespass on personal rights and liberties—control orders: disclosure of information provided to a court appointed advocate
Schedule 2, item 46, proposed subsections 104.28AA(4)–(6)

Proposed subsection 104.28AA(4) provides that a court appointed advocate is under no obligation to disclose information given to them by the child. However, proposed subsections 104.28AA(5) and (6) provide that the advocate may disclose such information to the issuing court even if the disclosure is made against the wishes of the child. Disclosure can only be made 'if the advocate considers the disclosure to be in the best interests of the person' [i.e. the child]. However, in practice the advocate will have a large area of discretion in making this judgment.

The explanatory memorandum states that the lack of any obligation to disclose information that the child communicates to the advocate is 'designed to facilitate a relationship of trust and open communication' (at p. 55). Given this purpose, the discretion given to the advocate to disclose information may inhibit a relationship of trust developing. The explanatory memorandum suggests that authority to disclose information is required as it may be in the best interest of the child, for example because the child is in danger (p. 55).

However, it appears that this approach undermines what is otherwise intended to be a mechanism designed to protect the interests of children. The provision for an advocate to disclose information could even place children at a disadvantage relative to the provisions for adults. This is particularly the case given the proposed extension of the control order regime to younger children than is currently allowed. In an individual case it is possible that a relationship of trust could develop between the child and a court appointed advocate and that information divulged in that context is later disclosed even though the child

reasonably believes disclosure would not be in their best interests. Such a possibility does not arise in the application of the scheme to adults. Whether or not an advocate will be well placed to make accurate judgments about the child's best interest in relation to disclosure of information is likely to vary from case to case.

The committee therefore seeks a more detailed justification from the Attorney-General for the proposed approach, including specific examples of situations in which it is envisaged that a court appointed advocate would be likely to disclose information against the wishes of the child. The committee also seeks advice as to whether consideration has been given to including:

- **a requirement that clear advice be given to the child that information given to their advocate may be disclosed to the issuing court against their wishes; and**
- **a default requirement to at least consult with a parent, guardian and/or lawyer (if such a person is available) before information is disclosed against the wishes of the child unless exceptional circumstances exist.**

Pending the Attorney-General's reply, the committee draws Senators' attention to this matter, 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

Independence of court appointed advocate and disclosure of information provided to a court appointed advocate (item 46, proposed subsections 104.28AA(1) and (4) - (6))

The court appointed advocate model in the Bill seeks to achieve the following outcomes:

- ensure the controls imposed by the control order and the consequences of failing to comply with them is fully explained to the child by an independent person (noting that interim control orders are generally obtained on an ex parte basis, such that the young person would not likely have legal representation at the time of service). The AFP will continue to be required to provide this and other information to the child at the time of service
- ensure there is an independent person who can provide the court with an assessment about what is in the child's best interests, and
- ensure, particularly in circumstances where the child does not have separate legal representation, that there is a legally qualified person from whom the child can seek advice, and who can adduce evidence and make submissions for the child during proceedings.

The proposed section 104.28AA of the Criminal Code provides guidance on the role and qualifications of the advocate. Specifically, the independence of the advocate from the young person is achieved by the requirements in the bill to form an independent view, to act in and to make submissions in the best interests of the child, rather to act on the child's instructions (see subsections 104.28AA(2) and (3)). The independence of the advocate from the court is achieved by the advocate not being under an obligation to disclose information communicated by the young person unless doing so would be in the best interests of the child (see subsections 104.28AA(4) and (5)).

Further, the provision authorising the advocate to disclose information communicated by the young person is an important safeguard for the child. Although it is envisaged that the situations in which a court appointed advocate would disclose information to the court against the wishes of the child would be rare.

On 14 December 2015, the PJCIS requested the Attorney-General's Department to review the submissions made by bodies such as the Law Council of Australia and the Gilbert and Tobin Centre of Pubic Law and respond to the issues raised. On 15 January 2016 the Department provided the PJCIS with a supplementary submission which sought to address each of those sets of issues. A number of the submissions discuss the court appointed advocate model and the PJCIS asked the Department to consider whether an alternate model is feasible. The Department has advised the PJCIS that an alternate model may help address the concerns raised in those submissions as well as those raised at pages 9 and 10 in the Committee's Digest, although any alternate model would be subject to agreement by the States and Territories as per the International Agreement on Counter-Terrorism Laws.

Recommendation two of the PJCIS report considers the court appointed advocate model. The Government is presently considering the PJCIS report.

Committee response

The committee thanks the Attorney-General for this response.

The committee notes:

- the intended outcomes of the court appointed advocate model;
- the matters identified as going to the role and qualifications, and to securing the independence, of advocates;
- the view that the ability for an advocate to disclose information is intended as a safeguard for the young person; and
- the Attorney-General’s discussion of relevant matters discussed in submissions to the PJCIS, including consideration of alternative models and the PJCIS recommendation to remove the role of these advocates, but for there to be an express requirement that a young person has a right to legal representation (recommendation 2)

continued

Pending the Government's response to PJCIS recommendation 2 and the details of any alternative scheme, the committee is unable to finalise its comments on this matter at this stage.

However the committee notes that, from a scrutiny perspective, any proposed scheme should incorporate legislative requirements as to the qualifications and independence of any representatives, relevant notification requirements, and other safeguards to ensure that a young person is appropriately represented at every stage of a proceeding.

In accordance with the committee's usual practice, the committee will consider (and, if appropriate, comment) on any amendments made to the bill by either House of the Parliament.

Alert Digest No. 13 of 2015 - extract

Trespass on personal rights and liberties
Schedule 5

Schedule 5 contains amendments to the Preventative Detention Order (PDO) regime set out in Division 105 of the *Criminal Code*.

Proposed replacement subsection 105.4(5) introduces a new definition of 'imminent terrorist act'. Under current subsection 105.4(5), in order to obtain a PDO to prevent a terrorist act, a terrorist act must be one that is 'imminent' and must be one that is 'expected to occur, in any event, at some time in the next 14 days'. The new definition of 'imminent terrorist act' is a terrorist act that 'is capable of being carried out, and could occur, within the next 14 days'. The new approach focuses on the question of capability and possibility rather than requiring any expectation that an event will occur in within the specified timeframe. In this way, the circumstances which may enable a PDO to be made are expanded.

The explanatory memorandum states that this approach is justified on the basis of the evolving terrorist threat. It is stated that 'radicalisation occurs with increasing speed and terrorists may seek to commit terrorist acts quickly to evade the attention of law enforcement'. It is also noted that law enforcement 'may be aware that a person has the intention, motivation and necessary tools to commit a terrorist act', but lacks evidence about the issue of timing. Further, the explanation suggests that the planned timing of an attack may be changed in response to surveillance being detected (see p. 61).

Although the explanatory memorandum thus justifies the expansion of circumstances in which a PDO may be sought, it may be noted that a significant change is being made to the basis for preventative detention: from an expectation that an attack will occur to a conclusion about the capability for an attack to be carried out.

The statement of compatibility rejects the notion that this change diminishes the right to freedom from arbitrary detention and arrest. The argument for this conclusion (at p. 22) is that:

> The right to freedom from arbitrary detention is safeguarded by the existing provisions in the PDO regime. These provisions continue to operate in conjunction with the amendments contained in Schedule 5. In particular, the basis for applying for a PDO and the proportionality requirements contained in subsection 105.4(4) mitigates the inappropriate imposition of a PDO. The application for a PDO requires that an AFP member must suspect on reasonable grounds that the suspect will engage in a terrorist act, possess a thing that is connected with the preparation for, or the engagement of a person in, a terrorist act or has done an act in preparation for, or planning, a terrorist act (subparagraphs 105.4(4)(a)(i)-(iii)). The issuing authority must similarly be satisfied that there are "reasonable grounds to suspect" the same matters (subparagraphs 105.4(4)(b)(i)-(iii)).
>
> Having satisfied this threshold, the AFP member and issuing authority must also satisfy the proportionality tests contained in paragraphs 105.4(4)(c) and 105.4(4)(d). That is, they must demonstrate that a PDO will "substantially assist" in preventing an imminent terrorist act occurring (paragraph 105.4(4)(c)) and that detention for the period specified is "reasonably necessary" for the purpose of preventing the imminent terrorist act (paragraph 105.4(4)(d)). This highlights the clearly preventative nature of the PDO power and creates a high threshold for its imposition. The combined operation of these criteria require that law enforcement agencies must make out a case for why the limitations imposed by the PDO are justified in each circumstance.

Although it may be accepted that existing elements of the PDO regime will continue to apply, and the committee notes the justification in the explanatory memorandum, the focus on the capability to mount a terrorist attack constitutes a broadening of the power to limit a person's liberty. **In this context the committee therefore:**

- **seeks the Attorney-General's more detailed explanation as to why the power to issue a PDO should be broadened in this way; and**
- **requests the Attorney-General's advice as to any alternative powers at the disposal of law enforcement to respond to knowledge that a person has the necessary tools to commit a terrorist act in circumstances where no evidence is available about when an attack may occur.**

Pending the Attorney-General's reply, the committee draws Senators' attention to the schedule, 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

Schedule 5
Preventative detention orders

Currently, the issuing authority must be satisfied there are reasonable grounds to suspect that a terrorist act is imminent and is expected to occur, in any event, at some time in the next 14 days. The problem with this test is that even where police have grounds to suspect a person has the capacity to carry out a terrorist act at any time, neither the AFP nor the issuing authority may have information as to the time that has been selected to carry out that act – if indeed a time has been selected. For example, if a terrorist is prepared and waiting for a signal or instruction to carry out their act, the AFP may not be able to identify when that signal or instruction will be sent. Indeed the terrorist themselves may not know. Under the existing test, the AFP may not be able to seek a preventative detention order without information as to the expected timing. Accordingly, there is an operational gap in ability to deal with terrorist acts that are not planned to occur on a particular date, even where the preparations for that terrorist act may be in their final stages, or complete.

As the AFP noted in their submission to the PJCIS, if the point in time that an incident will take place is not known, the issuing authority may not be satisfied the act is expected to occur sometime in the next 14 days. The proposed amendment addresses this issue by placing the emphasis on the capacity for an act to be carried out in the next 14 days. If a terrorist act is capable of being carried out, and could occur, within 14 days, that terrorist act will meet the definition of an 'imminent terrorist act'. Accordingly, the proposed amendment ensures the AFP has the ability to apply for a PDO to safeguard the public against such risks where they are identified. The inclusion of a 14-day timeframe in which the act could occur retains the imminence requirement, but focusses on the capability of a person to commit a terrorist act, as opposed to the specific time in which the terrorist act is expected to occur.

The issuing authority must be satisfied that making the preventative detention order would substantially assist in preventing an imminent terrorist act occurring, and that detaining the person is reasonably necessary for the purpose of preventing a terrorist act. Accordingly, the power is only available when detention of the person is required. The AFP can arrest and detain a person for the purpose of investigating a terrorism offence under Part 1C of the *Crimes Act 1914* (Cth). However, there will be situations when arrest is not a viable

option, but a person nonetheless presents a credible risk to public safety in relation to an imminent terrorist act.

Recommendation fifteen of the PJCIS report considers the threshold for obtaining a PDO. The Government is presently considering the PJCIS report.

Committee response

The committee thanks the Attorney-General for this response and notes the further information provided about the justification for the proposed approach. The committee requests that the additional points be included in the explanatory memorandum, **noting the importance of these documents as a point of access to understanding the law and, if needed, as extrinsic material to assist with interpretation (e.g. section 15AB of the *Acts Interpretation Act 1901*).**

The committee leaves the question of whether the proposed approach is appropriate to the Senate as a whole.

Alert Digest No. 13 of 2015 - extract

Trespass on personal rights and liberties—new 'monitoring warrant' regime Schedule 8, general comment and proposed sections 3ZZKF and 3ZZLC

Schedule 8 seeks to create a 'monitoring warrant' regime in a new Part IAAB of the *Crimes Act 1914* to confer powers on law enforcement agencies to monitor compliance with control orders. Unlike the existing search warrant regime, the new regime will not require the issuing authority to be satisfied that an offence has already occurred or is going to be committed. Rather, this regime will be targeted at monitoring compliance with the conditions of a control order for the purpose of preventing a person from engaging in terrorist act planning or preparatory acts.

The powers conferred by this schedule relate to:

- entering premises by consent or under a warrant (proposed section 3ZZKA);
- general monitoring powers in relation to premises, including the power to search premises and any thing on the premises, the power to search for and record fingerprints, the power to make any still or moving image or any recording of the premises or any thing on the premises, and the power to take extracts from, or make copies of, documents (proposed section 3ZZKB);

- operating and securing electronic equipment (proposed sections 3ZZKC and 3ZZKD);
- asking questions and seeking production of documents (proposed section 3ZZKE);
- seizing things found during the exercise of monitoring powers on a premises (proposed section 3ZZKF);
- the availability of assistance and use of force in executing a warrant (proposed sections 3ZZKG and 3ZZLD);
- searching a person by consent or under a warrant (proposed section 3ZZLA);
- monitoring powers in relation to persons, including the power to search things found in the possession of person, the power to search any recently used conveyance, and the power to record fingerprints and take samples from things (proposed section 3ZZLB); and
- seizing things located during the search of a person or a recently used conveyance (proposed section 3ZZLC).

The committee consistently expects that the expansion of circumstances in which coercive and intrusive powers can be utilised should be comprehensively justified.

As an example, proposed sections 3ZZKF and 3ZZLC will provide automatic authority to a constable to seize evidential material located during a search authorised under a monitoring warrant.

However, in its general consideration of monitoring warrant schemes, the *Guide to Framing Commonwealth Offences, Infringement Notices and Enforcement Powers* (the Guide) indicates (at p. 87) that these schemes typically confer power on an authorised officer to only secure evidence pending an application for a search/seizure warrant where he or she 'has reasonable grounds to believe that evidence of an offence would be lost, destroyed or tampered with by the time a search warrant is obtained' (p. 88). This is the approach taken in Part IAA of the Crimes Act.

In this respect the powers conferred by the monitoring powers in the bill appear to be in potential conflict with the Guide. The explanatory memorandum merely repeats the effect of the provision, without providing a justification for the proposed approach. **The committee therefore seeks the Attorney-General's justification for the approach taken and seeks advice as to whether the principles in the Guide have been considered.**

The committee also seeks advice as to whether each of the monitoring powers under the proposed 'monitoring warrant' regime established by this schedule are consistent with the principles in the Guide and the approach taken in Part IAA of the *Crimes Act 1914* (and if they are not, the rationale for taking an alternative approach in this instance).

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

Schedule 8
New 'monitoring warrant' regime

The power to seize evidentiary material pursuant to the new monitoring warrant regime is largely consistent with the *Guide to Framing Commonwealth Offences, Infringement Notices and Enforcement Powers* (the Guide). However, where minor differences exist between the provisions in the new monitoring warrant regime and existing precedents, the Government considers there is solid operational and policy justification.

The Guide refers to monitoring warrants precedents, including subsection 90-4(2) of the *Aged Care Act 1997*, which states that where an authorised officer is exercising monitoring powers and has reasonable grounds to believe that a thing that may afford evidence of the commission of an offence would be lost, destroyed or tampered with by the time a search warrant is obtained, they have the power to secure the evidence pending an application for a search and seizure warrant. However, the Act also allows the authorised officer to apply for a warrant to seize things in certain circumstances, including where possession of the thing could constitute an offence (section 92-3 of the *Aged Care Act* 1997).

Similarly, the proposed monitoring warrant regime for control orders allows for things to be secured in certain circumstances and seized in others. The regime allows a constable to secure electronic equipment in order to obtain expert assistance in operating the equipment. However, where a constable searches premises pursuant to a monitoring warrant they have the power to seize certain items including things relevant to an offence and seizable items. A seizable item is one that could be used to self-harm or to harm others.

The established principles for traditional monitoring warrants are appropriate for regimes that simply monitor compliance with legislative requirements in circumstances where the possibility or likelihood of the occupant engaging in harmful or even deadly conduct against others is remote. However, that may not necessarily be the case where the monitoring warrant relates to a person who on reasonable grounds the court suspects has engaged in conduct which is of security concern, such as participated in training with a terrorist organisation. Accordingly, the proposed monitoring warrant regime only authorises an issuing authority to authorise a warrant to monitor compliance with a control order if satisfied that the purpose of a search, pursuant to the warrant, is protecting the public from a terrorist act; preventing the provision of support for, or the facilitation of, a

terrorist act; preventing the provision of support for, or the facilitation of, the engagement in a hostile activity in a foreign country; **or** determining whether the control order has been, or is being, complied with. This threshold is different from other monitoring warrant regimes.

Furthermore, the issuing authority will take into consideration the things that are sought to be authorised pursuant to the warrant, which includes seizure of evidentiary material, when deciding whether to issue the warrant.

These targeted powers underline the important protective value of imposing a control order on a person who has already been identified as being of security concern, noting that terrorist acts can come to fruition very quickly. In addition, where police identify evidential material and seizable items, it is not only appropriate, but vital, that they are able to take action as quickly as possible with respect to those items to protect the Australian community. Unlike some monitoring warrant precedents that only allow for evidence to be 'secured' pending an application for a search and seizure warrant law enforcement, this would be inadequate to deal with the security risk in this proposed regime. If there is a delay in which the evidence can be used, caused by a requirement to get a second warrant, this could have significant adverse outcomes.

The regime provides a number of safeguards and accountability mechanisms to protect rights against arbitrary and unlawful interferences with privacy. The Attorney-General's Department is currently finalising a Privacy Impact Statement that will explore those issues fully.

In these circumstances it is appropriate to allow certain items to be seized rather than secured pending a further warrant.

Recommendations nine, ten and eleven of the PJCIS report also consider a number of aspects of the proposed monitoring warrant regime, including additional safeguards and accountability mechanisms. The Department is presently considering the PJCIS report.

Committee response

The committee thanks the Attorney-General for this response and notes the further information provided about the justification for the proposed approach.

In particular, the committee notes the justification for including the power to seize items in certain circumstances as well as to secure them; and the reference to ‘safeguards and accountability mechanisms’ and PJCIS recommendations 9, 10 and 11.

continued

The committee is interested in work the Attorney-General outlines that will 'explore those issues fully' and supports the inclusion of the measures outlined in PJCIS recommendations 9, 10 and 11 (going to 'least interference', the availability of the privilege against self-incrimination and legal professional privilege, notification to the Commonwealth Ombudsman, reporting and the retention of relevant information).

The committee requests that the additional points be included in the explanatory memorandum, noting the importance of these documents as a point of access to understanding the law and, if needed, as extrinsic material to assist with interpretation (e.g. section 15AB of the *Acts Interpretation Act 1901*).

The committee leaves the question of whether the proposed approach is appropriate to the Senate as a whole.

Alert Digest No. 13 of 2015 - extract

Trespass on personal rights and liberties—use of things seized, information obtained or a document produced where an interim control order is subsequently declared void
Schedule 8, item 1, proposed section 3ZZTC of the *Crimes Act 1914*
Schedule 9, item 53, proposed section 299 of the *Telecommunications (Interception and Access) Act 1979*
Schedule 10, item 39, proposed section 65B of the *Surveillance Devices Act 2004*

Proposed section 3ZZTC of the *Crimes Act 1914* (as outlined in item 1 of schedule 8), specifies certain purposes for which things seized, information obtained or a document produced pursuant to a monitoring warrant can be communicated or adduced as evidence where a court has subsequently declared the interim control order to be void. The explanatory memorandum (at p. 81) describes the effect of the provision, but does not expand on its rationale or circumstances in which it might apply.

The same issue arises in relation to information obtained under the provisions of *Telecommunications (Interception and Access) Act 1979* (see Schedule 9, item 53, proposed section 299) and to information obtained under the provisions of the *Surveillance Devices Act 2004* (see Schedule 10, item 39, proposed section 65B) where the control order is subsequently declared to be void.

The statement of compatibility (at p. 34) justifies the approach in these proposed provisions as follows:

> The amendments [allow] lawfully intercepted information to be dealt with in relation to state and territory PDOs, and allow lawfully intercepted information obtained under a warrant relating to a control order that is declared void to be used, communicated, recorded or given in evidence in a proceeding when it is necessary to assist in preventing or reducing the risk of the commission of a terrorist act, serious harm to a person, serious damage to property or a purpose connected with a Commonwealth, state or territory PDO regime. This will assist national security and law enforcement agencies to identify terrorism risks early, investigate potential terrorist threats, and thereby prevent an act of terrorism from occurring. Similarly, it will enable agencies to act to prevent individuals from involvement in hostile activity overseas.

The use of information obtained in these circumstances may have serious implications for personal rights and liberties. **As such, the committee seeks the Attorney-General's advice as to whether similar provisions appear in other Commonwealth legislation and requests a more detailed justification for the use of material obtained in circumstances in which the relevant control order has been declared void.**

> *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

Schedules 8, 9 and 10
Monitoring of compliance with control orders etc, Telecommunications interception, and surveillance devices (item 1, proposed section 3ZZTC of the *Crimes Act 1914*, item 53, proposed section 299 of the *Telecommunications (Interception and Access) Act 1979*, and item 39, proposed section 658 of the *Surveillance Devices Act 2004)*

The provisions, inserted into the *Crimes Act 1914* (the Crimes Act), *Surveillance Devices Act 2004* (the SD Act) and *Telecommunications (Interception and Access) Act 1979* (the TIA Act) are intended to address the unlikely scenario where:

- an interim control order has been issued in respect of a person;
- a law enforcement agency has duly obtained a monitoring warrant in relation to that person;

- under that monitoring warrant, the agency has obtained information that indicates that the person is likely to engage in a terrorist act, cause serious harm to a person, or cause serious damage to property;
- before the agency can act on that information, the interim control order is considered by a court at a confirmation hearing and declared void *ab initio* pursuant to subsection 104.14(6) of the Criminal Code on the grounds that, at the time of making the interim control order, there were no grounds on which to make the order.

As the existence of a valid control order is a condition for the issuing of a monitoring warrant, the likely effect of a court declaring an interim control order void *ab initio* pursuant to subsection 104.14(6) of the Criminal Code would be that any monitoring warrants predicated on that control order would also likely be void *ab initio.*

It is a fundamental principle of the Australian legal system that courts have a discretion as to whether or not information may be admitted as evidence into proceedings, irrespective of the manner in which the information was obtained. As an example, the *Bunning v Cross*[3] discretion places the onus on the accused to prove misconduct in obtaining certain evidence and to justify the exclusion of the evidence. This provision is expanded on in Commonwealth statute[4], where there is an onus on the party seeking admission of certain evidence to satisfy the court that the desirability of admitting the evidence outweighs the undesirability of admitting it, given the manner in which it was obtained. This fundamental principle reflects the need to balance the public interest in the full availability of relevant information in the administration of justice against competing public interests, and demonstrates the role the court plays in determining admissibility of evidence.

However, the SD Act and TIA Act depart from these fundamental principles, by imposing strict prohibitions on when material under those Acts may be used, communicated or admitted into evidence.[5] Under these Acts, it is a criminal offence for a person to deal in information obtained under these Acts for any purpose, unless the dealing is expressly permitted under one or more of the enumerated and exhaustive exceptions to the general prohibition. These provisions expressly override the discretion of the judiciary, both at common law and under the *Evidence Act 1995,* to admit information into evidence where the public interest in admitting the evidence outweighs the undesirability of admitting it, given the manner in which it was obtained. There is also a risk that these specific provisions might be interpreted, either by a court considering the matter after-the-fact, or by an agency considering the question *in extremis,* to override the general defence to criminal responsibility under the Criminal Code.

For this reason, the Bill would insert new section 658 to the SD Act and section 299 to the TIA Act, which would expressly permit agencies to rely on such information to prevent, or lessen the risk, of a terrorist act, serious harm to a person, or serious damage to property.

---

3 (1978) 141 CLR 54.
4 Section 138 of the *Evidence Act 1995* (Cth).
5 See section 63 of the TIA Act and 45 of the SD Act.

These provisions would also permit such information to be used to apply for, and in connection with, a preventative detention order.

The Crimes Act does not contain restrictions on dealing in information obtained under a search warrant equivalent to those contained in the SD Act and TIA Act. As such, the circumstances in which proposed new section 3ZZTC of the Crimes Act would be likely to modify the operation of the existing law are likely narrower than the circumstances in which proposed new section 658 of the SD Act and section 299 of the TIA Act would apply. Nevertheless, as the three monitoring warrant regimes, under the Crimes, SD and TIA Acts are intended to operate in parallel with one another, the Government proposes to include proposed new section 3ZZTC of the Crimes Act, so as to avoid any inference being drawn that the absence of such a provision might reflect Parliament's intent that information obtained under that Act be subject to more stringent controls than information obtained under the SD and TIA Acts.

Recommendations nine to thirteen of the PJCIS report consider a number of aspects of the proposed monitoring warrant regime, including additional safeguards and accountability mechanisms. The Department is presently considering the PJCIS report.

Committee response

The committee thanks the Attorney-General for this response. The committee notes the additional information provided outlining the justification for expressly permitting agencies 'to rely on [SD and TIA] information to prevent, or lessen the risk, of a terrorist act, serious harm to a person, or serious damage to property. These provisions would also permit such information to be used to apply for, and in connection with, a preventative detention order.'

While the committee notes the additional material provided, it seems to deal with the use of such material generally, rather than specifically addressing how it is appropriate in circumstances in which the relevant control order has been found to be void.

The committee also notes the reference to PJCIS recommendations 9 to 13, which include 'additional safeguards and accountability mechanisms' presently being considered by the government.

Pending the Government's response to these PJCIS recommendations the committee is unable to finalise its comments on this matter at this stage. **However, the committee notes that it would expect a comprehensive justification for allowing the use of SD and TIA material obtained in circumstances in which the relevant control order has been found to be void to be included in any further explanatory material relating to the bill. The committee would also be interested in the detail of legislative safeguards and accountability mechanisms.**

continued

In accordance with the committee's usual practice, the committee will consider (and, if appropriate, comment) on any amendments made to the bill by either House of the Parliament.

Alert Digest No. 13 of 2015 - extract

Trespass on personal rights and liberties—authorisation of intrusive powers Schedules 9, 10 and 14, general comment

As noted above, schedules 9 and 10 seek to extend telecommunications interception warrants and surveillance device warrants to the control order regime. The statement of compatibility (at p. 28) states that:

> Judicial oversight prior to the use of a privacy-intrusive surveillance device requires law enforcement agencies to demonstrate the necessity and proportionality of surveillance to an independent party. This is an important safeguard.

The committee agrees that judicial oversight of intrusive powers is an important safeguard in ensuring that these powers are appropriately utilised. In this regard, the committee's consistent preference is that the power to issue warrants authorising coercive or intrusive powers should only be conferred upon judicial officers (rather than non-judicial officers such as members of the AAT). The committee notes that current provisions allow 'nominated AAT members' to issue warrants under the *Telecommunications (Interception and Access) Act* 1979 and the *Surveillance Devices Act 2004*.

This issue also applies to schedule 14, which seeks to clarify the threshold requirements for the issue of a delayed notification search warrant ('eligible issuing officers' for the purposes of issuing delayed notification warrants are a judge of the Federal Court of Australia or of a state or territory Supreme Court or a nominated AAT member).

The committee generally does not regard factors such as 'administrative convenience' as being sufficient justification for conferring such power on non-judicial officers.

Noting the legal complexity of the relevant provisions, and given that this bill seeks to extend the circumstances in which telecommunications interception warrants and surveillance device warrants can be issued (schedules 9 and 10) and change the threshold requirements for the issue of a delayed notification search warrant (schedule 14), the committee seeks the Attorney-General's advice as to why the

categories of eligible issuing officers should not limited to persons who hold judicial office.

Pending the Attorney-General's reply, the committee draws Senators' attention to these matters, 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

Schedules 9, 10 and 14
Authorisation of intrusive powers

AAT members have extensive experience exercising personal functions under a broad range of legislative schemes. The role proposed for authorised members in the Bill is consistent with existing functions able to be undertaken by AAT members. As outlined below, there are legislative, ministerial and governance processes in place that support the appropriateness and value of AAT members being authorised to perform these roles.

AAT members as issuing officers in similar contexts

Enabling members to be nominated as issuing officers under the Bill is supported by a longstanding practice of allowing members, along with judicial officers, to undertake sensitive personal functions. AAT members have been eligible for nomination to issue interception and stored communications warrants under the *Telecommunications (Interception and Access) Act 1979* since 1997, and surveillance device warrants under the *Surveillance Devices Act 2004* since 2004. More recent reforms have expanded the range of sensitive functions able to be exercised by members who are issuing officers:

- in 2001, to extend the length of controlled operations beyond three months under the *Crimes Act 1914*
- in 2005, to make continued preventative detention orders under the *Criminal Code Act 1995*
- in 2007, to make orders allowing information given to the Inspector of Transport Security to be disclosed to another government agency under the *Inspector of Transport Security Act 2006,* and
- in 2012, to issue search warrants and exercise powers under the *Tobacco Plain Packaging Act 2011* and to issue examination notices under the *Fair Work (Building Industry) Act 2012.*

The nature and complexity of the functions proposed for issuing officers under the Bill is analogous to the roles already undertaken by authorised members and does not represent a departure from the approach taken in other recent legislation.

Qualification and eligibility requirements for AAT members

The legislation enabling the authorisation of members, including for the functions provided under schedules 9, 10 and 14 of the Bill, incorporate specific qualification and eligibility requirements for AAT members.

Deputy Presidents and senior members are eligible to be nominated under the Telecommunications (Interception and Access) Act and the Surveillance Devices Act.[6] Part-time senior members and members must be legal practitioners and have been enrolled for more than 5 years to be eligible for nomination under these Acts. Schedules 9, 10 and 14 preserve these eligibly requirements and qualification thresholds.

Ministerial authorisation provides an additional safeguard for the exercise of personal functions undertaken by members. Members meeting eligibility criteria and who consent to perform a function are individually considered for authorisation by the responsible minister. The role for the Attorney-General to authorise members under the Telecommunications (Interception and Access) Act and the Surveillance Devices Act is coupled with the power to revoke the authorisation of a member.[7] The department is not aware of any instance where the authorisation of an AAT member has been revoked by an Attorney-General.

Reporting and governance support provided within the AAT

A broad range of governance and support arrangements are provided by the AAT to assist members who are authorised and to support the transparency of their personal functions. For example, the AAT convenes a Warrants Committee, which is chaired by a Deputy President. The Warrants Committee provides training and support to authorised members on matters such as:

- the circumstances in which an application for a warrant might ordinarily be refused, or be granted subject to the provision of further information
- the circumstances in which an application for a warrant might ordinarily be granted subject to conditions, including the factors commonly considered when determining conditions, and
- where appropriate, organising professional development activities and distributing information to authorised members.

The Warrants Committee provides advice to the President of the AAT on the exercise of authorised member functions, including in relation to the collection of data and liaison about warrants related matters with the Attorney-General's Department.

---

6 Section 6DB *Telecommunications (Interception and Access) Act 1979* and section 13 *Surveillance Devices Act 2004.*

7 Section 6DB *Telecommunications (Interception and Access) Act 1979* and section 13 *Surveillance Devices Act 2004.*

The AAT also makes a broad range of training resources available to authorised members, such as practice manuals prepared by the AAT and the CDPP, guidelines to the operation of legislative schemes, information circulars about reforms in other jurisdictions, hosting guest speakers and enabling one-on-one training for newly authorised members with more experienced authorised members.

Information about the exercise of personal functions by authorised AAT members is recorded in the AAT's case management system and application related statistics are publicly reported in the AAT's Annual Report.

Promoting accessibility and access for law enforcement agencies

The inclusion of AAT members as eligible issuing officers provides law enforcement agencies with a larger pool of decision makers across most states and territories. The Telecommunications (Interception and Access) Act Annual Reports for 2012-13, 2013-14 and 2014-15 illustrate the significant volume of work undertaken by issuing officer members under that Act alone:

	Authorised members	**Warrants applications considered and issued under the telecommunication (Interception and Access) Act**
2012-13	37	3,330
2013-14	29	3,212
2014-15	29	3,223

Functions that are undertaken by judicial officers and AAT members in their personal capacity are subject to the consent of the issuing officer at the time an application is being made.

Reported statistics demonstrate that AAT members hear a large number of warrants applications. By comparison over the same period, fewer warrants were issued by authorised federal judicial officers under the Telecommunications (Interception and Access) Act, for example:

	Warrants applications considered and issued under the Telecommunications (Interception and Access) Act
2012-13	896
2013-14	795
2014-15	703

AAT members also regularly make themselves available to consider applications outside of business hours, enabling urgently arising applications to be considered. The AAT

reports that in 2014-15, 162 applications were made to members outside of business hours.[8]

There is no empirical material to suggest that members do not exercise their personal functions as issuing officers professionally and diligently. Data collected during 2012-13 by the AAT (set out below) indicates that in a number of cases where warrants have been issued, members have required further information or amendments to applications prior to issuing a warrant.

Warrant applications, 2012-2013	
Total issued	**4451**
Issued – as requested	4008
Issued – after further information provided	237
Issued – with conditions	147
Issued – for less time than sought	104
Issued – with revised privacy declaration	16
Refused	**55**

Constitutional impediments

Moreover, as the Committee is aware, strict constitutional requirements limit the functions members of the judiciary may exercise in a personal capacity. In *Grollo v Palmer* (1995) 184 CLR 348, the High Court held that the Parliament or executive cannot confer on a judge of a federal court a non-judicial function that is not incidental to a judicial function unless:

(a) the judge consents to the performance of the function, and

(b) the exercise of the function is not incompatible either with the judge's performance of his or her judicial functions or with the proper discharge by the judiciary of its responsibilities as an institution exercising judicial power.[9]

From an historical perspective, these constitutional limitations contributed to the basis for enabling AAT members to be issuing authorities. Following that decision of the High Court, a significant number of judges of the Federal Court made known to the then Attorney-General that they were not prepared to continue to issue warrants. As the Committee would appreciate, the ability for law enforcement agencies to use a range of investigative powers appropriate and adapted to the circumstances of a particular investigation is essential to the effective administration of justice. It would, therefore, be repugnant to the effective administration of justice for the proper conduct of investigations to be frustrated by the non-availability of issuing authorities to consider applications for warrants or authorisations for the use of such powers.

---

8 Administrative Appeals Tribunal Annual Report 2014-15, 34. This figure is not identified as being specific to applications under the Telecommunications (Interception and Access) Act only.

9 In *Wainohu v New South Wales* (2011) 243 CLR 181, the High Court held that the incompatibility restriction on the permissible functions of judges extended to judges of state and territory courts.

Given only a limited number of members of the judiciary wished to continue exercising this function, it was necessary to empower members of the AAT, being independent statutory office holders accustomed to reviewing the conduct of the executive, to also have the authority to consider applications for warrants and other investigative powers.

International law

It may also interest the Committee to know that comparable international jurisdictions do not require warrants to be issued by members of the judiciary. For example, within the European Union, the European Court of Human Rights has stated that, while 'it is in principle desirable to entrust supervisory control [of covert and intrusive investigatory powers] to a judge',[10] such powers can permissibly be authorised by members of the Executive provided that the warrant scheme is complemented by effective post-review of the authorisation.[11] More recently, in *Kennedy v The United Kingdom*[12], the Court held that the Interception of Communications Commissioner and the Investigatory Powers Tribunal provided effective safeguards in a system where authorisations are made at the Head of an Agency/Ministerial level.

In Australia, the current system entrusts the federal judiciary and nominated AAT members with issuing telecommunications interception and surveillance devices warrants. The Commonwealth Ombudsman and State and Territory oversight bodies conduct robust oversight of the warrants regime to ensure effective post-review of these investigatory powers.

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, noting the importance of these documents as a point of access to understanding the law and, if needed, as extrinsic material to assist with interpretation (e.g. section 15AB of the *Acts Interpretation Act 1901*)**.

continued

10 *Klass and others v Germany* [1978] ECHR 4.

11 Ibid.

12 (2010] ECHR 26839/05.

As noted above (and in previous comments by the committee—see, for example, the comments at p. 789 of the committee's *Fourteenth Report of 2014* in relation to the Counter-Terrorism Legislation Amendment (Foreign Fighters) Bill 2014), the committee's consistent preference is that the power to issue warrants authorising intrusive powers be conferred upon judicial officers. The committee generally does not regard factors such as 'administrative convenience' as being sufficient justification for conferring such power on non-judicial officers.

In addition, the committee notes that in some contexts the ability to issue warrants is limited to judicial officers and very senior members of the AAT (see, for example, sections 3ZZAD and 3ZZAF of the *Crimes Act 1914* which limits the issuing of delayed notification search warrants to a Deputy President or full-time senior member of the AAT who has been enrolled as a legal practitioner for not less than 5 years).

However, noting the explanation provided by the Attorney-General, the committee draws this matter to the attention of Senators and leaves the question of whether the proposed approach to the authorisation of warrants is appropriate to the Senate as a whole.

Alert Digest No. 13 of 2015 - extract

Retrospective validation
Schedule 9, item 54

This amendment seeks to retrospectively validate dealing with information relating to preventative detention orders in certain circumstances. The explanatory memorandum explains this item as follows (p. 94):

> This amendment is to ensure that an officer or staff member of a state or territory agency who previously communicated, made use of, or made a record of lawfully intercepted information for a purpose subsequently covered by the amended definition to "permitted purpose" (see item 3) would be taken not to have contravened the prohibition on communicating lawfully intercepted information under section 63 of the Act.
>
> This validation provision is to ensure that any officers who have in good faith used or communicated lawfully intercepted information for a purpose connected with state and territory PDO legislation are not liable for a breach of the Act. This provision is consistent with item 14 of the *Telecommunications (Interception and*

Access) Amendment Act 2010, which similarly validated past dealing in lawfully intercepted information in relation to the Commonwealth PDO regime.

While the explanatory memorandum refers to a requirement that information had been used or communicated in good faith, to the extent that the provision itself only requires that it would now be authorised by the extended definition of a 'permitted purpose' this does not specifically incorporate an element of dealing with the information in good faith. In addition, if the use of the information was not previously permitted then it seems appropriate that the reasons for retrospectively authorising the use of such information need to be explained in some detail. The committee consistently expects that the validation of the use of powers which may interfere with a person's privacy should be comprehensively justified. **The committee therefore requests a more detailed explanation from the Attorney-General in relation to the rationale for, and necessity 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

Schedule 9
Retrospective validation (item 54)

Telecommunications interception is considered a necessary and proportionate measure in preventing the terrorist threat in Australia. Preventative detention order regimes at the Commonwealth, state and territory level are also an important part of countering this threat.

There is a clear parliamentary intent to make lawfully intercepted information obtained under the TIA Act to be made available for the purposes of identifying, preventing and prosecuting acts of terrorism. This is reflected in the purposes for which lawfully intercepted information can be used, communicated, record and admitted into evidence in the TIA Act.

The PDO regime was established in 2005 based on a Council of Australian Governments agreement. The intention was for this to become a seamless national regime.

However, there is an anomaly in the TIA Act, which only allows lawfully intercepted information to be made available for the Commonwealth preventative detention order regime.

This anomaly has only been discovered as a result of recent operational activities and because of differences in the operation of preventative detention order regimes at the state and territory and Commonwealth level. These subtle differences have resulted from the implementation of the PDO regimes between jurisdictions. At the Commonwealth level, and in a number of states and territories, applications for PDOs are made to issuing authorities, who serve in their personal capacities, similar to an application for a warrant. In other jurisdictions, applications are made to a court, similar to applications for control orders. While subtle, this distinction has important implications for the operation of the TIA Act, which contains distinct rules for when lawfully intercepted information may be disclosed to a person (such as an issuing authority), and when it may be given and adduced into evidence in court. This amendment is designed to rectify this irregularity.

Committee response

The committee thanks the Attorney-General for this response and **requests that the key information above be included in the explanatory memorandum, noting the importance of these documents as a point of access to understanding the law and, if needed, as extrinsic material to assist with interpretation (e.g. section 15AB of the *Acts Interpretation Act 1901*)**.

In its initial comments the committee noted that the explanatory memorandum (at p. 94) refers to a requirement that the relevant information had been used or communicated *in good faith* in order for the use of the information to be retrospectively validated by this item.

As there is no explicit requirement for good faith on the face of this provision and the response does not address this matter, **the committee seeks the Attorney-General's further advice in this regard**.

Alert Digest No. 13 of 2015 - extract

Trespass on personal rights and liberties—freedom of expression
Schedule 11

This schedule seeks to create a new offence of publicly advocating genocide. The explanatory memorandum (at p. 108) states that:

> The offence applies to advocacy of genocide of people who are outside Australia or the genocide of national, ethnic, racial or religious groups within Australia. It only applies to advocacy done publicly.

Proposed new subsection 80.2D(3) defines 'advocate' for the purpose of the offence as counselling, promoting, encouraging or urging the commission of a genocide offence. These expressions will have their ordinary meaning.

The explanatory memorandum (at p. 109) suggests that it is important that the relevant expressions are interpreted broadly to ensure that a person who advocates genocide does not escape punishment by relying on a narrow construction of one of the terms. Some examples of the ordinary meaning of each of the expressions are included in the explanatory memorandum (at p. 109):

> …to "counsel" the doing of an act (when used as a verb) is to urge the doing or adoption of the action or to recommend doing the action; to "encourage" means to inspire or stimulate by assistance of approval; to "promote" means to advance, further or launch; and "urge" covers pressing by persuasion or recommendation, insisting on, pushing along and exerting a driving or impelling force.

The explanatory memorandum (at p. 110) also states that these questions will ultimately be determined by a judicial officer:

> Whether specific conduct, such as making or commenting on a particular post on the internet or the expression of support for committing genocide, is captured by the offence will depend on all the facts and circumstances. Whether a person has actually "advocated" the commission of a genocide offence will ultimately be a consideration for judicial authority based on all the facts and circumstances of the case.

While this may be accepted, the breadth of the definition may amount to an undue trespass on personal rights and liberties as it is not sufficiently clear what the law prohibits. This is particularly important given the substantial custodial penalty (7 years imprisonment). It is also possible that the provision may have a chilling effect on the exercise of the right of free expression. **However, in light of the explanation for the provision, the committee leaves the general question of whether it is appropriate to broadly define 'advocate' for the purpose of the offence of advocating genocide to the Senate as a whole.**

The explanatory memorandum (at p. 108) notes that 'publicly' is not defined in the bill although it would include, but not be limited to:

- causing words, sounds, images of writing to be communicated to the public, a section of the public, or a member of members of the public;
- conduct undertaken in a public place; or
- conduct undertaken in the sight or hearing of people who are in a public place.

While, as noted above, a definition of 'advocate' is included in proposed new subsection 80.2D(3), there is no guidance as to the meaning of 'publicly' on the face of the legislation. **The committee therefore seeks the Attorney-General's advice as to:**

- **whether it would be possible to include some guidance in the legislation itself in relation to the meaning of 'publicly' for the purpose of this proposed offence; and**
- **specific examples of the conduct intended to be covered by the 'public' component of the offence.**

The committee also notes that there are already a number of offences in the *Criminal Code* which may already cover conduct intended to be captured by this proposed offence. For example, section 80.2A (urging violence against groups) and section 80.2B (urging violence against members of groups) (these groups are distinguished by race, religion, nationality, national or ethnic origin or political opinion). **The committee therefore seeks the Attorney-General's advice as to what conduct is intended to be captured by this proposed offence that is not already captured by current offences.**

> *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

Schedule 11
Freedom of expression

In the current threat environment, the use of social media is accelerating the speed at which persons can become radicalised and prepared to carry out acts such as genocide. Law enforcement advises that it is no longer the case that explicit statements (which would provide evidence to meet the threshold of intention) are required to inspire others to take potentially devastating action in Australia or overseas. The cumulative effect of more generalised statements, particularly when made by a person in a position of influence and authority, can still have the impact of directly encouraging others to commit acts of violence, such as terrorism, hostile activities overseas, or genocide.

The proposed offence would supplement existing offences, such as those in Division 80 of the Criminal Code, that prohibit urging violence and advocating terrorism, and will be available as another tool available to law enforcement to intervene earlier in the radicalisation process to prevent and disrupt further engagement in terrorist activity.

Law enforcement is concerned about the impact those who advocate genocide, (commonly termed 'hate preachers') have on the current crime environment. The new advocating genocide offence is directed at those who supply the motivation and imprimatur. This is particularly the case where the person advocating genocide holds significant influence over other people who sympathise with, and are prepared to fight for, the genocide of a race or other group of individuals.

Under existing provisions in the Criminal Code, where a person 'incites' (within the meaning of section 11.4 of the Criminal Code) the commission of one of the primary genocide offences, the offence of incitement will only be made out where the person 'intended' a genocide offence to be committed. The current ancillary offence of inciting genocide carries a maximum penalty of 10 years imprisonment.

In contrast, the proposed new primary offence of advocating genocide will ensure that a person who advocates the commission of a primary genocide offence and is merely 'reckless' as to whether another person will commit a genocide offence as a result of their conduct. The new offence will only carry a maximum penalty of seven years imprisonment, reflecting the slightly lower fault element. As with 'tiered' offences, the option of a lower threshold/lower penalty offence can be important where a person's conduct breaches the criminal law, but the higher fault element cannot be proven beyond reasonable doubt.

Where there is sufficient evidence, existing offences of incitement or urging violence would be prosecuted. Those offences require proof that the person intended to incite or urge violence or a crime and intended the crime or violence to be committed. There will not always be enough evidence to meet the threshold of intention in relation to the second aspect. This is because persons advocating genocide can be very deliberate about the precise language they use, even though their overall message still has the impact of encouraging others to engage in genocide.

While 'publicly' is not defined, it would include, but would not be limited to:

- causing words, sounds, images of writing to be communicated to the public, a section of the public, or a member of members of the public (for example, creating a website which has no access restrictions and which encourages people to kill people of a particular race)
- conduct undertaken in a public place, (for example, gathering a crowd at a busy intersection in the centre of a city, shouting offensive language and urging people to take action to eradicate people of a particular religion), or
- conduct undertaken in the sight or hearing of people who are in a public place (for example, standing on a balcony above a cafe holding a banner which tells people to kill all people born in a particular country).

This is consistent with the *Convention on the Prevention and Punishment of the Crime of Genocide* (the Genocide Convention). Article III of the Genocide Convention requires

States Parties to punish individuals who engage in direct and public incitement to commit genocide.

The offence is also supported by Article 20(2) of the ICCPR, which requires States to create laws prohibiting advocacy for national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence.

The offence is subject to the existing 'good faith' defences to ensure it is a reasonable, necessary and proportionate limitation on the right to freedom of expression.

The department considers that the Explanatory Memorandum provides sufficient guidance as to what would constitute 'advocating' and 'publicly'. As is commonly done in legislative drafting, both words are intended to take their ordinary meaning when used in the Bill.

However the Committee may wish to consider that recommendations seventeen and eighteen of the PJCIS report consider aspects of the proposed advocating genocide offence. The Government is presently considering the PJCIS report.

Committee response

The committee thanks the Attorney-General for this response.

Further guidance in the explanatory memorandum

While the committee notes the advice that the 'department considers that the Explanatory Memorandum provides sufficient guidance as to what would constitute 'advocating' and 'publicly'', the committee **still requests that the key information above be included in the explanatory memorandum, noting the importance of these documents as a point of access to understanding the law and, if needed, as extrinsic material to assist with interpretation (e.g. section 15AB of the *Acts Interpretation Act 1901*). In particular, the committee notes that the advice in relation to the relationship between this proposed offence and existing offences in the Criminal Code, and the specific examples of the conduct intended to be covered by the 'public' component of the offence would be useful additions to the explanatory materials.**

Recommendations of the Parliamentary Joint Committee on Intelligence and Security (PJCIS)

The committee notes the recommendations of the PJCIS in relation to the proposed 'advocating genocide' offence.

continued

The PJCIS recommends that that the bill be amended so that, in order for a person to be convicted of the proposed advocating genocide offence, the person must be reckless as to whether another person might engage in genocide on the basis of their advocacy (recommendation 17). If the proposed offence is amended in accordance with this recommendation a person could only be guilty of the offence if it is proved beyond a reasonable doubt that the person *intentionally* advocated genocide and was *reckless* as to whether another person might engage in genocide on the basis of their advocacy. While this is a lower threshold than 'intention', the inclusion of a 'recklessness' threshold for the second element would still require the prosecution to prove that the accused was aware of a substantial risk that a genocide offence would occur as the result of their conduct and additionally, having regard to the circumstances known to him or her, it was unjustifiable to take that risk. **Noting the potential for this proposed offence to limit freedom of speech, the committee concurs with this recommendation of the PJCIS to include an additional element which will require, in order for a person to be convicted of the offence, that there must be a possibility that the advocacy was capable of influencing others to act.**

The PJCIS also recommended that the bill be amended to remove the word 'publicly' from the proposed advocating genocide offence (recommendation 18). In relation to this recommendation, the PJCIS suggests (at p. 167) that:

> Removing the term 'publicly' would be consistent with the existing 'advocating terrorism' offence, for which no such limitation applies. It would also address concerns raised by inquiry participants that it is not clear what conduct it is intended to be included—and excluded—by the use of the term.

The committee acknowledges that removing the 'public' component of the offence would address concerns in relation to the lack of clarity about what is intended to be captured by this component of the offence. However, such an amendment would also increase the scope of the offence to include all advocacy of genocide, whether in public or private. The committee notes that it would be possible to address the first concern by further clarifying the meaning of the term 'publicly' for the purpose of the proposed offence, rather than removing this component of the offence entirely. **The committee therefore leaves the question of the appropriate approach to take in relation to the 'public' component of this proposed offence to the Senate as a whole.**

Alert Digest No. 13 of 2015 - extract

Trespass on personal rights and liberties—requirements for obtaining a delayed notification search warrant
Schedule 14, general comment

The delayed notification search warrant scheme was established by the *Counter-Terrorism Legislation Amendment (Foreign Fighters) Act 2014*. The explanatory memorandum to that Act outlined the rationale for the scheme as follows:

> Under current Commonwealth search warrant provisions in the Crimes Act, the occupier of searched premises or their representative must be given a copy of the warrant if they are present (section 3H), which ensures that a search cannot occur without the occupier being made aware that the search is taking place. A delayed notification search warrant scheme will allow AFP officers to covertly enter and search premises for the purposes of preventing or investigating Commonwealth terrorism offences, without the knowledge of the occupier of the premises, with the occupier to be given notice at a later time. (p. 95 of the explanatory memorandum to the *Counter-Terrorism Legislation Amendment (Foreign Fighters) Act 2014*)

The statement of compatibility in relation to the current bill notes that:

> When the delayed notification search warrant regime was inserted into the Crimes Act in 2014, the threshold for issue required, not only the applicant (eligible officer), but also the police officer approving the application (chief officer) and the person considering whether to approve the warrant (eligible issuing officer) to suspect and believe certain things on reasonable grounds. (p. 3)

Current section 3ZZBA of the *Crimes Act 1914* provides that the threshold for issue of a delayed notification search warrant is met in respect of particular premises if the relevant person:

- suspects, on reasonable grounds, that one or more eligible offences have been, are being, are about to be or are likely to be committed; and
- suspects, on reasonable grounds, that entry and search of the premises will substantially assist in the prevention or investigation of one or more of those offences; and
- believes, on reasonable grounds, that it is necessary for the entry and search of the premises to be conducted without the knowledge of the occupier of the premises or any other person present at the premises.

The amendments in this schedule will amend the delayed notification search warrant regime 'to clarify that while the eligible [AFP] officer must suspect and believe [the above matters] on reasonable grounds, the chief officer [the AFP Commissioner] and eligible

issuing officer [a judge of the Federal Court of Australia or of a state or territory Supreme Court or a nominated AAT member] are not required to personally hold the relevant suspicions and belief. Rather, they must be satisfied that there are reasonable grounds for the eligible [AFP] officer to hold those suspicions and belief' (statement of compatibility, p. 3).

Given the potential for the delayed notification search warrant scheme to trespass on personal rights and liberties (by allowing AFP officers to covertly enter and search premises, without the knowledge of the occupier of the premises), the committee considers that the lowering of the threshold for issuing a delayed notification search warrant should be comprehensively justified. The committee therefore seeks the Attorney-General's detailed advice as to the rationale for this proposed change.

> *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

Schedule 14
Requirements for obtaining a delayed notification search warrant

The purpose of this amendment is to clarify the requirements for the issue of a delayed notification search warrant. A literal reading of the provision as drafted in Crimes Act would require a chief officer and an issuing officer to personally hold suspicions or beliefs that they are not in a position to personally hold as persons removed from the investigation. This was not intended when the provision was drafted.

The intended operation of the regime was, as with other warrant regimes, to provide safeguards against abuse of the regime by requiring the chief officer and eligible issuing officer to independently be satisfied that the eligible officer in fact holds the requisite suspicions and belief, and that there are reasonable grounds for holding the suspicions and belief. In the case of the eligible issuing officer, this is to be achieved by receiving information from the eligible officer on oath or affirmation. For example, a search warrant may be issued under subsection 3E(1) of the Crimes Act only where the issuing officer is satisfied that there are reasonable grounds for suspecting that there will be evidential material at a premises, rather than where the issuing officer personally holds such a suspicion him/herself.

Committee response

The committee thanks the Attorney-General for this response and **requests that the key information above be included in the explanatory memorandum, noting the importance of these documents as a point of access to understanding the law and, if needed, as extrinsic material to assist with interpretation (e.g. section 15AB of the *Acts Interpretation Act 1901*)**.

The committee notes the Attorney-General's advice that a 'literal reading of the provision as drafted in Crimes Act would require a chief officer and an issuing officer to personally hold suspicions or beliefs that they are not in a position to personally hold as persons removed from the investigation'.

Noting this advice, the committee leaves the question of whether the lowering of the threshold for issuing a delayed notification search is appropriate to the Senate as a whole.

Alert Digest No. 13 of 2015 - extract

Trespass on personal rights and liberties—fair hearing
Schedule 15, item 19, proposed new section 38J

The broad purpose of the *National Security Information (Criminal and Civil Proceedings) Act 2004* (the NSI Act) is to prevent the disclosure of information in federal criminal and civil proceedings where disclosure is likely to prejudice national security. This Schedule proposes some significant amendments to that Act by enabling a court to make three new types of orders in control order proceedings. The effect of the proposed amendments can generally be described as allowing the court to determine that it can rely, in control order proceedings, on secret evidence in particular circumstances. The three new orders a court may make are:

- that the subject of the control order and their legal representative may only be provided with a redacted or summarised form of national security information. Despite this, however, the court may consider the information in its entirety (proposed new subsection 38J(2));
- that the subject of the control order and their legal representative may not be provided with any information in an original source document. Despite this, however, the court may consider all of that information (proposed new subsection 38J(3)); and

- when a hearing is required under subsection 38H(6) the subject of the control order and their legal representative can be prevented from calling the relevant witness, and if the witness is otherwise called, the information provided by the witness need not be disclosed to the subject of the control order or their legal representative. Despite this, however, the court may consider all of the information provided by the witness (proposed new subsection 38J(4)).

Notably, proposed section 38I provides that a court may determine whether one of the new orders should be made in a closed hearing, that is, a hearing at which the parties to the control order proceeding and their legal representatives are not present.

These proposals clearly undermine the fundamental principle of natural justice which includes a fair hearing. In judicial proceedings a fair hearing traditionally includes the right to contest any charges against them but also to test any evidence upon which any allegations are based. In many instances it may not be possible in practice to contest the case for the imposition of control orders without access to the evidence on which the case is built. Evidence is susceptible to being misleading if it is insulated from challenge. Given that the burden of proof in civil cases is lower than criminal proceedings, that risk is magnified.

The explanatory materials point to the increasing 'speed of counter-terrorism investigations' as the reason why these powers are necessary (p. 119). At the general level, the explanatory memorandum suggests that 'for control orders to be effective, law enforcement needs to be able to act quickly, and be able to present sensitive information…to a court as part of a control order proceeding without risking the integrity, safety or security of the information or its source' (p. 119). (See also the statement of compatibility at pp 23–24)

On the other hand, the explanatory memorandum also recognises that it is important that a court, in the context of control order proceedings, continue to be able to 'ensure procedural fairness and the administration of justice'. Given the extent to which the non-disclosure of evidence compromises a fair hearing it is, however, doubtful whether the amendments in this provision adequately preserve procedural fairness to the subject of a control order.

The statement of compatibility suggests that 'the inherent capacity of the court to act fairly and impartially as well as the safeguards built into the NSI Act provide several mechanisms through which a fair hearing is guaranteed' (pp 24–25). More particularly, the following features of the statutory scheme are thought to justify the abrogation of the fair hearing rules which section 38J orders necessarily entail:

- Paragraph 38J(1)(c) provides that before issuing a 'special court order' under section 38J, the court must be 'satisfied that the relevant person has been given notice of the allegations on which the control order request was based (even if the relevant person has not been given notice of the information supporting those allegations)'.

- Prior to making a special order under section 38J, the court must (see proposed subsection 38J(5)) have regard to (a) the risk posed to national security, (b) 'whether any such order would have a substantial adverse effect on the substantive hearing in the proceeding', and (c) any other matter the court considers relevant.
- It is suggested that requiring a court to consider whether making an order would have an adverse impact on the substantive hearing 'ensures that the court expressly contemplates the effect of any potential order…on a party's ability to receive a fair hearing' and that this provides 'the court with the discretion to adequately assess the impact of an order under revised section 38J on each subject (or proposed subject) of the control order' (pp 24–25).
- The NSI Act, it is suggested, 'guarantees procedural fairness by preserving the discretion of the court' not to make an order (or the nature of the order to make) under section 38J. It is also noted that the court has the discretion under proposed subsection 38I(3A) to refuse to exclude specified parties and their legal representatives from the closed hearing proceedings (p. 25).
- The right of the court to stay a control order proceeding where an order would have a substantial adverse effect on the substantive control order proceeding has been preserved in this context. Relatedly, the point is made that the court has a general power (under existing subsection 19(3)) to control the conduct of civil proceedings, 'in particular with respect to abuse of process unless the NSI Act expressly or impliedly provides otherwise' (p. 25).

A number of objections can be raised in response to this justification of the proposed amendments.

First, notice of allegations in the absence of notice of the information supporting those allegations, may well deprive a person of the practical means by which he or she is able to make their case. In many contexts, a case against a person cannot be tested unless the basis of that case is disclosed. Allegations can be denied, but without details it may not be possible to disprove them or even to cast doubt on them.

Secondly, the requirement to consider the effect an order may have on the 'substantive hearing' does not require the court to place a particular weight upon this factor. In this context, it can be noted that courts are not well placed to second-guess law enforcement evaluations of national security risk which means that it may be particularly challenging to protect an individual's interest in a fair hearing. Furthermore, the language of 'substantive hearing' does not clearly identify procedural fairness as a fundamental relevant consideration to the decision-making exercise. When it comes to the consideration of a risk to national security, the court is not expressly limited to making orders where that risk is considered to reach a threshold degree of seriousness.

Thirdly, the fact that the court has discretion as to how to draw the balance between national security and any adverse effect on the 'substantive hearing' (in relation to whether a special order be made, or in the exercise of any general powers to stay or control its

proceedings) cannot be said to 'guarantee' procedural fairness. In considering the extent to which judges will be able, in the exercise of their discretionary powers under the proposed regime, to resist the claims of a law enforcement agency that an order should be made, it should be noted that judges routinely accept that the courts are 'are ill-equipped to evaluate intelligence' [*Leghaei v Director-General of Security* (2007) 241 ALR 141; (2007) 97 ALD 516] and the possibility that law enforcement agencies may be wrong in their national security assessments. For this reason, the fact that security information is read by judges in the context of the legislative regime proposed in this schedule does not mean that they will be well placed to draw a different balance between security risk and fairness than is drawn by law enforcement agencies.

For the above reasons, it is suggested that the assertion that the proposed approach upholds the right to a fair hearing is significantly overstated. **In this context the committee therefore seeks a more detailed justification from the Attorney-General for the proposed approach. In particular, the committee seeks advice as to whether further safeguards for fairness have been considered, and if so why they have not been included in the legislation, for example, whether the court could be expressly limited to making these special orders where a risk to national security is considered to reach a threshold degree of seriousness.**

The committee also notes the UK system of special advocates and recommendations in the 2013 'Council of Australian Governments Review of Counter-Terrorism Legislation'.

> *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

Schedule 15
Fair hearing (item 19, proposed new section 381)

Under the NSI Act, there are existing provisions that enable a court to consider, in a closed hearing, whether national security information may be disclosed and if so, in what form. The court has the discretion to exclude non-security cleared parties, their non-security cleared legal representatives and non-security cleared court officials from the hearing where the court considers that disclosing the relevant information to these persons would likely prejudice national security. If a party's legal representative is not security cleared, does not wish to apply for a security clearance, or a clearance is unable to be obtained in sufficient time before the closed hearing, then the court may still hold the closed hearing and determine the matter without the assistance of a legal representative of the party. Alternatively, the court could decide to appoint a security cleared special counsel to

represent the interests of the party during the closed hearing (although there has been no need for a security cleared special counsel to be appointed under the NSI Act to date). However, any information the court decides should not be disclosed under the NSI Act cannot be used in the substantive proceeding.

The purpose of the proposed amendments to the NSI Act is to provide the court with two further options when the NSI Act has been invoked in a control order proceeding. First, the option to exclude a respondent's legal representative, even if they are security cleared, at the closed hearing to determine if or how the information should be disclosed in the substantive control order proceeding. Second, it provides the option for the court to still consider that evidence in the substantive control order proceeding, even if it cannot be disclosed to the party or their lawyer (whether security cleared or not). The rationale for these amendments is that the evidence may be so sensitive that even a security cleared legal representative cannot see the information.

The AFP's submission to the PJCIS inquiry into the Bill explains the importance of protecting sensitive information, not only to maintain the confidentiality and integrity of law enforcement and intelligence operations and methodologies, but also to maintain the trust with which law enforcement has been provided this information. It also explains that in the current threat environment, it is increasingly likely that law enforcement will need to rely on evidence that is extremely sensitive, such that its disclosure, even to a security-cleared lawyer, could jeopardise the safety of sources and the integrity of investigations. There is a substantial risk that the inability to rely on sensitive information may mean that control orders are unable to be obtained in relation to a person posing a high risk to the safety of the community. Accordingly, the purpose of the amendments is aimed at achieving the legitimate objective of protecting national security information in control order proceedings, the disclosure of which may be likely to prejudice national security.

The amendments to the NSI Act will provide the court with the ability to make three new types of orders to protect national security information that may result in the court being able to consider information in a control order proceeding that the person the subject of the control order proceeding (or their legal representative) may not see. Prior to making one of these new orders, under paragraph 38J(1)(c), the court must be satisfied that the subject of the control order proceeding has been provided sufficient notice of the allegation on which the control order request is based (even if the person has not been given notice of the information supporting those allegations).

When considering the effect of the proposed amendments to the NSI Act, it is important to consider the proposed amendments as a whole rather than considering the sections in isolation. There are several protections built into the legislation that mitigate any procedural unfairness. Prior to making one of the new orders, the court must consider whether the order would have a substantial adverse effect on the substantive control order proceeding (subsection 38J(5)). This requires the court to contemplate the effect that withholding the information from the respondent or their legal representative will have on procedural fairness for the subject of the control order proceeding. Furthermore, the

proposed amendment to subsection 19(4) will confirm that the court has discretion to later order a stay of a control order proceeding, if one of the new orders has been made and later in the proceedings it becomes evident that the order would have a substantial adverse effect on the substantive control order proceeding.

Importantly, the court also has discretion to decide which order to make and the form the order should take. For example, if the AFP proposes to withhold an entire document from the subject of a control order, but use it in support of the control order application, the court may decide that only part of the document may be withheld and used, or that the entire document can be withheld and used but the person must be provided with a summary of the information it contains. This is often referred to as 'gisting'.

Furthermore, the normal rules of evidence apply to evidence sought to be introduced under these new orders, in accordance with the express terms of section 38J and the existing Criminal Code provisions (section 104.28A). The effect of those provisions is that if any material is withheld from the respondent but used in the proceeding, that material must otherwise be admissible as evidence under the normal rules of evidence applicable in control order proceedings. There is also nothing in the new provisions that would dictate to the court what weight it should give to any evidence that is withheld (either in full or in part) from the respondent in the substantive control order proceeding.

Accordingly, the amendments provide an appropriate balance between the need to protect national security information in control order proceedings, and procedural fairness to the person to whom the control order relates. It preserves the independence and discretion of the court and instils it with the powers needed to mitigate unfairness to the subject of a control order proceeding.

The Committee asked whether the court could be expressly limited to making one of the new orders under section 38J where a risk to national security is considered to reach a threshold degree of seriousness. This is unnecessary. The court will only be able to consider making one of the new orders under section 38J if the Attorney-General or the Attorney-General's legal representative has requested the court to make such an order. This will ensure that one of the new orders will only be sought in limited situations. Furthermore, the courts are well-equipped to make judgments as to the weight that should be given to the risk that disclosing information will prejudice national security information, any substantial adverse effect on the substantive control order proceeding, and any other matter the court considers relevant, when determining whether to grant one of the new orders. There is no requirement that the court must provide greater weight to one factor above others when determining whether to make one of the new orders under section 38J.

Recommendations four to six of the PJCIS report consider various aspects of the proposed amendments to the NSI Act. The Government is presently considering the PJCIS report.

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, noting the importance of these documents as a point of access to understanding the law and, if needed, as extrinsic material to assist with interpretation (e.g. section 15AB of the *Acts Interpretation Act 1901*)**.

The committee notes the Attorney-General's advice, however the committee does not agree with the Attorney-General's conclusion that:

> …the amendments provide an appropriate balance between the need to protect national security information in control order proceedings, and procedural fairness to the person to whom the control order relates. It preserves the independence and discretion of the court and instils it with the powers needed to mitigate unfairness to the subject of a control order proceeding.

For example, in relation to the statement that 'the courts are well-equipped to make judgments as to the weight that should be given to the risk that disclosing information will prejudice national security information', the committee reiterates its comments about the extent to which judges will be able (in practice) to independently assess the claims of a law enforcement agency that an order should be made. In this context, it should be noted that judges routinely accept that the courts are 'are ill-equipped to evaluate intelligence' [*Leghaei v Director-General of Security* (2007) 241 ALR 141; (2007) 97 ALD 516] and the possibility that law enforcement agencies may be wrong in their national security assessments. For this reason, the fact that security information is read by judges in the context of the legislative regime proposed in this schedule does not mean that they will be well placed to draw a different balance between security risk and fairness than is drawn by law enforcement agencies. The fact that the courts are not well placed to second-guess law enforcement evaluations of national security risk means that it may be particularly challenging for the courts to appropriately protect an individual's interest in a fair hearing.

In light of this, the committee is not persuaded that the amendments 'provide an appropriate balance between the need to protect national security information in control order proceedings, and procedural fairness to the person to whom the control order relates' as suggested by the Attorney-General.

The committee draws its concerns in relation to this matter to the attention of Senators.

continued

Recommendations of the Parliamentary Joint Committee on Intelligence and Security (PJCIS)

Noting the above concerns, the committee draws the following relevant recommendations of the PJCIS to the attention of Senators.

The committee concurs with the view of the PJCIS (at p. 74) that:

The proposed amendments to the NSI Act mark a significant departure from the existing architecture of the NSI Act, which currently does not provide for information to be adduced in substantive proceedings (be it control order proceedings, or otherwise) that can be withheld from the affected party and their legal representative.

Minimum standard of disclosure and system of special advocates

The committee notes that the minimum standard of disclosure proposed in paragraph 38J(1)(c) of the bill as currently drafted stems from the decision of the High Court in *Assistant Commissioner Condon v Pompano Pty Ltd* (2013) 252 CLR 38. This minimum standard states that the subject of the control order application must be provided 'notice of the allegations on which the control order request was based (even if the relevant person has not been given notice of the information supporting those allegations)'.

The PJCIS recommended that the bill be amended:

… such that the minimum standard of information disclosure outlined in proposed paragraph 38J(1)(c) of the *National Security Information (Criminal and Civil Proceedings Act) 2004* reflects the intent of Recommendation 31 of the Council of Australian Governments Review of Counter-Terrorism Legislation, namely that the subject of the control order proceeding be provided 'sufficient information about the allegations against him or her to enable effective instructions to be given in relation to those allegations' (recommendation 4).

In relation to the possibility of establishing a system of special advocates, the PJCIS recommended:

…that a system of special advocates be introduced to represent the interests of persons subject to control order proceedings where the subject and their legal representative have been excluded under the proposed amendments to the National Security Information (Criminal and Civil Proceedings) Act 2004 contained in Schedule 15 of the Counter-Terrorism Legislation Amendment Bill (No. 1) 2015 (recommendation 5).

In light of the committee's scrutiny concerns outlined above, the committee considers that providing for a system of special advocates and amending the minimum standard of disclosure so that it explicitly requires at least sufficient information to be provided so as to enable the subject of a control order proceeding to give effective instructions may represent an improvement to the bill as currently drafted.

continued

In accordance with the committee's usual practice, the committee will consider (and, if appropriate, comment) on any amendments made to the bill by either House of the Parliament.

Reporting and oversight

The committee concurs with the view of the PJCIS that 'public confidence in and oversight of the regime would benefit from ascertaining the frequency with which these orders are made' (p. 81). **In particular, the committee welcomes the recommendation that the bill:**

…be amended to require that, as part of the Attorney-General's annual reporting obligations to the Parliament under section 47 of the *National Security Information (Criminal and Civil Proceedings) Act 2004*, the Attorney-General must also annually report on:
(a) the number of orders under proposed section 38J that were granted by the court, and
(b) the control order proceedings to which the orders granted by the court under proposed section 38J relate (recommendation 6).

The committee also agrees with the view of the PJCIS that it would be useful for the INSLM to 'review the operation, effectiveness and implications of the proposed amendments to the NSI Act contained in this schedule, as well as to consider whether it contains appropriate safeguards for protecting the rights of individuals and remains proportionate and necessary' (p. 82).

Alert Digest No. 13 of 2015 - extract

Retrospective application
Schedule 15, item 27

Item 27 of schedule 15 states that the new special orders in relation to secret evidence that may be made under proposed section 38J apply to civil proceedings that begin before or after the commencement of this section.

The explanatory materials do not explain why the amendments should apply to proceedings which have already begun, especially given that (as explained above) the amendments appear to be in conflict with the fair hearing principle. **The committee therefore seeks the Attorney-General's advice as to the rationale for the proposed**

retrospective application of the amendments to proceedings already commenced and as to how many current proceedings or potential proceedings are, or are likely to be, affected by 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

Retrospective application (item 27)

It is appropriate that the new orders are available as soon as they come into force, regardless of whether a control order proceeding has already commenced. This is consistent with existing protections that are available under the NSI Act. Section 6A of the NSI Act provides that the Act can apply to civil proceedings that take place after the NSI Act has been invoked, irrespective of whether the proceedings commenced prior to the invocation of the Act. However, the new orders will only be available to those parts of the proceeding that have not yet occurred. Accordingly, the provisions will not operate retrospectively.

Committee response

The committee thanks the Attorney-General for this response and **requests that the key information above be included in the explanatory memorandum, noting the importance of these documents as a point of access to understanding the law and, if needed, as extrinsic material to assist with interpretation (e.g. section 15AB of the *Acts Interpretation Act 1901*)**.

The committee leaves the question of whether the new orders should be available in proceedings that have started before the commencement of these new provisions to the Senate as a whole.

Alert Digest No. 13 of 2015 - extract

Trespass on personal rights and liberties—protected taxation information and privacy
Schedule 17, general comment

This schedule enables disclosure of protected information by taxation officers for the purposes of preventing, detecting, disrupting or investigating conduct that relates to a matter of security as defined by the ASIO Act.

Clearly there are implications for personal privacy in relation to the amendment. The explanatory materials suggest that the importance of the public purposes of enabling government agencies to use information where so doing could prevent, detect, disrupt or investigate conduct that relates to a matter of security outweigh this adverse consequence (statement of compatibility, p. 31).

From a scrutiny perspective it is, however, a matter of concern that disclosure is authorised to 'any' Australian government agency. The statement of compatibility suggests that this is justified because 'as with bodies that have a role in preventing or reducing a serious threat to an individual's life, health or safety or the public's health or safety, bodies that have a role in preventing, disrupting or investigating a threat related to security vary from time to time' (p. 31). The statement of compatibility notes that bodies such as the National Disruption Group are multi-jurisdictional and the composition may change at short notice.

Although the committee accepts that some breadth in the authorisation to disclose may be appropriate, it is not persuaded that it is necessary to authorise disclosure to 'any' Australian government agency for the purposes of this provision. **The committee therefore seeks the Attorney-General's advice about more targeted alternative authorisation options and why they were rejected. The committee notes that flexibility with some parliamentary oversight could be maintained through the use of a disallowable legislative instrument to extend authorisation to additional agencies.**

> *Pending the Attorney-General's reply, the committee draws Senators' attention to the schedule, 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

Schedule 17
Protected taxation information and privacy

This amendment will authorise taxation officers to disclose information to an Australian government agency for certain specified purposes. It is important that the amendment allows the ability to disclose information for the purposes of preventing, detecting, disrupting or investigating conduct that involves a threat related to security, to 'any' Australian government agency. This is because, as with bodies with a role in preventing or taking steps to reduce a serious threat to an individual's life, health or safety or the public's health or safety (see section 355-65(2) Table 1 item 9 of the *Taxation Administration Act 1953)*, bodies that have a role in preventing, detecting, disrupting or investigating conduct that involves a matter of security vary over time.

Currently, the key agencies envisaged to seek disclosure under this provision are the National Disruption Group (NDG), which is comprised of officers from a range of Departments, and the Australian Counter-Terrorism Centre (ACTC). However, as we have already seen, the membership or composition of such bodies can change at short notice.

This amendment will ensure that ATO officers have the ability to disclose relevant information to allow early intervention in terrorist activities to prevent the possible widespread and devastating consequences of a terrorist attack. Tax information could be extremely useful for that purpose (although we acknowledge in limited circumstances – and therefore we do not anticipate this amendment being used on a regular basis) and we consider that the possible benefits disclosing that information may have for protecting security outweighs the associated loss of privacy.

Options arbitrarily limiting the Australian government agencies to which disclosures could be made to those agencies that have a national security role today could prevent disclosure to an agency with a national security role tomorrow. This could have devastating outcomes, including loss of many lives in time critical scenarios.

Recommendation twenty of the PJCIS report considers the Commonwealth Ombudsman having oversight of the disclosure of protected tax information. The Government is presently considering the PJCIS report.

Committee response

The committee thanks the Attorney-General for this response and **requests that the key information above be included in the explanatory memorandum, noting the importance of these documents as a point of access to understanding the law and, if needed, as extrinsic material to assist with interpretation (e.g. section 15AB of the *Acts Interpretation Act 1901*)**.

As stated above, the committee accepts that some breadth in the authorisation to disclose may be appropriate and notes that it is not suggesting 'arbitrarily limiting' the scope of the provision. However, it is not persuaded that it is necessary to authorise disclosure to 'any' Australian government agency for the purposes of this provision without any parliamentary oversight. The committee emphasises that flexibility with some parliamentary oversight could be maintained through the use of a disallowable legislative instrument to extend authorisation to additional agencies or classes of agencies where necessary.

The committee draws its concerns to the attention of Senators and leaves the question of whether allowing disclosure of taxation information to 'any' Australian government agency is appropriate to the Senate as a whole.

Social Security Legislation Amendment (Community Development Program) Bill 2015

Introduced into the House of Representatives on 2 December 2015
Portfolio: Indigenous Affairs

Introduction

The committee dealt with this bill in *Alert Digest No. 1 of 2016*. The Minister responded to the committee's comments in a letter dated 23 February 2016. A copy of the letter is attached to this report.

Alert Digest No. 1 of 2016 - extract

Background

This bill amends the: *Social Security Act 1991* and *Social Security (Administration) Act 1999* to:

- create new income support payment and compliance arrangements for individuals living in remote Australia who are eligible for activity tested income support payments including Newstart, youth allowance, parenting payment, disability support pension and special benefit; and
- remove spent provisions in relation to the Northern Territory Community CDEP Transition Payment and the Community Development Employment Project Scheme.

The bill also to makes consequential amendments to the *Social Security (Administration) Act 1999* and *Social Services Legislation Amendment (Youth Employment) Act 2015*.

Delegation of legislative power
Insufficient Parliamentary scrutiny
General

The purpose of this bill is to introduce a distinctive community development program in remote areas. The objective is to better achieve positive outcomes in encouraging job seekers in remote Australia to understand the link between fulfilling requirements under the CDP program and income support payments. The bill establishes a structure which will enable simpler payment and compliance arrangements to be introduced.

To achieve this outcome the Minister will be authorised to exercise legislative power in two ways. First, the Minister will be empowered to determine, in a legislative instrument, the scheme for the imposition of obligations and to ensure compliance in relation to remote income support recipients. Second, the Minister may specify, by legislative instrument,

remote income support regions in which these measures will operate (see proposed section 1061ZAAZ). The Minister may also determine by legislative instrument that the operation of the social security law be modified in relation to remote income recipients.

It therefore appears that the central elements of the scheme are to be determined by legislative instrument and that these matters will be of great practical importance to those affected by them. The explanatory materials contain a detailed justification of the need for differentiated CDP arrangements in remote communities. It is argued that the generally applicable framework is failing in remote regions and that an approach targeted specifically to the unique circumstances in remote communities in relation to strengthening incentives for job seekers is necessary. The key rationale for providing for central elements of the scheme in legislative instruments rather than the primary legislation is that this 'will allow the Minister to consult with communities and the Parliament to determine participation requirements and compliance arrangements and to make amendments to meet the changing needs of communities' (at p. 3). The intention in enabling the Minister to determine which specific regions will be covered by the scheme is to enable the targeted consideration of relevant matters (such as the level of social and economic disadvantage). The explanatory memorandum indicates that it is expected that 'these arrangements will be phased in and will initially apply in no more than four regions'. The explanatory memorandum also provides the assurance that there 'will be extensive community consultation with communities to be included…and participating providers will be assessed and supported to ensure they have sufficient capability and capacity to deliver the new arrangements' (see pp ii-iii).

While these matters are very significant and may be considered more suitable for Parliamentary enactment, in light of the detailed explanation provided the committee draws this matter to the attention of Senators, but leaves the general question of whether the proposed approach is appropriate to the consideration of the Senate as a whole.

However, in light of the importance of the issues involved, the committee seeks the Minister's advice as to whether consideration can be given to including a reporting requirement to evaluate: (a) the operation of the scheme and (b) the appropriateness of the use of delegated legislation (to be tabled in Parliament to facilitate parliamentary scrutiny).

> *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 and to insufficiently subject the exercise of legislative power to parliamentary scrutiny, in breach of principle 1(a)(v) of the committee's terms of reference.*

Minister's response - extract

The CDP Bill provides a framework for amending welfare arrangements to increase incentives to take up work in remote communities. There are a number of outstanding policy decisions regarding the detail of the compliance arrangements and other legislative instruments. This is intentional to ensure sufficient time to develop the instruments in consultation with people likely to be affected by their operation such as CDP providers and job seekers.

Please see below my advice on whether consideration can be given to including a reporting requirement to evaluate:

a) the operation of the scheme

I will undertake a review on phase one for the CDP legislative reforms prior to consideration of the detail of future phases. This review will be undertaken prior to the 2017-18 Budget.

Further consideration will be given to including an evaluation of the CDP Bill.

b) the appropriateness of the use of delegated legislation

Compliance arrangements will be determined in a legislative instrument, subject to the usual rules providing for possible disallowance by either House of Parliament and scrutiny by the Senate Standing Committee on Regulations and Ordinances.

In relation to the determination of remote income support regions, I will consider service provider capacity and fulfil the consultation requirements under the *Legislative Instruments Act 2003* before the relevant legislative instrument is made. Again, this legislative instrument would be subject to disallowance by either House of Parliament and available for scrutiny by the Senate Standing Committee on Regulations and Ordinances.

Use of legislative instruments is appropriate in this case because of the technical and detailed nature of the requirements contained in the legislative instruments that require further consultation with relevant stakeholders. In addition, legislative instruments may need to be amended either during or following the initial phase of implementation.

Please note that I have committed to making further information in relation to the detail of the scheme available to members of Parliament before debate of the CDP Bill and expect to circulate consultation papers on the proposed CDP penalties scheme and compliance framework by mid-March.

I note your advice in relation to the delegation of legislative powers and decision to leave open to the consideration of the Senate whether this is appropriate.

Thank you for the opportunity to respond to your concerns.

Committee response

The committee thanks the Minister for this response and notes the advice provided in relation to (1) the Minister's proposed review of phase one before the 2017-18 Budget and (2) the further explanation for reliance on delegated legislation for such significant matters, including the technical and detailed nature of much of the content, the commitment to making further information available before debate and the fact that instruments will be disallowable.

While the committee retains it concern that these significant matters may be considered more suitable for Parliamentary enactment, the committee welcomes the proposed commitment to make further information available before debate and the Minister's intention review phase one after a period of implementation. The committee draws this reliance on delegated legislation to the attention of Senators, but leaves the general question of whether the proposed approach is appropriate to the consideration of the Senate as a whole.

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

Senator Helen Polley
Chair

THE HON SUSSAN LEY MP
MINISTER FOR HEALTH
MINISTER FOR AGED CARE
MINISTER FOR SPORT

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

Dear Senator Polley

I refer to the Committee Secretary's letter of 25 February 2016, seeking advice on the proposed operation of subsection 23B-1(1) relating to prioritised home care recipients in the Aged Care Legislation Amendment (Increasing Consumer Choice) Bill 2016.

Schedule 1, item 44, proposed subsection 23B-1(1)
The Committee is seeking further information as to why merits review is impractical in the circumstances of the programme and in the exercise of this particular power.

Subject to passage of the Bill, new Part 2.3A of the *Aged Care Act 1997* (the Act) sets out the process for the prioritisation of home care recipients (consumers). The introduction of a consistent national system for prioritising access to subsidised home care will allow for a more equitable and flexible distribution of packages to consumers based on individual needs and circumstances.

This is important because the number of home care packages will continue to be capped or limited at each of the four package levels. In determining the number of consumers who can be prioritised for packages, the Secretary of the Department of Health will continue to work within the Government's policy parameters of the aged care planning ratio and the forward estimates. The Secretary does not have flexibility to adjust these parameters. At present, demand for packages substantially exceeds number of packages available, particularly for higher level packages.

The proposed subsection 23B-1(1) provides that the Secretary may, by written notice, determine that a person is a 'prioritised home care recipient' for the purposes of the programme. This is one of the criteria that must be satisfied in order for home care subsidy to be paid to an approved provider under section 46-1 of the Act for the provision of care to that person.

In making a determination under subsection 23B-1(1), the Secretary must consider the factors set out in subsection 23B-1(4). These factors are: (a) the time that a person has been waiting for care; (b) a person's 'priority for home care services' determined under section 22-2A; and (c) any other matters specified in the Prioritised Home Care Recipient Principles.

The time that a person has been waiting for home care (from the date of the person's approval under Part 2.3 of the Act) is an objective criterion that does not allow discretion in decision-making by the Secretary and is therefore not suitable for merits review.

The determination of a person's priority for home care services under section 22-2A is a decision of the Secretary, based on information about a person's clinical and care needs (collected as part of the comprehensive assessment undertaken by an Aged Care Assessment Team). Decisions regarding a person's priority will be subject to merits review under Part 6.1 of the Act. In addition, the Act provides for written notice, including reasons for these decisions, to be provided to the consumer. The outcome of a decision under section 22-2A will directly impact on a decision made under subsection 23B-1(1).

It is not intended that any additional matters would be specified in the Prioritised Home Care Recipient Principles at this time. However, if any other matters are specified in the future, these would relate to objective factors because, as indicated in new section 23B-4, it is anticipated that the issuing of a notice under subsection 23B-1(1) will be an automatic process through the My Aged Care computer system.

Subsection 23B-1(5) allows the Secretary to consider any other exceptional circumstances in addition to the criteria set out in subsection (4). This provision would only be used in limited circumstances and to the benefit of consumers requiring priority access to care. The kinds of exceptional circumstances envisaged under subsection (5) include emergency care situations or instances of market failure (e.g. where individuals or groups of people are not able to access care in an appropriate and timely manner). Decisions would be made by the Secretary, or a delegate at the SES officer level within the Department.

Generally only individuals who are the subject of a decision can seek a review. It is therefore considered impractical for merits review because the individual will have been prioritised for a home care package.

The Committee is also seeking advice as to whether any measures, such as alternatives to merits review, have been considered in relation to determinations made under subsection 23B-1(1).

The legislation will provide transparency regarding the factors to be considered in the prioritisation process. To assist stakeholders to understand how decisions will be made, the prioritisation process, including review rights available to consumers under section 22-2A, will be clearly explained in public materials. Information resources will be developed specifically for consumers, carers, assessors and providers. The My Aged Care Gateway and advocacy services will also support consumers and carers. The prioritisation process will be closely monitored to ensure that the factors are applied correctly and consistently.

To further support accountability in the programme, the Department will make available information about expected waiting times, i.e. the time that a person would typically wait for a package after their approval by an Aged Care Assessment Team. The outcomes of the prioritisation process will be closely monitored to ensure that consumers, including people with special needs and those living in rural and regional areas, are able to access care in a fair and equitable manner. There will be regular public reporting on the operation of the prioritisation process and access to care though the programme.

Thank you for bringing these issues to my attention and I trust the information will address the concerns of the Committee.

Thank you for bringing these issues to my attention and I trust the information will address the concerns of the Committee.

The Hon Sussan Ley MP

29 FEB 2016

THE HON MICHAEL KEENAN MP
Minister for Justice
Minister Assisting the Prime Minister on Counter-Terrorism

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

Dear Chair

I refer to the Senate Scrutiny of Bills Committee's request for further information about the Australian Crime Commission Amendment (National Policing Information) Bill 2015, as outlined in the Committee's Alerts Digest No. 1 of 2016 tabled on 3 February 2016.

The Committee has sought additional information about Schedule 1, items 17 and 30 – proposed subsections 46A(5), (6) and (7) and section 59AAA – on the basis that they may unduly trespass on the right to privacy.

Specifically, the Committee has asked for further advice on:

1. whether the legislation should contain more guidance in relation to the types of bodies that may access nationally coordinated criminal history checks under subsections 46A(5), (6) and (7)
2. whether directions issued by the ACC Board in relation to accreditation under subsections 46A(5), (6) and (7) should be subject to Parliamentary oversight and disallowance, and
3. whether the legislation should contain guidance about the setting of limits and conditions for s59AAA disclosures and, if not, whether the setting of such limits should be, at least, subject to disallowance.

For the reasons outlined in the Statement of Compatibility with Human Rights for the Bill and further detailed below, I am satisfied that the further measures suggested by the Committee are not necessary to protect the right to privacy.

Current arrangements for nationally coordinated criminal history checks

CrimTrac currently conducts nationally coordinated criminal history checks through the National Police Checking Service (NPCS). The NPCS provides accredited organisations with timely and accurate police history information, helping the organisation make informed decisions about potential employment of the individual subject to the check. Police history information may include charges, court convictions, good behaviour bonds or other court orders, matters awaiting court hearing, or traffic offences. The service enables controlled access to disclosable police history information from all Australian police agencies. A police check can be used for a number of purposes, including to screen employees applying for employment that involves working with children and vulnerable groups. Police agencies may

also seek criminal history checks directly from CrimTrac for the purpose of the administration of justice, such as screening potential jurors. These checks do not require the subject's consent.

Except in the cases of checks for police for the administration of justice, CrimTrac can only disclose police checks to accredited organisations. The NPCS Terms of Service (**Attachment A**), which are available on the CrimTrac website, provide that an accredited organisation must not request a police check unless the individual subject to the check has provided informed consent. An accredited organisation is also required to provide the police history check result to the individual subject to the check. This gives the individual an opportunity to verify the check result and submit a dispute if necessary.

The CrimTrac CEO has the role of approving accredited organisations on the advice of the CrimTrac Board (comprised of the Police Commissioner from each state and territory, the Chief Police Officer of the ACT, the AFP Commissioner and a nominated representative from the Commonwealth Attorney-General's Department). When an application to become an accredited agency is submitted, the CrimTrac CEO consults with state and territory police agencies.

Extensive guidance on the types of bodies that may be eligible to become accredited organisations is publically available on the CrimTrac website. It provides that an accredited organisation must:

- be an Australian registered business
- commit to submitting at least 500 nationally coordinated police checks over a three year period
- implement the required security management measures contained in the Information Technology – Security Management document (also publically available on the CrimTrac website).

CrimTrac currently has arrangements with in excess of 200 accredited organisations, which include Australian government agencies, private sector businesses, not-for-profit organisations and screening units for working with children or vulnerable people.

Arrangements following a merger

The Bill would amend the *Australian Crime Commission Act 2002* to merge the functions of CrimTrac into the Australian Crime Comission.

Item 17 of the Bill would insert new subsection 46A(5) to provide that the ACC CEO may approve a body of the Commonwealth, a state or territory, or any other body or body as an accredited body for the purposes of receiving nationally coordinated criminal history checks. Subsection 46A(6) provides that the ACC CEO must act in accordance with any policy or direction given by the ACC Board when deciding whether to approve a body or organisation under subsection 46A(5). Subsection 46A(7) provides that an instrument approving a body or organisation as an accredited body is not a legislative instrument.

These arrangements are designed to reflect the current CrimTrac arrangements.

Importantly, the provision of nationally coordinated criminal history checks will continue to occur on the basis that the individual to which the police information relates will have to consent to the provision of that information to an accredited agency. The current NPCS

Terms of Service will continue to apply and the guidance available on the website will be transitioned to the website of the merged agency.

1. ***Should the legislation contain more guidance in relation to the types of bodies that may access nationally coordinated criminal history checks under subsections 46A(5), (6) and (7)?***

Information provided by a nationally coordinated criminal history check is collected from state and territory police. It is appropriate that the merged agency Board – which will include all current CrimTrac board members and six heads of Commonwealth agencies – maintains control of, and can limit the release of, the specific type of national policing information contained in nationally coordinated criminal history checks, by providing guidance to the ACC CEO. The Board is very experienced in dealing with national policing information and has extensive knowledge about which bodies would or would not be suitable to access nationally coordinated criminal history checks under subsections 46A(5) and (6).

2. ***Should directions issued by the ACC Board in relation to accreditation under subsections 46A(5), (6) and (7) be subject to Parliamentary oversight and disallowance?***

Given the large number of accredited agencies, Parliamentary oversight and disallowance of the Board's directions is likely to be onerous and would add uncertainty to the accreditation process.

Further, the ACC and its Board are already subject to a comprehensive oversight regime. The ACC Board reports to the Inter-Governmental Committee on the ACC, which comprises police ministers from all jurisdictions. The ACC is also subject to review and monitoring by the Parliamentary Joint Committee on Law Enforcement. These bodies have extensive expertise on the ACC, its functions, statutory regime and secrecy provisions, making them the most appropriate forums to monitor the ACC Board's directions about approving accredited bodies.

Therefore, the Government does not consider that additional Parliamentary oversight of Board decisions is warranted.

3. ***Should the legislation contain guidance about the setting of limits and conditions for s59AAA disclosures and, if not, should the setting of such limits and conditions be, at least, subject to disallowance?***

Item 30 would insert a new section 59AAA to enable the merged agency to disclose nationally coordinated criminal history checks to accredited bodies or to the person to whom the check relates, if:

a) disclosing the information would not be contrary to a Commonwealth, state or territory law that would otherwise apply, and
b) disclosing the information would not be contrary to any conditions or restrictions determined by the Board in relation to providing nationally coordinated criminal history checks.

This provision is linked with new paragraph 7C(1)(gd), under which the Board may determine any conditions or restrictions that the merged agency must comply with in providing nationally coordinated criminal history checks. Together, the provisions are

intended to enable the Board to play a role in limiting or restricting the disclosure of this specific type of national policing information, if it chooses to do so.

Information disclosed by a nationally coordinated criminal history check is currently sourced from state and territory police databases so it is appropriate that the Board, which includes all state and territory police representatives, has the power to issue a direction about the disclosure of this information, if it wishes. This will maintain the Board's power to limit and restrict access to the specific type of national policing information.

The Government considers that the inclusion of detailed guidance about any limits and conditions in legislation would be unnecessary and inappropriate and would limit the Board's flexibility in dealing with national policing information.

Subjecting these limits and conditions to disallowance would be an unnecessary administrative burden that could delay the provision of nationally coordinated criminal history checks to accredited bodies and to individuals.

The Government considers that the ACC's existing and comprehensive oversight regime provides appropriate assurance that the ACC Board will issue reasonable and appropriate directions to the ACC CEO about the type of bodies that can receive nationally coordinated criminal history checks and the disclosure of this information.

I trust this information is of assistance to the Committee.

Should your office required any further information, the relevant adviser in my office is David Hughes, who can be contacted on (02) 6277 7290.

Yours sincerely

Australian Government

CRIMTRAC

TERMS OF SERVICE

for controlled access by duly Accredited Organisations to the National Police Checking Service

Copyright Notice

CrimTrac Agency
GPO Box 1573
Canberra City ACT 2601

Content

© Commonwealth of Australia 2014

With the exception of the Commonwealth Coat of Arms, any material protected by a trade mark, and where otherwise noted, this work is licensed under a Creative Commons Attribution 3.0 Australia licence (http://creativecommons.org/licenses/by/3.0/au/).

The details of the relevant licence conditions are available on the Creative Commons website (accessible using the links provided) as is the full legal code for the CC BY 3 AU licence.

Use of the Coat of Arms

The terms under which the Coat of Arms can be used are detailed on the following website: http://www.itsanhonour.gov.au/coat-arms/.

Content from this website should be attributed as the CrimTrac Agency.

Version: 2.0

Table of contents

Introduction

CrimTrac is the national information sharing service for Australia's police and law enforcement agencies.

In partnership with the Australian police agencies, CrimTrac delivers the National Police Checking Service to provide access to police history information in accordance with relevant Australian legislation and with the informed consent of the applicant.

The National Police Checking Service provides Australian police and accredited organisations with police history information to support processes assessing the suitability of people applying for employment, Australian citizenship, appointment to positions of trust, volunteer service, or for various licensing or registration schemes.

Organisations accredited by CrimTrac to access the Service do so pursuant to these Terms of Service.

1 Context and Term

1.1 Context of this Agreement

1.1.1 Every Accredited Organisation enters into an Agreement with the Commonwealth, represented by CrimTrac, for access to the National Police Checking Service. The Agreement consists of these Terms of Service and the Accredited Organisation's Schedule. Provisions regarding the interpretation of this Agreement are contained in clause 9.

1.1.2 **An Accredited Organisation must agree to these Terms of Service in order to access the Service, and must not use or access the Service otherwise. By executing the Schedule, an Accredited Organisation confirms its understanding and commitment to comply fully with this Agreement and, in particular, the applicable provisions of the *Privacy Act 1988* (Cth).**

1.1.3 These Terms of Service may be amended by CrimTrac from time to time. CrimTrac will notify all Accredited Organisations of any changes (whether material or not) with at least three (3) months' notice unless clause 2.3.4 applies.

1.2 Term of this Agreement

1.2.1 This Agreement commences on the Commencement Date and, unless terminated earlier, will remain in force for three (3) years.

1.3 Memorandum of Understanding for Commonwealth Government Agencies

1.3.1 This clause 1.3 only applies if the Accredited Organisation is a Commonwealth Government Agency.

1.3.2 This Agreement is executed as a memorandum of understanding. The Parties acknowledge that each Party is part of the Commonwealth and does not intend to enter into a legally binding agreement with the other. The Parties instead commit to working together in good faith to implement the Provisions of this Agreement.

1.3.3 Notwithstanding clause 7, the Parties acknowledge that Confidential Information may be disclosed between the Parties and that the existing scheme of obligations on Commonwealth Government Agency employees is reasonably sufficient to maintain the confidential nature of this information.

1.3.4 Any dispute arising under or in connection with this Agreement will be dealt with by negotiation between the Parties.

1.4 Provision of the Service to Customers

1.4.1 This clause 1.4 only applies if the Accredited Organisation has been authorised by CrimTrac to provide the Service to one or more of the Accredited Organisation's clients ("**Customers**"). Each Customer must be a distinct legal entity capable of entering into a contract.

1.4.2 The Accredited Organisation must enter into a written agreement with each Customer related to the provision of the Service (each a "**Customer Contract**"). Upon CrimTrac's request, the Accredited Organisation must produce a copy of any or all of its Customer Contracts. The Accredited Organisation must ensure that each Customer Contract:

a. requires the Customer to act as if it were an APP Entity;

b. gives effect to, and is not inconsistent with, the Accredited Organisation's obligations and CrimTrac's rights under this Agreement, especially in relation to the protection of Personal Information (clause 2.2), the collection of the Applicant's Informed Consent (clause 3.2) and the inclusion of an acknowledgement regarding the limitations of a National Police History Check (clause 3.3.2); and

c. grants CrimTrac a right of access to the Customer's premises (and to records and accounts in connection with the handling of Police History Information, including the right to copy) which CrimTrac must exercise reasonably and subject to the Customer's reasonable safety and security requirements.

1.4.3 The Accredited Organisation must not request a National Police History Check from CrimTrac on behalf of a Customer unless the Accredited Organisation or the Customer has collected an Informed Consent from the Applicant.

2 The Accredited Organisation's responsibilities

2.1 Compliance with this Agreement

2.1.1 The Accredited Organisation (including its Personnel) must use the Service strictly in accordance with this Agreement.

2.1.2 From time to time information in and access to the National Police Checking Service may be subject to technical changes as well as changes in Commonwealth policy or law. To the extent that it is necessary to ensure the Accredited Organisation can receive continued access to the Service, the Accredited Organisation (including its Personnel) must comply with any Commonwealth policy or change in technical requirements of which CrimTrac provides reasonable notice.

2.2 Protection of Personal Information

2.2.1 This clause 2.2 is a material clause of the Agreement and the obligations outlined in this clause 2.2 survive the expiration of this Agreement. The Accredited Organisation must take reasonable and practical steps to ensure compliance by its Personnel with this clause 2.2 and must provide evidence of that compliance to CrimTrac upon CrimTrac's request at any time. For the avoidance of doubt, this includes the Accredited Organisation's Subcontractor(s). Moreover, the Accredited Organisation must notify CrimTrac immediately if it becomes aware of a breach or possible breach by any person of any of the Accredited Organisation's obligations under this clause 2.2.

2.2.2 The *Privacy Act 1988* (Cth) protects every individual's Personal Information (information that identifies or could reasonably identify that individual). The Australian Privacy Principles regulate the handling of Personal Information by both Australian Government Agencies and businesses. **Irrespective of whether or not the Accredited Organisation would otherwise be bound, by entering into this Agreement the Accredited Organisation agrees to be bound by the *Privacy Act 1988* (Cth) as an APP Entity.**

2.2.3 The Accredited Organisation must, in conducting National Police History Checks and using the Service generally:

a. use or disclose Personal Information obtained during the course of this Agreement only for the purposes of this Agreement;

b. comply with any directions, guidelines, determinations or recommendations of CrimTrac, to the extent that they are consistent with the Australian Privacy Principles;

c. not do any act or engage in any practice which, if done or engaged in by CrimTrac, would be a breach of the *Privacy Act 1988* (Cth), in particular, the Australian Privacy Principles;

d. implement safeguards to keep Police History Information secure;

e. not summarise, précis or otherwise alter Police History Information provided by CrimTrac to the Accredited Organisation; and

f. not retain a National Police History Check result or an Applicant's Informed Consent for longer than twelve (12) months following release of the result, unless legislation applying to the Accredited Organisation mandates a longer document retention period.

2.2.4 The Accredited Organisation must, on request by CrimTrac at any time, promptly provide CrimTrac with the Accredited Organisation's privacy policy.

2.3 Claims for payment

2.3.1 CrimTrac is entitled to charge the Accredited Organisation the following Fees for its use of the Service:

a. $23.00 (GST exclusive) for each National Police History Check (Standard); and

b. $7.00 (GST exclusive) for each National Police History Check (Volunteer).

2.3.2 CrimTrac is entitled to submit claims for payment to the Accredited Organisation and each claim will be in the form of a valid tax invoice, contain the number of National Police History Checks requested by the Accredited Organisation during the previous month and include the amount payable calculated in accordance with the applicable Fees.

2.3.3 The Accredited Organisation must pay claims for payment made in accordance with clause 2.3.2 within thirty (30) days of the date of the claim.

2.3.4 CrimTrac may, at its absolute discretion, adjust the Fees by giving the Accredited Organisation six (6) months' written notice.

2.4 Taxes, duties and government charges

2.4.1 In this clause 2.4 the terms '**supply**', '**taxable supply**', '**tax invoice**', '**GST**', '**input tax credit**' and '**decreasing adjustment**' have the same meaning as given in the *A New Tax System (Goods and Services Tax) Act 1999* (Cth).

2.4.2 The Accredited Organisation must pay all taxes, duties and government charges imposed or levied in connection with the performance of this Agreement.

2.4.3 Unless otherwise indicated, all consideration for any supply made under this Agreement is exclusive of GST imposed on the supply. If CrimTrac makes a taxable supply to the Accredited Organisation under this Agreement, on receipt of a tax invoice from CrimTrac, the Accredited Organisation must pay, without setoff, an additional amount to CrimTrac equal to the GST imposed on the supply in question.

2.4.4 No Party may claim from the other Party under this Agreement any amount which the first Party may claim as an input tax credit or decreasing adjustment.

2.5 Indemnity

2.5.1 Unless clause 1.3 applies, the Accredited Organisation indemnifies the Commonwealth and the Commonwealth's Personnel from and against any:

a. loss or liability incurred by the Commonwealth or its Personnel;

b. loss of or damage to property of the Commonwealth or its Personnel; or

c. loss or expense incurred by the Commonwealth or its Personnel in dealing with (including investigation of, responding to and settlement of) any claim against it or them including legal costs and expenses on a solicitor/own client basis and the cost of time spent, resources used or disbursements paid by the Commonwealth,

arising from:

d. any breach of the Accredited Organisation's obligations or warranties in this Agreement; or any act or omission by the Accredited Organisation or the Accredited Organisation's Personnel in connection with this Agreement, where there was fault (including any negligent or other tortious or unlawful act or omission) on the part of the person whose conduct gave rise to that liability, loss, damage or expense; and

e. if clause 1.4 applies, any act or omission on the part of a Customer that, were that act or omission performed by the Accredited Organisation, would constitute a breach of this Agreement, or any breach by a Customer of a Customer Contract or any act or omission involving fault on the part of a Customer, or its equivalent to Personnel, in connection with a Customer Contract.

2.5.2 The Accredited Organisation's liability to indemnify the Commonwealth and the Commonwealth's Personnel under this Agreement will be reduced proportionately to the extent that any negligent or other tortious or unlawful act or omission of the Commonwealth or its Personnel contributed to the relevant liability, loss, damage or expense.

2.5.3 The right of the Commonwealth or its Personnel to be indemnified under this Agreement is in addition to, and not exclusive of, any other right, power or remedy provided by law, and does not entitle the Commonwealth or its Personnel to be compensated in excess of the amount of the relevant liability, loss, damage, or expense.

2.6 Corporate trustees

2.6.1 If any trust of which the Accredited Organisation is a trustee has any relevance to matters within the scope of this Agreement, without limiting in any way the Accredited Organisation's obligations under this Agreement, the Accredited Organisation represents and warrants that it has the power and authority as trustee to perform relevant obligations and has a right of indemnity from the trust assets in relation to all relevant matters.

3 The National Police Checking Service

3.1 Provision and use of the Service

3.1.1 The Accredited Organisation must use the Service only:

a. through the secure network established by CrimTrac for the Service; and

b. to request National Police History Checks for the Authorised Check Purposes set out in the Schedule;

and otherwise in accordance with this Agreement.

3.1.2 Subject to the Accredited Organisation's compliance with this Agreement, CrimTrac will process a request for a National Police History Check relating to an Applicant upon receipt from the Accredited Organisation of the following information:

a. the Applicant's Informed Consent for CrimTrac to undertake a National Police History Check on the Applicant;

b. the Applicant's surname and given name(s), and all names under which the Applicant is or has been known;

c. the Applicant's date and place of birth;

d. the Applicant's sex;

e. the Applicant's residential address(es) for the past five (5) years;

f. if available, the Applicant's driver's licence details and/or firearms licence details;

g. the position title, occupation or entitlement being sought by the Applicant; and

h. the proposed place of work and whether contact with children or vulnerable groups such as the elderly is likely.

3.1.3 The Accredited Organisation must ensure that the Applicant is notified of the Applicant's National Police History Check result as soon as practicable after the Accredited Organisation (or Customer, if clause 1.4 applies) receives that result.

3.2 Informed Consent

3.2.1 The Accredited Organisation must not request a National Police History Check from CrimTrac under clause 3.1.2 unless the Accredited Organisation (or Customer, if clause 1.4 applies) has collected an Informed Consent from the Applicant.

3.2.2 For the purposes of this Agreement, an Informed Consent is a consent form completed and signed by an Applicant that sets out or contains at a minimum:

a. the information listed in clause 3.1.2 as well as the Applicant's signature;

b. a statement or endorsement confirming that the Accredited Organisation (or Customer, if clause 1.4 applies) is satisfied as to the correctness of the Applicant's identity and has sighted original or certified copies of the Applicant's identity documents in accordance with clause 3.2.3;

c. the meaning or nature of a National Police History Check;

d. the purpose(s) for which the Applicant's Personal Information is being collected and the purpose(s) for which the National Police History Check is being undertaken;

e. any person to whom, or organisation (including its Australian Business Number) to which, Personal Information (including Police History Information) may be disclosed and in what circumstances (including CrimTrac, Australian police agencies, third parties);

f. any law which requires that the Applicant's Personal Information be collected and the consequences of non-compliance;

g. the likelihood of the Applicant's Personal Information being disclosed to overseas recipients and, if so, to whom and in which country or countries;

h. an acknowledgement that the Applicant understands that their Personal Information may be used for general law enforcement purposes;

i. advice to the Applicant that the Applicant may dispute the Police History Information contained in their National Police History Check by contacting the Accredited Organisation in the first instance;

j. the Accredited Organisation's full name and contact details, including the name and contact details of its privacy officer; and

k. advice that the CrimTrac privacy officer can be contacted on (02) 6268 7000 or privacy@crimtrac.gov.au or GPO Box 1573 Canberra City ACT 2601.

CrimTrac provides a model Informed Consent form to assist Accredited Organisations comply with this clause 3.2.2.

3.2.3 When reviewing an Applicant's Informed Consent form, the Accredited Organisation (or Customer, if clause 1.4 applies) must be satisfied as to the Applicant's identity and sight original or certified copies of the following identity documents relating to the Applicant and totalling at least 100 points:

CATEGORY A—Each document is worth 70 points
• Birth Certificate • Australian Passport (current, or expired within the previous two years, but not cancelled) • Australian Citizenship Certificate • International Passport (current, or expired within the previous two years, but not cancelled) • Other document of identity having same characteristics as a passport e.g. diplomatic/ refugee (Photo or Signature)
CATEGORY B—The first document is worth 40 points and each additional document is worth 25 points
• Current Licence or Permit (Government Issued) • Working With Children/Teachers Registration Card • Aviation Security Identification Card/Maritime Security Identification Card • Public Employee Photo ID Card (Government Issued) • Department of Veterans' Affairs Card • Centrelink Pensioner Concession Card or Health Care Card • Current Tertiary Education Institution Photo ID • Reference from a medical practitioner (must have known the applicant for a period of at least 12 months)

CATEGORY C—Each document is worth 25 points
• Birth Extract • Foreign/International Driver's Licence • Proof of Age Card (Government Issued) • Medicare Card/Private Health Care Card • Council Rates Notice • Property Lease/Rental Agreement • Property Insurance Papers • Australian Tax Office Assessment • Superannuation Statement • Seniors Card • Electoral Roll Registration • Motor Vehicle Registration or Insurance Documents • Professional or Trade Association Card If relied upon, the following documents must be from different organisations: • Utility Bills (e.g. Telephone, Gas, Electricity, Water) • Credit/Debit Card • Bank Statement/Passbook

In addition to the requirement that the documents supplied equal or exceed 100 points, the combination of the Applicant's identity documents must include the Applicant's full name, date of birth, at least one document from either Category A or Category B, and a photograph of the Applicant. If the Applicant does not have an identity document containing a photograph, the Applicant must submit a passport style photograph that has been certified by a person listed in Schedule 2 of the *Statutory Declarations Regulations 1993* (Cth).

There are special provisions that apply to the following categories of Applicants who may be unable to meet the identity requirements in this clause 3.2.3: recent arrivals (persons that have been in Australia for 6 weeks or less), Aboriginal and Torres Strait Islander residents in remote areas and communities, and persons under 18 years of age. Accredited Organisations must meet the minimum requirements for these categories contained in the most recent version of CrimTrac's model Informed Consent form.

3.3 Limitations of the Service

3.3.1 The Accredited Organisation acknowledges and agrees that CrimTrac makes the information contained in a National Police History Check available for use on the following conditions:

a. CrimTrac makes no representation or warranty of any kind without limitation in respect to accuracy; and

b. CrimTrac does not accept responsibility or liability for any error or omission in the information.

3.3.2 The Accredited Organisation must ensure that any record of Police History Information provided to any person under this Agreement includes the following disclaimer:

LIMITATIONS ON ACCURACY AND USE OF THIS INFORMATION

1. *The accuracy and quality of this National Police History Check depends on accurate identification of the Applicant (including aliases) and information provided in the application form and the comprehensiveness of police records.*
2. *While every care has been taken by CrimTrac to conduct a search of Police History Information held by it and Australian police agencies that relate to the Applicant, this report may not include all Police History Information relating to the Applicant. Reasons for Police History Information being excluded from the report include the operation of laws that prevent disclosure of certain Police History Information, or that the Applicant's record is not identified by the search process across the Police History Information holdings.*
3. *The National Police History Check is a point in time check and should not be relied upon for an unreasonable amount of time.*
4. *The Applicant must be notified of their National Police History Check result and provided with a reasonable opportunity to respond to or validate the information in this report.*
5. *To the extent permitted by law, neither CrimTrac nor Australian police agencies accept responsibility or liability for any error or omission in the information.*

THE NATIONAL POLICE HISTORY CHECK PROCESS

The information in this report has been obtained according to the following process:

a) CrimTrac searching a central index for potential matches with the name(s) of the Applicant;

b) CrimTrac and the relevant Australian police agencies comparing name matches with Police History Information held in Australian police records;

c) The relevant Australian Police Agency identifying any Police History Information held in their police records and releasing the information subject to relevant spent convictions, non-disclosure legislation or information release policies;

d) CrimTrac providing a result of the National Police History Check to [the Accredited Organisation] indicating that a record of Police History Information relating to the Applicant is held or not; and

e) CrimTrac providing that Police History Information to [the Accredited Organisation].

3.4 CrimTrac's rights to suspend the Service

3.4.1 CrimTrac may, at its discretion and in addition to any other rights it has under this Agreement, suspend or reduce the Accredited Organisation's level of access to the Service where:

a. the Accredited Organisation has breached a Provision of this Agreement; or

b. CrimTrac reasonably suspects that the Accredited Organisation has committed or may commit a breach of a Provision of this Agreement,

until such time as the breach by the Accredited Organisation has been remedied to CrimTrac's satisfaction.

3.4.2 The Accredited Organisation must continue to perform its obligations under this Agreement notwithstanding any suspension or reduction of the Service.

4 Parties' relationship and Personnel

4.1 Provision of information and liaison

4.1.1 The Accredited Organisation must at no cost to CrimTrac:

a. liaise with and provide CrimTrac with any information that it reasonably requires, including information regarding the Accredited Organisation's Personnel, financial viability and compliance with the terms of this Agreement; and

b. comply with all of CrimTrac's reasonable requests, directions and monitoring requirements,

in relation to this Agreement or any review or audit of the Accredited Organisation's compliance with this Agreement that is conducted by or for the Commonwealth.

4.2 Relationship of the Parties

4.2.1 Nothing in this Agreement makes the Accredited Organisation an employee, partner or agent of CrimTrac, or gives the Accredited Organisation any power or authority to bind or represent CrimTrac in any way or for any purpose. The Accredited Organisation must not, and must ensure that its Personnel do not:

a. misrepresent themselves as being CrimTrac's officer, employee, partner or agent, or as otherwise able to bind or represent CrimTrac; or

b. engage in any misleading or deceptive conduct in relation to the Service including conduct that is likely to mislead or deceive any person in relation to the Service.

4.3 Notices

4.3.1 A Party ('First Party') giving notice to the other Party under this Agreement must do so in writing and that notice must be signed by the First Party's Authorised Officer, marked for the attention of the other Party's Authorised Officer and hand delivered or sent by prepaid post or email to the other Party's address for notices.

4.3.2 A notice given in accordance with clause 4.3.1 is received:

a. if hand delivered or if sent by pre-paid post, on delivery to the relevant address; or

b. if sent by email, when received by the addressee or when the sender's computer generates written notification that the notice has been received by the addressee, whichever is earlier.

4.4 Use of CrimTrac or police agency logos

4.4.1 The Accredited Organisation must not create Material which uses a CrimTrac logo or any branding or logo associated with an Australian police agency for the purposes of marketing or promotion of the Accredited Organisation.

4.5 Commonwealth collection of Personal Information

4.5.1 Personal Information may be collected from or about the Accredited Organisation (including its Personnel). The Accredited Organisation must notify its Personnel that CrimTrac may collect and use their Personal Information for the purposes of administering, monitoring, reviewing, promoting and evaluating this Agreement.

4.6 The Accredited Organisation's Personnel

4.6.1 The Accredited Organisation must always have an Authorised Officer whose contact details are registered with CrimTrac.

4.6.2 The Accredited Organisation must ensure that its Personnel are of good fame and character and will act in all circumstances in a fit and proper manner in relation to any Personal Information or Police History Information to which they have access under this Agreement.

4.6.3 The Accredited Organisation must, at all times, restrict its Personnel's access to Police History Information to a strictly 'need to know' basis.

4.7 Legal process consultation

4.7.1 Where Police History Information is subject to any legal processes including a subpoena or a freedom of information request, the Accredited Organisation will consult to the extent allowable under law with CrimTrac upon receipt of such action or application and again prior to its finalisation.

5 Access to premises and information

5.1 Access to premises and Material

5.1.1 Subject to clause 5.1.4, the Accredited Organisation must allow access to sites or premises at which records and Materials associated with this Agreement are stored for the following officers:

a. the CrimTrac Authorised Officer;

b. the Auditor-General (established under the *Auditor-General Act 1997* (Cth));

c. the Privacy Commissioner or statutory appointee administering the *Privacy Act 1988* (Cth);

d. the Commonwealth Ombudsman (established under the *Ombudsman Act 1976* (Cth)); and

e. any person authorised by a person described in clause 5.1.1.a to 5.1.1.d.

5.1.2 Subject to clause 5.1.4, the Accredited Organisation must arrange for the persons listed in clause 5.1.1 to inspect and copy Materials in the Accredited Organisation's possession or control for purposes associated with this Agreement or any review of the Accredited Organisation's performance of this Agreement.

5.1.3 The Accredited Organisation must ensure that Subcontracts require Subcontractors to give the persons listed in clause 5.1.1 access to the Subcontractor's premises, and to records and Materials in connection with the performance of work under the Subcontract, including rights to inspect and copy Materials equivalent to those in clause 5.1.2.

5.1.4 The rights referred to in clauses 5.1.1 and 5.1.2 are, wherever practicable, subject to:

a. CrimTrac providing the Accredited Organisation (or, where applicable, a Subcontractor) with at least three (3) business days' prior notice; and

b. the Accredited Organisation's (or, where applicable, a Subcontractor's) reasonable security requirements or codes of behaviour,

except where a person listed in clause 5.1.1 or their delegate believes that there is a suspected or actual breach of law.

5.1.5 Nothing in this Agreement limits or restricts in any way any duly authorised function, power, right or entitlement of the persons listed in clause 5.1.1 or their respective delegates.

5.2 Access to documents

5.2.1 If the Commonwealth receives a request for access to a document created by or in the possession of the Accredited Organisation or a Subcontractor that relates to this Agreement, CrimTrac may at any time by notice require the Accredited Organisation to provide, or arrange for the provision of, the document to CrimTrac and the Accredited Organisation must, at no additional cost to the Commonwealth, promptly comply with the notice.

5.2.2 If the Accredited Organisation receives a request for access to a document in its possession (including in the possession of its Personnel and/or Subcontractor) that relates to this Agreement, the Accredited Organisation must consult with CrimTrac upon receipt of the request.

5.2.3 The Accredited Organisation must include in any Subcontract relating to the performance of this Agreement provisions that will enable the Accredited Organisation to comply with its obligations under this clause 5.2.

6 Intellectual Property

6.1 Ownership of Police History Information

6.1.1 Intellectual Property in Police History Information is owned by the Commonwealth and the Australian police agencies. Nothing in this Agreement affects the ownership of Intellectual Property in Police History Information (including any copy thereof) provided to the Accredited Organisation. CrimTrac grants to the Accredited Organisation a royalty-free, non-exclusive licence to use and communicate Police History Information in accordance with this Agreement.

6.2 No change to ownership of other relevant documents

6.2.1 Nothing in this Agreement affects the Commonwealth's ownership of Intellectual Property in any other Material relevant to or associated with the Service or this Agreement, including branding, graphic design, policies, guidance materials, certificates and forms.

7 Confidentiality

7.1 Confidential Information not to be disclosed

7.1.1 Subject to clause 7.2, a Party must not disclose Confidential Information of the other Party without the prior written consent of that other Party, who may give that consent subject to conditions.

7.2 Exceptions to non-disclosure

7.2.1 A Party can disclose Confidential Information of the other Party to the extent that it:

a. is disclosed by the Party to its Personnel solely in order to comply with obligations, or to exercise rights, under this Agreement;

b. is disclosed by the Party to its internal management (including advisers) solely to enable effective management or auditing of Agreement-related activities;

c. is disclosed by the Party to its responsible Minister;

d. is disclosed by the Party, in response to a request by a House or a Committee of the Parliament of the Commonwealth of Australia or State and Territory Parliament;

e. is shared by CrimTrac within the Commonwealth, or with another Government Agency, where this serves the Commonwealth's or the Government Agency's legitimate interests;

f. is required by law or statutory or portfolio duties to be disclosed;

g. is disclosed by CrimTrac in order to protect the health or safety of any person; or

h. is in the public domain otherwise than due to a breach of this clause 7.

7.2.2 Where a Party discloses Confidential Information to another person under clauses 7.2.1.a to 7.2.1.d and 7.2.1.g, the disclosing Party must notify the receiving person that the information is confidential.

7.2.3 In the circumstances referred to in clauses 7.2.1.a and 7.2.1.b, the disclosing Party agrees not to provide the information unless the receiving person agrees to keep the information confidential (subject to the exceptions in this clause 7).

7.3 Security of Commonwealth's Confidential Information

7.3.1 The Accredited Organisation agrees to secure all of the Commonwealth's Confidential Information (including Police History Information) against loss and unauthorised access, use, modification or disclosure.

7.3.2 The Accredited Organisation may wish to provide Applicants with the opportunity to submit Personal Information electronically. If so, the Accredited Organisation must secure Personal Information belonging to Applicants against loss and unauthorised access, use, modification or disclosure, and notify the Applicant of these risks.

7.4 Written undertakings

7.4.1 The Accredited Organisation must, on request by CrimTrac at any time, promptly arrange for the Accredited Organisation's Personnel to give a written undertaking in a form acceptable to CrimTrac relating to the use and non-disclosure of the Commonwealth's Confidential Information (including Police History Information).

7.5 Period of Confidentiality

7.5.1 The obligations under this clause 7 will continue, notwithstanding the expiry or termination of this Agreement:

a. in relation to an item of information described in the Schedule—for the period set out in respect of that item or, if no such period is specified, in perpetuity; and

b. in relation to any item of information agreed by the Parties to be Confidential Information and not described in the Schedule—for the period agreed by the Parties in writing in respect of that item or, if no such period is agreed by the Parties, in perpetuity.

7.5.2 The obligations contained in this clause 7 are in addition to those specified in clauses 2.2 and 5.2.

8 Termination and disputes

8.1 Termination or reduction in scope for convenience

8.1.1 CrimTrac may by notice, at any time and in its absolute discretion, terminate this Agreement or reduce the scope of the Agreement (including by reducing or removing Authorised Check Purposes) immediately.

8.1.2 The Accredited Organisation will not be entitled to any compensation whatsoever including for loss of prospective profits or loss of any benefits that would have been conferred on the Accredited Organisation if the termination or reduction had not occurred. CrimTrac shall only be liable for repayment of any outstanding National Police History Checks requested by the Accredited Organisation prior to the effective date of termination.

8.1.3 This clause 8.1 does not affect the Commonwealth's other rights under this Agreement or otherwise at law.

8.2 Termination for default

8.2.1 CrimTrac may terminate this Agreement immediately by notice to the Accredited Organisation if any of the following termination events occur:

a. the Accredited Organisation breaches any Provision of this Agreement and CrimTrac reasonably considers that the breach cannot be rectified;

b. the Accredited Organisation breaches any Provision of this Agreement and does not rectify the breach within 14 days after receipt of CrimTrac's notice to do so;

c. CrimTrac considers that its decision to accredit and grant the Accredited Organisation access to the Service was affected by a statement in its accreditation application that was incorrect, incomplete, false or misleading;

d. CrimTrac is satisfied on reasonable grounds that the Accredited Organisation is unable or unwilling to satisfy the terms of this Agreement;

e. the Accredited Organisation comes under any form of administration or assigns its rights otherwise than in accordance with this Agreement;

f. the Accredited Organisation is unable to pay all its debts as and when they become payable or fails to comply with a statutory demand;

g. proceedings are initiated with a view to obtaining an order for winding up the Accredited Organisation;

h. if the Accredited Organisation is a local government organisation, the relevant State Government takes action to cease the Accredited Organisation's operations and/or to amalgamate them with the operations of another local government organisation;

i. the Accredited Organisation becomes bankrupt or enters into a scheme of arrangement with creditors;

j. anything analogous to, or of a similar effect to, anything described in clauses 8.2.1.e to 8.2.1.i occurs in respect of the Accredited Organisation; or

k. another Provision of this Agreement allows for termination under this clause 8.2.

8.2.2 If a purported termination by CrimTrac under this clause 8.2 is determined by a competent authority not to be properly a termination under this clause 8.2, then that termination by CrimTrac will be deemed to be a termination for convenience under clause 8.1 with effect from the date of the notice of termination referred to in this clause 8.2.

8.2.3 This clause 8.2 does not affect the Commonwealth's other rights under this Agreement or otherwise at law.

8.3 Procedure for dispute resolution

8.3.1 Except for the circumstances set out in clause 8.3.2, a Party must not commence any legal proceedings in respect of any dispute arising under this Agreement until the following procedure has been followed:

a. the Party claiming that there is a dispute will send the other Party a notice setting out the nature of the dispute ('**Dispute Notice**');

b. the Parties will try to resolve the dispute through direct negotiation, including by referring the matter to persons who have the authority to intervene and direct some form of resolution;

c. if:

i. there is no resolution of the dispute within 30 days from the date that the Dispute Notice was received;

ii. there is no agreement on submission of the dispute to mediation or some alternative dispute resolution procedure within 30 days from the date that the Dispute Notice was received; or

iii. the Parties agree to submit to mediation or some other form of alternative dispute resolution procedure but there is no resolution within 30 days of that submission (or such extended time agreed upon by the Parties),

then, either Party may commence legal proceedings.

8.3.2 Clause 8.3.1 does not apply to the following circumstances:

a. either Party commences legal proceedings for urgent interlocutory relief;

b. action is taken by CrimTrac under, or purportedly under clause 5, clause 8.1 or clause 8.2; or

c. an authority of the Commonwealth, a State or Territory is investigating a breach or suspected breach of the law by the Accredited Organisation.

8.3.3 Each Party will bear its own costs of complying with this clause 8.3, and the Parties will bear equally the cost of any person engaged under clause 8.3.1.b.

8.3.4 Despite the existence of a dispute, both Parties must (except to the extent notified by the other Party not to do so) continue to perform their respective obligations under this Agreement.

9 Interpretation

9.1 General interpretation of this Agreement

9.1.1 In this Agreement, unless the contrary intention appears:

a. clause headings are inserted for convenient reference only and have no effect in limiting or extending the language of provisions to which they refer;

b. words in the singular include the plural and vice versa;

c. words importing a gender include any other gender;

d. the word 'person' includes an individual, partnership, a body (whether corporate or otherwise) and Government Agencies;

e. if the last day of any period prescribed for the doing of an action falls on a day which is not a business day, the action shall be done no later than the end of the next business day;

f. a reference to any statute is to a statute of the Commonwealth, State or Territory of Australia, as amended from time to time, and includes a reference to any subordinate legislation made under the statute;

g. all references to dollars are to Australian dollars;

h. where any word or phrase is given a defined meaning, any other form of that word or phrase has a corresponding meaning;

i. an uncertainty or ambiguity in the meaning of a Provision of this Agreement will not be interpreted against a Party just because that Party prepared the provision;

j. a reference to the word 'including' in any form is not to be construed or interpreted as a word of limitation; and

k. a reference to a 'clause' is to a clause in this document, a reference to 'Item' is to an Item in the Schedule to this Agreement, and a reference to 'Annexures' is a reference to documents attached to the Schedule.

9.1.2 If there is any conflict or inconsistency, the provisions in documents forming part of this Agreement take priority in the following (descending) order:

a. the Schedule;

b. these Terms of Service;

c. any documents incorporated by reference into the above documents.

9.1.3 This Agreement is governed by the law of the Australian Capital Territory and the Parties submit to the jurisdiction of the courts of the Australian Capital Territory.

9.1.4 This Agreement:

a. records the entire agreement between the Parties about its subject matter; and

b. supersedes all offers, prior representations, communications, statements, understandings, negotiations and agreements, whether oral or written, between the Parties about that subject matter.

9.1.5 A Provision of this Agreement contained in the Accredited Organisation's Schedule may only be varied by the written agreement of both Parties.

9.1.6 If part of this Agreement is found to be invalid, the rest of this Agreement continues in effect as if the invalid part were severed. Any reading down or severance of a particular provision does not affect the other Provisions of this Agreement.

9.1.7 A waiver of any Provision of this Agreement must be agreed to in writing by the Commonwealth's Authorised Officer to be effective. Failure by either Party to enforce a term or condition of this Agreement shall not be construed as in any way affecting the enforceability of that term or condition or this Agreement as a whole.

9.1.8 The Accredited Organisation must not assign, novate or transfer its rights or obligations under this Agreement without CrimTrac's prior written approval.

9.2 Survival

9.2.1 The termination or expiration of this Agreement will not affect the continued operation of any Provision of this Agreement which expressly or by implication from its nature is intended to survive including but not limited to clauses 2.2 (protection of Personal Information), 2.5 (indemnity), 5 (access to premises and information) and 7 (confidentiality).

9.3 Definitions

9.3.1 In this Agreement, unless the contrary intention appears, a term in bold type in this clause 9.3 has the meaning shown opposite it:

Accredited Organisation	means the entity specified as such in the Schedule and includes, where the context permits, its Personnel, administrators, successors and permitted assigns, including any person to whom the Accredited Organisation novates any part of this Agreement;
Agreement	means an agreement between CrimTrac and the Accredited Organisation comprising these Terms of Service and the Schedule, and which is a legally binding contract unless clause 1.3 applies in which case it is a memorandum of understanding;
APP Entity	has the same meaning as given in the *Privacy Act 1988* (Cth);
Applicant	means an individual who provides Informed Consent to a National Police History Check of their name being conducted;
Australian Privacy Principle (APP)	has the same meaning as given in the *Privacy Act 1988* (Cth);
Authorised Check Purpose	means the types/categories of National Police History Checks exhaustively set out in the Schedule that the Accredited Organisation is authorised to perform subject to its compliance with this Agreement;
Authorised Officer	a. in relation to the Accredited Organisation, the person listed in the Schedule; and b. in relation to the Commonwealth, the Director at CrimTrac responsible for managing the National Police Checking Service;
Commencement Date	means the last day on which the Schedule was signed by a Party unless otherwise specified in the Schedule;
Commonwealth	means the Commonwealth of Australia and includes CrimTrac;

Confidential Information	means information that: a. is Police History Information; b. is by its nature confidential, including the name or contact details of any staff member or security information relating to the provision of the Service; c. is described as such in the Schedule; or d. the Parties agree in writing after the Commencement Date is confidential information for the purposes of this Agreement;
CrimTrac	means the Australian Government Agency that is responsible for administering this Agreement and includes the agency's officers, delegates, employees and agents;
Customer	has the meaning as given in clause 1.4.1;
Fees	means the amount(s) payable by the Accredited Organisation for the Services pursuant to clause 2.3;
Government Agency	means any governmental, administrative, fiscal, judicial or quasi-judicial body, department, commission, authority, tribunal, agency or entity;
Informed Consent	has the meaning as given in clause 3.2.2;
Intellectual Property	means: a. all copyright (including rights in relation to phonograms, sound recordings and broadcasts); b. all rights in relation to inventions (including patent rights), plant varieties, registered and unregistered trade marks (including service marks), registered and unregistered designs, circuit layouts; and c. all other rights resulting from intellectual activity in the industrial, scientific, literary or artistic fields but does not include: d. Moral Rights; e. the rights of performers (other than a performer's right of co-ownership of copyright in the sound recording of a Performance); or f. rights in relation to Confidential Information;
Material	means any article or thing in relation to which Intellectual Property rights arise or which incorporates a 'performance' (as defined in the *Copyright Act 1968* (Cth)) or a recording thereof;
Moral Rights	means the following non-proprietary rights of authors of copyright material: a. the right of attribution of authorship or performership; b. the right of integrity of authorship or performership; and c. the right not to have authorship or performership falsely attributed.
National Police Checking Service	means the service established by CrimTrac to provide access to Police History Information, to support processes assessing the suitability of people applying for employment (including positions of trust, volunteer service) or entitlements (including Australian citizenship, licensing or registration schemes);
National Police History Check	means a police history record check on an Applicant carried out in accordance with this Agreement and attracting the Fees;

Party	means a party to this Agreement as specified in the Schedule;
Personal Information	has the meaning given in the *Privacy Act 1988* (Cth);
Personnel	a. in relation to the Accredited Organisation, means the Accredited Organisation's Authorised Officer, each Subcontractor and any officer, employee, contractor, partner, volunteer or agent of the Accredited Organisation or a Subcontractor who collects, views or handles Police History Information or Personal Information in the course of performing their duties in connection with this Agreement; and b. in relation to the Commonwealth, means officers, employees, volunteers, agents or contractors of CrimTrac or any entity that is contracted by CrimTrac other than the persons and entities referred to in paragraph (a) of this definition;
Police History Information	means any information or result released as part of a National Police History Check;
Provision of this Agreement	means a requirement in this Agreement including a requirement in a clause in the Terms of Service and the Schedule;
Schedule	means the document entitled 'Terms of Service Schedule' that must be executed by both Parties and includes any Annexures;
Service	means the National Police Checking Service;
Subcontractor	means any person engaged by the Accredited Organisation to undertake any part of the Accredited Organisation's obligations under this Agreement, and 'Subcontract' means the written agreement between the Accredited Organisation and the Subcontractor; and
Terms of Service	means all of the clauses in this document.

ATTORNEY-GENERAL

CANBERRA

MC15-009261

Senator Helen Polley
Chair
Senate Scrutiny of Bills Committee
Suite1.111
Parliament House
CANBERRA ACT 2600

25 FEB 2016

Dear Senator Polley

Thank you for the letters of 26 November 2015 and 4 February 2016 from the Senate Standing Committee for the Scrutiny of Bills (the Committee) concerning the Counter-Terrorism Legislation Amendment Bill (No. 1) 2015 (Bill).

In Alert Digest No. 13 of 2015, the Committee considered the Bill, and has sought additional advice regarding a number of its components. In response to the Committee's request, I enclose detailed responses to the issues raised in the Digest.

I apologise for not responding sooner, however I wished to ensure that my response to the Committee was informed by my Department's supplementary submission to the Parliamentary Joint Committee on Intelligence and Security of 14 January 2016, as well as the Parliamentary Joint Committee on Intelligence and Security report on the Bill which was released on 15 February 2016.

I trust this information is of assistance to the Committee.

Thank you again for writing on this matter.

Attorney-General's response to the Senate Standing Committee for the Scrutiny of Bills

Alert Digest No. 13 of 2015

Counter-Terrorism Legislation Amendment Bill (No. 1) 2015

Introduced into the Senate on 12 November 2015

Portfolio: Attorney-General

Contents

Introduction

The Counter-Terrorism Legislation Amendment Bill (No. 1) 2015 was introduced into the Senate on 12 November 2015. On 25 November 2015, the Senate Standing Committee for the Scrutiny of Bills (the Committee) released Alert Digest number 13 of 2015, providing commentary on the Bill.

The Attorney-General's Department (the Department) thanks the Committee for its considered response on the Bill and provides the below information in reply.

The Committee may also wish to note that on 15 February 2016 the Parliamentary Joint Committee on Intelligence and Security (PJCIS) reported on its inquiry into the Bill. The Government is presently considering the 21 recommendations made by the PJCIS.

Schedule 2

Control orders for young people

On page 7 of the Digest, the Committee raised the following concern with respect to the extension of the control order regime in Division 104 of the *Criminal Code Act 1995* (Criminal Code) in the context of comments made by the former Independent National Security Legislation Monitor (the former INSLM).

> **Noting the questions that have been raised in relation to the efficacy and appropriateness of the control order regime, the committee seeks the Attorney-General's response to these concerns and, in particular, why it is not appropriate to wait for the INSLM to complete his current inquiry into control order safeguards before extending the regime to 14 and 15 year olds.**
>
> *Pending the Attorney-General's reply, the committee draws Senators' attention to the schedule, 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.*

Control orders play an important role in protecting the public from terrorist threats. They ensure that law enforcement has a legal basis on which to take action to prevent a terrorist threat from eventuating where an arrest or a prosecution is not open, but a person nonetheless presents a credible risk to public safety. In addition, these orders can be used as a less coercive tool than arrest and prosecution by facilitating the monitoring of individuals who pose a threat to the community through the imposition of certain controls on the person's behaviour.

Control orders can also be utilised in relation to individuals who continue to pose a threat to the public following charge, prosecution, conviction and release, to facilitate reintegration into society while also mitigating the risk that the person will engage again in risky behaviour (for example, associating with other people of security concern or accessing websites that advocate extremist views).

Control orders are not intended to replace investigations and prosecutions. They are a preventative mechanism which complements other law enforcement tools.

In 2012, the former INSLM recommended the control order regime be repealed and replaced with a new scheme of post-sentence orders. The Government, however, supports recommendation 26 of the COAG *Review of Counter-Terrorism Legislation*, which recommended the retention of control orders (with additional safeguards and

protections). The proposed amendments to extend the regime to 14 to 15-year-olds include additional safeguards. These additional safeguards are being extended to 16 and 17-year-olds – who are already covered by the regime but without those additional safeguards. The Government will of course consider any further recommendations of the current INSLM concerning additional safeguards and protections to the regime to ensure it remains targeted and robust while not unnecessarily impacting on an individual's rights.

The former INSLM further noted in his 2012 report that the efficacy of a control order depends largely upon the subject's willingness to respect a court order, and that in the absence of the ability to effectively monitor a person's compliance with the terms of a control order, there is no guarantee that a person will not breach the order or go on to commit a terrorist offence.

This is a position shared by our law enforcement agencies. That is because existing Commonwealth coercive powers in relation to the conduct of physical searches, telecommunication interception and surveillance devices are only available for the purposes of investigating an offence that has already been committed or is about to be committed.

The proposed new monitoring powers seek to resolve this issue by adopting a threshold appropriate to the monitoring of a person in relation to whom a superior court has already decided the relevant threshold for issue of a control order has been met and who therefore, by definition, is of security concern. The new regimes will allow monitoring to mitigate the risk of breaches of control orders and, consequently, to mitigate the risk of the person engaging in preparatory acts, planning and terrorist acts.

As noted above, the PJCIS has completed its inquiry into the Bill, which included consideration of Part One of the INSLMS's report on control order safeguards. The Government is presently considering the reports of the INSLM and the PJCIS.

For additional information concerning the new monitoring powers which increase the efficacy of control orders, please see our response under that relevant heading below.

Service of documents on a parent or guardian (items 11, 13 and 14)

On page 8 of the Digest, the Committee raised the following concern with respect to the requirement to take reasonable steps to serve a control order on a young person's parent or guardian.

> **While the committee notes this explanation, the committee seeks further information from the Attorney-General as to the options considered to deal with this potential problem with a view to ensuring that documents are served on a parent or guardian in all but the most exceptional circumstances. For example, the committee is interested whether consideration was given to including a provision in the bill that would have the effect of requiring that *all* reasonable steps are taken to notify a parent or guardian.**
>
> *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.*

The requirement to take reasonable steps to serve the order on a young person's parent or guardian will ensure a parent or guardian is served whenever possible. Service on a parent or guardian will occur unless it is not reasonably possible to do so. There are a number of reasons the AFP may be unable to serve a parent or guardian. It may be that a parent or guardian cannot be located. It may also be that it would be inappropriate to

serve a parent or guardian because, for example, the young person is estranged from the parent. Providing that the AFP 'must' serve the parent or guardian could potentially frustrate the process in circumstances where the AFP is unable to effect service or where service would actually infringe on the young person's civil liberties and privacy, where they are estranged from the parent.

In considering how to formulate the obligation to serve the parent or guardian the Government adopted the term 'reasonable steps', a phrase that is commonly used in Australian laws and has been considered in case law, thus providing guidance to its interpretation.

The term bears its ordinary meaning, as being based upon or according to reason and capable of sound explanation. What is reasonable is a question of fact in each individual case. It is an objective test that has regard to how a reasonable person, who is properly informed, would be expected to act in the circumstances. What is reasonable can be influenced by current standards and practices. In a related context, the High Court has observed that whether there are 'reasonable grounds' to support a course of action 'requires the existence of facts which are sufficient to [persuade] a reasonable person';[1] it 'involves an evaluation of the known facts, circumstances and considerations which may bear rationally upon the issue in question'.[2]

It will be the responsibility of law enforcement to justify that reasonable steps were taken.

Amending the requirement to require that '*all* reasonable steps' are taken could be interpreted as requiring the AFP to take steps that another person contemplates, but that were not contemplated by the AFP at the time. In other words, it could bring an element of hindsight into the test, resulting in an AFP officer who acted in good faith and took reasonable steps to undertake service being found not to have taken a further step that another person identified after the fact.

Recommendation three of the PJCIS report considers the requirement to serve a parent or guardian. The Government is presently considering the PJCIS report.

Independence of court appointed advocate and disclosure of information provided to a court appointed advocate (item 46, proposed subsections 104.28AA(1) and (4)–(6))

On page 9 of the Digest, the Committee requested further information about the independent of court appointed advocate.

The committee therefore seeks the Attorney-General's advice as to:

- **how the independence of the court appointed advocate is to be secured in practice;**
- **more detail about the intended professional obligations applying to advocates; and**
- **the justification for not providing more guidance about the qualifications of advocates and mechanisms designed to ensure their independence in the legislation.**

---

[1] *George v Rockett* (1990) 170 CLR 104 at 112 (Mason CJ, Brennan, Deane, Dawson, Toohey, Gaudron & McHugh JJ).

[2] *McKinnon v Secretary, Department of Treasury* (2006) 228 CLR 423 at 430 (Gleeson CJ & Kirby J).

Pending the Attorney-General's reply, the committee draws Senators' attention to this matter, 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.

On page 10 of the Digest, the Committee requested further information and justification in relation to provision authorising the court appointed advocate to disclose information that a young person subject to a control order has communicated to the advocate to the court in certain limited circumstances.

The committee therefore seeks a more detailed justification from the Attorney-General for the proposed approach, including specific examples of situations in which it is envisaged that a court appointed advocate would be likely to disclose information against the wishes of the child. The committee also seeks advice as to whether consideration has been given to including:

- **a requirement that clear advice be given to the child that information given to their advocate may be disclosed to the issuing court against their wishes; and**
- **a default requirement to at least consult with a parent, guardian and/or lawyer (if such a person is available) before information is disclosed against the wishes of the child unless exceptional circumstances exist.**

Pending the Attorney-General's reply, the committee draws Senators' attention to this matter, 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.

The court appointed advocate model in the Bill seeks to achieve the following outcomes:

- ensure the controls imposed by the control order and the consequences of failing to comply with them is fully explained to the child by an independent person (noting that interim control orders are generally obtained on an ex parte basis, such that the young person would not likely have legal representation at the time of service). The AFP will continue to be required to provide this and other information to the child at the time of service
- ensure there is an independent person who can provide the court with an assessment about what is in the child's best interests, and
- ensure, particularly in circumstances where the child does not have separate legal representation, that there is a legally qualified person from whom the child can seek advice, and who can adduce evidence and make submissions for the child during proceedings.

The proposed section 104.28AA of the Criminal Code provides guidance on the role and qualifications of the advocate. Specifically, the independence of the advocate from the young person is achieved by the requirements in the bill to form an independent view, to act in and to make submissions in the best interests of the child, rather to act on the child's instructions (see subsections 104.28AA(2) and (3)). The independence of the advocate from the court is achieved by the advocate not being under an obligation to disclose information communicated by the young person unless doing so would be in the best interests of the child (see subsections 104.28AA(4) and (5)).

Further, the provision authorising the advocate to disclose information communicated by the young person is an important safeguard for the child. Although it is envisaged that the situations in which a court appointed advocate would disclose information to the court against the wishes of the child would be rare.

On 14 December 2015, the PJCIS requested the Attorney-General's Department to review the submissions made by bodies such as the Law Council of Australia and the Gilbert and Tobin Centre of Pubic Law and respond to the issues raised. On 15 January 2016 the Department provided the PJCIS with a supplementary submission which sought to address each of those sets of issues. A number of the submissions discuss the court appointed advocate model and the PJCIS asked the Department to consider whether an alternate model is feasible. The Department has advised the PJCIS that an alternate model may help address the concerns raised in those submissions as well as those raised at pages 9 and 10 in the Committee's Digest, although any alternate model would be subject to agreement by the States and Territories as per the International Agreement on Counter-Terrorism Laws.

Recommendation two of the PJCIS report considers the court appointed advocate model. The Government is presently considering the PJCIS report.

Schedule 5

Preventative detention orders

On page 12 of the Digest, the Committee requested further information about the amendment of the threshold for obtaining a preventative detention order.

> **In this context the committee therefore:**
>
> - **seeks the Attorney-General's more detailed explanation as to why the power to issue a PDO should be broadened in this way; and**
> - **requests the Attorney-General's advice as to any alternative powers at the disposal of law enforcement to respond to knowledge that a person has the necessary tools to commit a terrorist act in circumstances where no evidence is available about when an attack may occur.**
>
> *Pending the Attorney-General's reply, the committee draws Senators' attention to the schedule, 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.*

Currently, the issuing authority must be satisfied there are reasonable grounds to suspect that a terrorist act is imminent and is expected to occur, in any event, at some time in the next 14 days. The problem with this test is that even where police have grounds to suspect a person has the capacity to carry out a terrorist act at any time, neither the AFP nor the issuing authority may have information as to the time that has been selected to carry out that act – if indeed a time has been selected. For example, if a terrorist is prepared and waiting for a signal or instruction to carry out their act, the AFP may not be able to identify when that signal or instruction will be sent. Indeed the terrorist themselves may not know. Under the existing test, the AFP may not be able to seek a preventative detention order without information as to the expected timing. Accordingly, there is an operational gap in ability to deal with terrorist acts that are not planned to occur on a particular date, even where the preparations for that terrorist act may be in their final stages, or complete.

As the AFP noted in their submission to the PJCIS, if the point in time that an incident will take place is not known, the issuing authority may not be satisfied the act is expected to occur sometime in the next 14 days. The proposed amendment addresses this issue by placing the emphasis on the capacity for an act to be carried out in the next 14 days. If a terrorist act is capable of being carried out, and could occur, within 14 days, that terrorist act will meet the definition of an 'imminent terrorist act'. Accordingly, the proposed

amendment ensures the AFP has the ability to apply for a PDO to safeguard the public against such risks where they are identified. The inclusion of a 14-day timeframe in which the act could occur retains the imminence requirement, but focusses on the capability of a person to commit a terrorist act, as opposed to the specific time in which the terrorist act is expected to occur.

The issuing authority must be satisfied that making the preventative detention order would substantially assist in preventing an imminent terrorist act occurring, and that detaining the person is reasonably necessary for the purpose of preventing a terrorist act. Accordingly, the power is only available when detention of the person is required. The AFP can arrest and detain a person for the purpose of investigating a terrorism offence under Part 1C of the *Crimes Act 1914* (Cth). However, there will be situations when arrest is not a viable option, but a person nonetheless presents a credible risk to public safety in relation to an imminent terrorist act.

Recommendation fifteen of the PJCIS report considers the threshold for obtaining a PDO. The Government is presently considering the PJCIS report.

Schedule 8

New 'monitoring warrant' regime

On page 14 of the Digest, the Committee requested further information and justification in relation to the proposed monitoring search warrant regime.

> **The committee therefore seeks the Attorney-General's justification for the approach taken and seeks advice as to whether the principles in the Guide have been considered.**
>
> **The committee also seeks advice as to whether each of the monitoring powers under the proposed 'monitoring warrant' regime established by this schedule are consistent with the principles in the Guide and the approach taken in Part IAA of the *Crimes Act 1914* (and if they are not, the rationale for taking an alternative approach in this instance).**
>
> *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.*

The power to seize evidentiary material pursuant to the new monitoring warrant regime is largely consistent with the *Guide to Framing Commonwealth Offences, Infringement Notices and Enforcement Powers* (the Guide). However, where minor differences exist between the provisions in the new monitoring warrant regime and existing precedents, the Government considers there is solid operational and policy justification.

The Guide refers to monitoring warrants precedents, including subsection 90-4(2) of the *Aged Care Act 1997*, which states that where an authorised officer is exercising monitoring powers and has reasonable grounds to believe that a thing that may afford evidence of the commission of an offence would be lost, destroyed or tampered with by the time a search warrant is obtained, they have the power to secure the evidence pending an application for a search and seizure warrant. However, the Act also allows the authorised officer to apply for a warrant to seize things in certain circumstances, including where possession of the thing could constitute an offence (section 92-3 of the *Aged Care Act 1997*).

Similarly, the proposed monitoring warrant regime for control orders allows for things to be secured in certain circumstances and seized in others. The regime allows a constable to secure electronic equipment in order to obtain expert assistance in operating the equipment. However, where a constable searches premises pursuant to a monitoring warrant they have the power to seize certain items including things relevant to an offence and seizable items. A seizable item is one that could be used to self-harm or to harm others.

The established principles for traditional monitoring warrants are appropriate for regimes that simply monitor compliance with legislative requirements in circumstances where the possibility or likelihood of the occupant engaging in harmful or even deadly conduct against others is remote. However, that may not necessarily be the case where the monitoring warrant relates to a person who on reasonable grounds the court suspects has engaged in conduct which is of security concern, such as participated in training with a terrorist organisation. Accordingly, the proposed monitoring warrant regime only authorises an issuing authority to authorise a warrant to monitor compliance with a control order if satisfied that the purpose of a search, pursuant to the warrant, is protecting the public from a terrorist act; preventing the provision of support for, or the facilitation of, a terrorist act; preventing the provision of support for, or the facilitation of, the engagement in a hostile activity in a foreign country; **or** determining whether the control order has been, or is being, complied with. This threshold is different from other monitoring warrant regimes.

Furthermore, the issuing authority will take into consideration the things that are sought to be authorised pursuant to the warrant, which includes seizure of evidentiary material, when deciding whether to issue the warrant.

These targeted powers underline the important protective value of imposing a control order on a person who has already been identified as being of security concern, noting that terrorist acts can come to fruition very quickly. In addition, where police identify evidential material and seizable items, it is not only appropriate, but vital, that they are able to take action as quickly as possible with respect to those items to protect the Australian community. Unlike some monitoring warrant precedents that only allow for evidence to be 'secured' pending an application for a search and seizure warrant law enforcement, this would be inadequate to deal with the security risk in this proposed regime. If there is a delay in which the evidence can be used, caused by a requirement to get a second warrant, this could have significant adverse outcomes.

The regime provides a number of safeguards and accountability mechanisms to protect rights against arbitrary and unlawful interferences with privacy. The Attorney-General's Department is currently finalising a Privacy Impact Statement that will explore those issues fully.

In these circumstances it is appropriate to allow certain items to be seized rather than secured pending a further warrant.

Recommendations nine, ten and eleven of the PJCIS report also consider a number of aspects of the proposed monitoring warrant regime, including additional safeguards and accountability mechanisms. The Department is presently considering the PJCIS report.

Schedules 8, 9 and 10

Monitoring of compliance with control orders etc, Telecommunications interception, and surveillance devices (item 1, proposed section 3ZZTC of

the *Crimes Act 1914*, item 53, proposed section 299 of the *Telecommunications (Interception and Access) Act 1979*, and item 39, proposed section 65B of the *Surveillance Devices Act 2004)*

On page 16 of the Digest, the Committee requested information about the use of information or evidence obtained before an order that formed part of the basis for obtaining the information or evidence was declared void.

> **As such, the committee seeks the Attorney-General's advice as to whether similar provisions appear in other Commonwealth legislation and requests a more detailed justification for the use of material obtained in circumstances in which the relevant control order has been declared void.**
>
> *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.*

The provisions, inserted into the *Crimes Act 1914* (the Crimes Act), *Surveillance Devices Act 2004* (the SD Act) and *Telecommunications (Interception and Access) Act 1979* (the TIA Act) are intended to address the unlikely scenario where:

- an interim control order has been issued in respect of a person;
- a law enforcement agency has duly obtained a monitoring warrant in relation to that person;
- under that monitoring warrant, the agency has obtained information that indicates that the person is likely to engage in a terrorist act, cause serious harm to a person, or cause serious damage to property;
- before the agency can act on that information, the interim control order is considered by a court at a confirmation hearing and declared void *ab initio* pursuant to subsection 104.14(6) of the Criminal Code on the grounds that, at the time of making the interim control order, there were no grounds on which to make the order.

As the existence of a valid control order is a condition for the issuing of a monitoring warrant, the likely effect of a court declaring an interim control order void *ab initio* pursuant to subsection 104.14(6) of the Criminal Code would be that any monitoring warrants predicated on that control order would also likely be void *ab initio*.

It is a fundamental principle of the Australian legal system that courts have a discretion as to whether or not information may be admitted as evidence into proceedings, irrespective of the manner in which the information was obtained. As an example, the *Bunning v Cross*[3] discretion places the onus on the accused to prove misconduct in obtaining certain evidence and to justify the exclusion of the evidence. This provision is expanded on in Commonwealth statute[4], where there is an onus on the party seeking admission of certain evidence to satisfy the court that the desirability of admitting the evidence outweighs the undesirability of admitting it, given the manner in which it was obtained. This fundamental principle reflects the need to balance the public interest in the full availability of relevant information in the administration of justice against competing

---

[3] (1978) 141 CLR 54.

[4] Section 138 of the *Evidence Act 1995 (Cth)*.

public interests, and demonstrates the role the court plays in determining admissibility of evidence.

However, the SD Act and TIA Act depart from these fundamental principles, by imposing strict prohibitions on when material under those Acts may be used, communicated or admitted into evidence.[5] Under these Acts, it is a criminal offence for a person to deal in information obtained under these Acts for any purpose, unless the dealing is expressly permitted under one or more of the enumerated and exhaustive exceptions to the general prohibition. These provisions expressly override the discretion of the judiciary, both at common law and under the *Evidence Act 1995*, to admit information into evidence where the public interest in admitting the evidence outweighs the undesirability of admitting it, given the manner in which it was obtained. There is also a risk that these specific provisions might be interpreted, either by a court considering the matter after-the-fact, or by an agency considering the question *in extremis*, to override the general defence to criminal responsibility under the Criminal Code.

For this reason, the Bill would insert new section 65B to the SD Act and section 299 to the TIA Act, which would expressly permit agencies to rely on such information to prevent, or lessen the risk, of a terrorist act, serious harm to a person, or serious damage to property. These provisions would also permit such information to be used to apply for, and in connection with, a preventative detention order.

The Crimes Act does not contain restrictions on dealing in information obtained under a search warrant equivalent to those contained in the SD Act and TIA Act. As such, the circumstances in which proposed new section 3ZZTC of the Crimes Act would be likely to modify the operation of the existing law are likely narrower than the circumstances in which proposed new section 65B of the SD Act and section 299 of the TIA Act would apply. Nevertheless, as the three monitoring warrant regimes, under the Crimes, SD and TIA Acts are intended to operate in parallel with one another, the Government proposes to include proposed new section 3ZZTC of the Crimes Act, so as to avoid any inference being drawn that the absence of such a provision might reflect Parliament's intent that information obtained under that Act be subject to more stringent controls than information obtained under the SD and TIA Acts.

Recommendations nine to thirteen of the PJCIS report consider a number of aspects of the proposed monitoring warrant regime, including additional safeguards and accountability mechanisms. The Department is presently considering the PJCIS report.

Schedules 9, 10 and 14

Authorisation of intrusive powers

On page 18 of the Digest, the Committee requested information about the breadth of individuals who can be appointed as eligible issuing officers for the purposes of the telecommunications interception warrants and surveillance device warrants regimes.

> **Noting the legal complexity of the relevant provisions, and given that this bill seeks to extend the circumstances in which telecommunications interception warrants and surveillance device warrants can be issued (schedules 9 and 10) and change the threshold requirements for the issue of a delayed notification search warrant (schedule 14), the committee seeks the Attorney-General's advice as to why the categories of eligible issuing officers should not limited to persons who hold judicial office.**

[5] See section 63 of the TIA Act and 45 of the SD Act.

Pending the Attorney-General's reply, the committee draws Senators' attention to these matters, 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.

AAT members have extensive experience exercising personal functions under a broad range of legislative schemes. The role proposed for authorised members in the Bill is consistent with existing functions able to be undertaken by AAT members. As outlined below, there are legislative, ministerial and governance processes in place that support the appropriateness and value of AAT members being authorised to perform these roles.

AAT members as issuing officers in similar contexts

Enabling members to be nominated as issuing officers under the Bill is supported by a longstanding practice of allowing members, along with judicial officers, to undertake sensitive personal functions. AAT members have been eligible for nomination to issue interception and stored communications warrants under the *Telecommunications (Interception and Access) Act 1979* since 1997, and surveillance device warrants under the *Surveillance Devices Act 2004* since 2004. More recent reforms have expanded the range of sensitive functions able to be exercised by members who are issuing officers:

- in 2001, to extend the length of controlled operations beyond three months under the *Crimes Act 1914*
- in 2005, to make continued preventative detention orders under the *Criminal Code Act 1995*
- in 2007, to make orders allowing information given to the Inspector of Transport Security to be disclosed to another government agency under the *Inspector of Transport Security Act 2006*, and
- in 2012, to issue search warrants and exercise powers under the *Tobacco Plain Packaging Act 2011* and to issue examination notices under the *Fair Work (Building Industry) Act 2012*.

The nature and complexity of the functions proposed for issuing officers under the Bill is analogous to the roles already undertaken by authorised members and does not represent a departure from the approach taken in other recent legislation.

Qualification and eligibility requirements for AAT members

The legislation enabling the authorisation of members, including for the functions provided under schedules 9, 10 and 14 of the Bill, incorporate specific qualification and eligibility requirements for AAT members.

Deputy Presidents and senior members are eligible to be nominated under the Telecommunications (Interception and Access) Act and the Surveillance Devices Act.[6] Part-time senior members and members must be legal practitioners and have been enrolled for more than 5 years to be eligible for nomination under these Acts. Schedules 9, 10 and 14 preserve these eligibly requirements and qualification thresholds.

Ministerial authorisation provides an additional safeguard for the exercise of personal functions undertaken by members. Members meeting eligibility criteria and who consent to perform a

[6] Section 6DB *Telecommunications (Interception and Access) Act 1979* and section 13 *Surveillance Devices Act 2004.*

function are individually considered for authorisation by the responsible minister. The role for the Attorney-General to authorise members under the Telecommunications (Interception and Access) Act and the Surveillance Devices Act is coupled with the power to revoke the authorisation of a member.[7] The department is not aware of any instance where the authorisation of an AAT member has been revoked by an Attorney-General.

Reporting and governance support provided within the AAT

A broad range of governance and support arrangements are provided by the AAT to assist members who are authorised and to support the transparency of their personal functions. For example, the AAT convenes a Warrants Committee, which is chaired by a Deputy President. The Warrants Committee provides training and support to authorised members on matters such as:

- the circumstances in which an application for a warrant might ordinarily be refused, or be granted subject to the provision of further information
- the circumstances in which an application for a warrant might ordinarily be granted subject to conditions, including the factors commonly considered when determining conditions, and
- where appropriate, organising professional development activities and distributing information to authorised members.

The Warrants Committee provides advice to the President of the AAT on the exercise of authorised member functions, including in relation to the collection of data and liaison about warrants related matters with the Attorney-General's Department.

The AAT also makes a broad range of training resources available to authorised members, such as practice manuals prepared by the AAT and the CDPP, guidelines to the operation of legislative schemes, information circulars about reforms in other jurisdictions, hosting guest speakers and enabling one-on-one training for newly authorised members with more experienced authorised members.

Information about the exercise of personal functions by authorised AAT members is recorded in the AAT's case management system and application related statistics are publicly reported in the AAT's Annual Report.

Promoting accessibility and access for law enforcement agencies

The inclusion of AAT members as eligible issuing officers provides law enforcement agencies with a larger pool of decision makers across most states and territories. The Telecommunications (Interception and Access) Act Annual Reports for 2012-13, 2013-14 and 2014-15 illustrate the significant volume of work undertaken by issuing officer members under that Act alone:

	Authorised members	**Warrants applications considered and issued under the Telecommunications (Interception and Access) Act**
2012-13	37	3,330
2013-14	29	3,212
2014-15	29	3,223

[7] Section 6DB *Telecommunications (Interception and Access) Act 1979* and section 13 *Surveillance Devices Act 2004.*

Functions that are undertaken by judicial officers and AAT members in their personal capacity are subject to the consent of the issuing officer at the time an application is being made.

Reported statistics demonstrate that AAT members hear a large number of warrants applications. By comparison over the same period, fewer warrants were issued by authorised federal judicial officers under the Telecommunications (Interception and Access) Act, for example:

	Warrants applications considered and issued under the Telecommunications (Interception and Access) Act
2012-13	896
2013-14	795
2014-15	703

AAT members also regularly make themselves available to consider applications outside of business hours, enabling urgently arising applications to be considered. The AAT reports that in 2014-15, 162 applications were made to members outside of business hours.[8]

There is no empirical material to suggest that members do not exercise their personal functions as issuing officers professionally and diligently. Data collected during 2012-13 by the AAT (set out below) indicates that in a number of cases where warrants have been issued, members have required further information or amendments to applications prior to issuing a warrant.

Warrant applications, 2012 -2013	**Total**
Total issued	**4451**
Issued - as requested	4008
Issued - after further information provided	237
Issued - with conditions	147
Issued - for less time than sought	104
Issued - with revised privacy declaration	16
Refused	**55**

Constitutional impediments

Moreover, as the Committee is aware, strict constitutional requirements limit the functions members of the judiciary may exercise in a personal capacity. In *Grollo v Palmer* (1995) 184 CLR 348, the High Court held that the Parliament or executive cannot confer on a judge of a federal court a non-judicial function that is not incidental to a judicial function unless:

(a) the judge consents to the performance of the function, and

[8] Administrative Appeals Tribunal Annual Report 2014-15, 34. This figure is not identified as being specific to applications under the Telecommunications (Interception and Access) Act only.

(b) the exercise of the function is not incompatible either with the judge's performance of his or her judicial functions or with the proper discharge by the judiciary of its responsibilities as an institution exercising judicial power.[9]

From an historical perspective, these constitutional limitations contributed to the basis for enabling AAT members to be issuing authorities. Following that decision of the High Court, a significant number of judges of the Federal Court made known to the then Attorney-General that they were not prepared to continue to issue warrants. As the Committee would appreciate, the ability for law enforcement agencies to use a range of investigative powers appropriate and adapted to the circumstances of a particular investigation is essential to the effective administration of justice. It would, therefore, be repugnant to the effective administration of justice for the proper conduct of investigations to be frustrated by the non-availability of issuing authorities to consider applications for warrants or authorisations for the use of such powers.

Given only a limited number of members of the judiciary wished to continue exercising this function, it was necessary to empower members of the AAT, being independent statutory office holders accustomed to reviewing the conduct of the executive, to also have the authority to consider applications for warrants and other investigative powers.

International law

It may also interest the Committee to know that comparable international jurisdictions do not require warrants to be issued by members of the judiciary. For example, within the European Union, the European Court of Human Rights has stated that, while "it is in principle desirable to entrust supervisory control [of covert and intrusive investigatory powers] to a judge",[10] such powers can permissibly be authorised by members of the Executive provided that the warrant scheme is complemented by effective post-review of the authorisation.[11] More recently, in *Kennedy v The United Kingdom*[12], the Court held that the Interception of Communications Commissioner and the Investigatory Powers Tribunal provided effective safeguards in a system where authorisations are made at the Head of an Agency/Ministerial level.

In Australia, the current system entrusts the federal judiciary and nominated AAT members with issuing telecommunications interception and surveillance devices warrants. The Commonwealth Ombudsman and State and Territory oversight bodies conduct robust oversight of the warrants regime to ensure effective post-review of these investigatory powers.

Schedule 9

Retrospective validation (item 54)

On page 19 of the Digest, the Committee requested further information about the proposed amendments that would ensure certain past actions in relation to information obtained through interceptions were not unlawful.

---

[9] In *Wainohu v New South Wales* (2011) 243 CLR 181, the High Court held that the incompatibility restriction on the permissible functions of judges extended to judges of state and territory courts.
[10] *Klass and others v Germany* [1978] ECHR 4.
[11] Ibid.
[12] [2010] ECHR 26839/05.

The committee therefore requests a more detailed explanation from the Attorney-General in relation to the rationale for, and necessity 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.

Telecommunications interception is considered a necessary and proportionate measure in preventing the terrorist threat in Australia. Preventative detention order regimes at the Commonwealth, state and territory level are also an important part of countering this threat.

There is a clear parliamentary intent to make lawfully intercepted information obtained under the TIA Act to be made available for the purposes of identifying, preventing and prosecuting acts of terrorism. This is reflected in the purposes for which lawfully intercepted information can be used, communicated, record and admitted into evidence in the TIA Act.

The PDO regime was established in 2005 based on a Council of Australian Governments agreement. The intention was for this to become a seamless national regime.

However, there is an anomaly in the TIA Act, which only allows lawfully intercepted information to be made available for the Commonwealth preventative detention order regime.

This anomaly has only been discovered as a result of recent operational activities and because of differences in the operation of preventative detention order regimes at the state and territory and Commonwealth level. These subtle differences have resulted from the implementation of the PDO regimes between jurisdictions. At the Commonwealth level, and in a number of states and territories, applications for PDOs are made to issuing authorities, who serve in their personal capacities, similar to an application for a warrant. In other jurisdictions, applications are made to a court, similar to applications for control orders. While subtle, this distinction has important implications for the operation of the TIA Act, which contains distinct rules for when lawfully intercepted information may be disclosed to a person (such as an issuing authority), and when it may be given and adduced into evidence in court. This amendment is designed to rectify this irregularity.

Schedule 11

Freedom of expression

On page 21 of the Digest, the Committee requested further information about the breadth of the proposed new advocating genocide offence.

However, in light of the explanation for the provision, the committee leaves the general question of whether it is appropriate to broadly define 'advocate' for the purpose of the offence of advocating genocide to the Senate as a whole.

On page 21 of the Digest, the Committee requested further information about the meaning of 'publicly' and examples of conduct captured by the proposed new advocating genocide offence.

The committee therefore seeks the Attorney-General's advice as to:

- **whether it would be possible to include some guidance in the legislation itself in relation to the meaning of 'publicly' for the purpose of this proposed offence; and**
- **specific examples of the conduct intended to be covered by the 'public' component of the offence.**

On pages 21 and 22 of the Digest, the Committee requested further information about the difference in the coverage of the proposed new advocating genocide offence as compared with existing criminal offences, including those in Division 80 of the Criminal Code.

> **The committee therefore seeks the Attorney-General's advice as to what conduct is intended to be captured by this proposed offence that is not already captured by current offences.**
>
> *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.*

In the current threat environment, the use of social media is accelerating the speed at which persons can become radicalised and prepared to carry out acts such as genocide. Law enforcement advises that it is no longer the case that explicit statements (which would provide evidence to meet the threshold of intention) are required to inspire others to take potentially devastating action in Australia or overseas. The cumulative effect of more generalised statements, particularly when made by a person in a position of influence and authority, can still have the impact of directly encouraging others to commit acts of violence, such as terrorism, hostile activities overseas, or genocide.

The proposed offence would supplement existing offences, such as those in Division 80 of the Criminal Code, that prohibit urging violence and advocating terrorism, and will be available as another tool available to law enforcement to intervene earlier in the radicalisation process to prevent and disrupt further engagement in terrorist activity.

Law enforcement is concerned about the impact those who advocate genocide, (commonly termed 'hate preachers') have on the current crime environment. The new advocating genocide offence is directed at those who supply the motivation and imprimatur. This is particularly the case where the person advocating genocide holds significant influence over other people who sympathise with, and are prepared to fight for, the genocide of a race or other group of individuals.

Under existing provisions in the Criminal Code, where a person "incites" (within the meaning of section 11.4 of the Criminal Code) the commission of one of the primary genocide offences, the offence of incitement will only be made out where the person "intended" a genocide offence to be committed. The current ancillary offence of inciting genocide carries a maximum penalty of 10 years imprisonment.

In contrast, the proposed new primary offence of advocating genocide will ensure that a person who advocates the commission of a primary genocide offence and is merely "reckless" as to whether another person will commit a genocide offence as a result of their conduct. The new offence will only carry a maximum penalty of seven years imprisonment, reflecting the slightly lower fault element. As with "tiered" offences, the option of a lower threshold/lower penalty offence can be important where a person's conduct breaches the criminal law, but the higher fault element cannot be proven beyond reasonable doubt.

Where there is sufficient evidence, existing offences of incitement or urging violence would be prosecuted. Those offences require proof that the person intended to incite or urge violence or a crime and intended the crime or violence to be committed. There will not always be enough evidence to meet the threshold of intention in relation to the second aspect. This is because persons advocating genocide can be very deliberate about the precise language they use, even though their overall message still has the impact of encouraging others to engage in genocide.

While 'publicly' is not defined, it would include, but would not be limited to:

- causing words, sounds, images of writing to be communicated to the public, a section of the public, or a member of members of the public (for example, creating a website which has no access restrictions and which encourages people to kill people of a particular race)

- conduct undertaken in a public place, (for example, gathering a crowd at a busy intersection in the centre of a city, shouting offensive language and urging people to take action to eradicate people of a particular religion), or

- conduct undertaken in the sight or hearing of people who are in a public place (for example, standing on a balcony above a café holding a banner which tells people to kill all people born in a particular country).

This is consistent with the *Convention on the Prevention and Punishment of the Crime of Genocide* (the Genocide Convention). Article III of the Genocide Convention requires States Parties to punish individuals who engage in direct and public incitement to commit genocide.

The offence is also supported by Article 20(2) of the ICCPR, which requires States to create laws prohibiting advocacy for national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence.

The offence is subject to the existing 'good faith' defences to ensure it is a reasonable, necessary and proportionate limitation on the right to freedom of expression.

The department considers that the Explanatory Memorandum provides sufficient guidance as to what would constitute 'advocating' and 'publicly'. As is commonly done in legislative drafting, both words are intended to take their ordinary meaning when used in the Bill.

However the Committee may wish to consider that recommendations seventeen and eighteen of the PJCIS report consider aspects of the proposed advocating genocide offence. The Government is presently considering the PJCIS report.

Schedule 14

Requirements for obtaining a delayed notification search warrant

On page 23 of the Digest, the Committee requested further justification for the proposed amendments to the threshold for the delayed notification search warrant regime.

Given the potential for the delayed notification search warrant scheme to trespass on personal rights and liberties (by allowing AFP officers to covertly enter and search premises, without the knowledge of the occupier of the premises), the committee considers that the lowering of the threshold for issuing a delayed notification search warrant should be comprehensively justified. The committee therefore seeks the Attorney-General's detailed advice as to the rationale for this proposed change.

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.

The purpose of this amendment is to clarify the requirements for the issue of a delayed notification search warrant. A literal reading of the provision as drafted in Crimes Act would require a chief officer and an issuing officer to personally hold suspicions or beliefs that they are not in a position to personally hold as persons removed from the investigation. This was not intended when the provision was drafted.

The intended operation of the regime was, as with other warrant regimes, to provide safeguards against abuse of the regime by requiring the chief officer and eligible issuing officer to independently be satisfied that the eligible officer in fact holds the requisite suspicions and belief, and that there are reasonable grounds for holding the suspicions and belief. In the case of the eligible issuing officer, this is to be achieved by receiving information from the eligible officer on oath or affirmation. For example, a search warrant may be issued under subsection 3E(1) of the Crimes Act only where the issuing officer is satisfied that there are reasonable grounds for suspecting that there will be evidential material at a premises, rather than where the issuing officer personally holds such a suspicion him/herself.

Schedule 15

Fair hearing (item 19, proposed new section 38J)

On page 27 of the Digest, the Committee requested further justification for the proposed amendments to the NSI Act.

In this context the committee therefore seeks a more detailed justification from the Attorney-General for the proposed approach. In particular, the committee seeks advice as to whether further safeguards for fairness have been considered, and if so why they have not been included in the legislation, for example, whether the court could be expressly limited to making these special orders where a risk to national security is considered to reach a threshold degree of seriousness.

The Committee also notes the UK system of special advocates and recommendations in the 2013 'Council of Australian Governments Review of Counter-Terrorism Legislation'.

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.

Under the NSI Act, there are existing provisions that enable a court to consider, in a closed hearing, whether national security information may be disclosed and if so, in what form. The court has the discretion to exclude non-security cleared parties, their non-security cleared legal representatives and non-security cleared court officials from the hearing

where the court considers that disclosing the relevant information to these persons would likely prejudice national security. If a party's legal representative is not security cleared, does not wish to apply for a security clearance, or a clearance is unable to be obtained in sufficient time before the closed hearing, then the court may still hold the closed hearing and determine the matter without the assistance of a legal representative of the party. Alternatively, the court could decide to appoint a security cleared special counsel to represent the interests of the party during the closed hearing (although there has been no need for a security cleared special counsel to be appointed under the NSI Act to date). However, any information the court decides should not be disclosed under the NSI Act cannot be used in the substantive proceeding.

The purpose of the proposed amendments to the NSI Act is to provide the court with two further options when the NSI Act has been invoked in a control order proceeding. First, the option to exclude a respondent's legal representative, even if they are security cleared, at the closed hearing to determine if or how the information should be disclosed in the substantive control order proceeding. Second, it provides the option for the court to still consider that evidence in the substantive control order proceeding, even if it cannot be disclosed to the party or their lawyer (whether security cleared or not). The rationale for these amendments is that the evidence may be so sensitive that even a security cleared legal representative cannot see the information.

The AFP's submission to the PJCIS inquiry into the Bill explains the importance of protecting sensitive information, not only to maintain the confidentiality and integrity of law enforcement and intelligence operations and methodologies, but also to maintain the trust with which law enforcement has been provided this information. It also explains that in the current threat environment, it is increasingly likely that law enforcement will need to rely on evidence that is extremely sensitive, such that its disclosure, even to a security-cleared lawyer, could jeopardise the safety of sources and the integrity of investigations. There is a substantial risk that the inability to rely on sensitive information may mean that control orders are unable to be obtained in relation to a person posing a high risk to the safety of the community. Accordingly, the purpose of the amendments is aimed at achieving the legitimate objective of protecting national security information in control order proceedings, the disclosure of which may be likely to prejudice national security.

The amendments to the NSI Act will provide the court with the ability to make three new types of orders to protect national security information that may result in the court being able to consider information in a control order proceeding that the person the subject of the control order proceeding (or their legal representative) may not see. Prior to making one of these new orders, under paragraph 38J(1)(c), the court must be satisfied that the subject of the control order proceeding has been provided sufficient notice of the allegation on which the control order request is based (even if the person has not been given notice of the information supporting those allegations).

When considering the effect of the proposed amendments to the NSI Act, it is important to consider the proposed amendments as a whole rather than considering the sections in isolation. There are several protections built into the legislation that mitigate any procedural unfairness. Prior to making one of the new orders, the court must consider whether the order would have a substantial adverse effect on the substantive control order proceeding (subsection 38J(5)). This requires the court to contemplate the effect that withholding the information from the respondent or their legal representative will have on procedural fairness for the subject of the control order proceeding. Furthermore, the proposed amendment to subsection 19(4) will confirm that the court has discretion to later order a stay of a control order proceeding, if one of the new orders has been made

and later in the proceedings it becomes evident that the order would have a substantial adverse effect on the substantive control order proceeding.

Importantly, the court also has discretion to decide which order to make and the form the order should take. For example, if the AFP proposes to withhold an entire document from the subject of a control order, but use it in support of the control order application, the court may decide that only part of the document may be withheld and used, or that the entire document can be withheld and used but the person must be provided with a summary of the information it contains. This is often referred to as 'gisting'.

Furthermore, the normal rules of evidence apply to evidence sought to be introduced under these new orders, in accordance with the express terms of section 38J and the existing Criminal Code provisions (section 104.28A). The effect of those provisions is that if any material is withheld from the respondent but used in the proceeding, that material must otherwise be admissible as evidence under the normal rules of evidence applicable in control order proceedings. There is also nothing in the new provisions that would dictate to the court what weight it should give to any evidence that is withheld (either in full or in part) from the respondent in the substantive control order proceeding.

Accordingly, the amendments provide an appropriate balance between the need to protect national security information in control order proceedings, and procedural fairness to the person to whom the control order relates. It preserves the independence and discretion of the court and instils it with the powers needed to mitigate unfairness to the subject of a control order proceeding.

The Committee asked whether the court could be expressly limited to making one of the new orders under section 38J where a risk to national security is considered to reach a threshold degree of seriousness. This is unnecessary. The court will only be able to consider making one of the new orders under section 38J if the Attorney-General or the Attorney-General's legal representative has requested the court to make such an order. This will ensure that one of the new orders will only be sought in limited situations. Furthermore, the courts are well-equipped to make judgments as to the weight that should be given to the risk that disclosing information will prejudice national security information, any substantial adverse effect on the substantive control order proceeding, and any other matter the court considers relevant, when determining whether to grant one of the new orders. There is no requirement that the court must provide greater weight to one factor above others when determining whether to make one of the new orders under section 38J.

Recommendations four to six of the PJCIS report consider various aspects of the proposed amendments to the NSI Act. The Government is presently considering the PJCIS report.

Retrospective application (item 27)

On pages 27 and 28 of the Digest, the Committee requested further information about the proposed retrospective application of the relevant amendments in the NSI Act.

> **The committee therefore seeks the Attorney-General's advice as to the rationale for the proposed retrospective application of the amendments to proceedings already commenced and as to how many current proceedings or potential proceedings are, or are likely to be, affected by 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.

It is appropriate that the new orders are available as soon as they come into force, regardless of whether a control order proceeding has already commenced. This is consistent with existing protections that are available under the NSI Act. Section 6A of the NSI Act provides that the Act can apply to civil proceedings that take place after the NSI Act has been invoked, irrespective of whether the proceedings commenced prior to the invocation of the Act. However, the new orders will only be available to those parts of the proceeding that have not yet occurred. Accordingly, the provisions will not operate retrospectively.

Schedule 17

Protected taxation information and privacy

On page 29 of the Digest, the Committee requested information about any alternative thresholds for the disclosure of taxation information that were considered.

The committee therefore seeks the Attorney-General's advice about more targeted alternative authorisation options and why they were rejected. The committee notes that flexibility with some parliamentary oversight could be maintained through the use of a disallowable legislative instrument to extend authorisation to additional agencies.

Pending the Attorney-General's reply, the committee draws Senators' attention to the schedule, 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.

This amendment will authorise taxation officers to disclose information to an Australian government agency for certain specified purposes. It is important that the amendment allows the ability to disclose information for the purposes of preventing, detecting, disrupting or investigating conduct that involves a threat related to security, to "any" Australian government agency. This is because, as with bodies with a role in preventing or taking steps to reduce a serious threat to an individual's life, health or safety or the public's health or safety (see section 355-65(2) Table 1 item 9 of the *Taxation Administration Act 1953*), bodies that have a role in preventing, detecting, disrupting or investigating conduct that involves a matter of security vary over time.

Currently, the key agencies envisaged to seek disclosure under this provision are the National Disruption Group (NDG), which is comprised of officers from a range of Departments, and the Australian Counter-Terrorism Centre (ACTC). However, as we have already seen, the membership or composition of such bodies can change at short notice.

This amendment will ensure that ATO officers have the ability to disclose relevant information to allow early intervention in terrorist activities to prevent the possible widespread and devastating consequences of a terrorist attack. Tax information could be extremely useful for that purpose (although we acknowledge in limited circumstances – and therefore we do not anticipate this amendment being used on a regular basis) and we consider that the possible benefits disclosing that information may have for protecting security outweighs the associated loss of privacy.

Options arbitrarily limiting the Australian government agencies to which disclosures could be made to those agencies that have a national security role today could prevent disclosure to an agency with a national security role tomorrow. This could have devastating outcomes, including loss of many lives in time critical scenarios.

Recommendation twenty of the PJCIS report considers the Commonwealth Ombudsman having oversight of the disclosure of protected tax information. The Government is presently considering the PJCIS report.

MINISTER FOR INDIGENOUS AFFAIRS

Reference: MC16-010138

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

Dear Senator Polley

Thank you for your letter dated 4 February 2016 regarding the Scrutiny of Bills Committee assessment of the *Social Security Legislation Amendment (Community Development Program) Bill 2015* (the CDP Bill).

The CDP Bill provides a framework for amending welfare arrangements to increase incentives to take up work in remote communities. There are a number of outstanding policy decisions regarding the detail of the compliance arrangements and other legislative instruments. This is intentional to ensure sufficient time to develop the instruments in consultation with people likely to be affected by their operation such as CDP providers and job seekers.

Please see below my advice on whether consideration can be given to including a reporting requirement to evaluate:

a) the operation of the scheme

I will undertake a review on phase one for the CDP legislative reforms prior to consideration of the detail of future phases. This review will be undertaken prior to the 2017-18 Budget.

Further consideration will be given to including an evaluation of the CDP Bill.

b) the appropriateness of the use of delegated legislation

Compliance arrangements will be determined in a legislative instrument, subject to the usual rules providing for possible disallowance by either House of Parliament and scrutiny by the Senate Standing Committee on Regulations and Ordinances.

In relation to the determination of remote income support regions, I will consider service provider capacity and fulfil the consultation requirements under the *Legislative Instruments Act 2003* before the relevant legislative instrument is made. Again, this legislative instrument would be subject to disallowance by either House of Parliament and available for scrutiny by the Senate Standing Committee on Regulations and Ordinances.

Use of legislative instruments is appropriate in this case because of the technical and detailed nature of the requirements contained in the legislative instruments that require further consultation with relevant stakeholders. In addition, legislative instruments may need to be amended either during or following the initial phase of implementation.

Please note that I have committed to making further information in relation to the detail of the scheme available to members of Parliament before debate of the CDP Bill and expect to circulate consultation papers on the proposed CDP penalties scheme and compliance framework by mid-March.

I note your advice in relation to the delegation of legislative powers and decision to leave open to the consideration of the Senate whether this is appropriate.

Thank you for the opportunity to respond to your concerns.

NIGEL SCULLION

23 / 2 / 2016