Counter-Terrorism Legislation Amendment Bill (No. 1) 2016

Contacts

Cat Barker – Schedules 1 to 14, Schedule 15 Part 1, Schedules 16 and 17
Foreign Affairs, Defence and Security Section

Christina Raymond – Schedule 15 Part 2, Schedule 18
Law and Bills Digest Section

This Bills Digest updates an earlier version dated 15 February 2016 that was prepared for an earlier version of this Bill (the Counter-Terrorism Legislation Amendment Bill (No. 1) 2015).

Contents

Glossary ................................................................. 4
The Bills Digest at a glance ........................................... 5
History of the Bill ..................................................... 6
Purpose and structure of the Bill ................................... 6
Background ................................................................ 7
  Implementation of COAG and INSLM recommendations ...... 8
Committee consideration ............................................. 9
  Parliamentary Joint Committee on Intelligence and Security ......................................................... 9
  Senate Standing Committee for the Scrutiny of Bills ........... 10
Policy position of non-government parties/independents... 10
Position of major interest groups ................................. 11
  Control orders ............................................................. 11
  Offences relating to special intelligence operations .......... 14
  Other measures .......................................................... 14
Financial implications .................................................. 15
  Special advocate scheme .......................................... 15
Statement of Compatibility with Human Rights ................. 15
  Parliamentary Joint Committee on Human Rights .......... 15

Date introduced: 15 September 2016
House: Senate
Portfolio: Attorney-General
Commencement: Sections 1 to 3 on Royal Assent. Part 2 of Schedule 15 on proclamation or 12 months after Royal Assent, whichever is earlier. Part 1 of Schedule 15 and all other Schedules the day after Royal Assent.

Links: The links to the Bill, its Explanatory Memorandum and second reading speech can be found on the Bill’s home page, or through the Australian Parliament website.

When Bills have been passed and have received Royal Assent, they become Acts, which can be found at the Federal Register of Legislation website.

All hyperlinks in this Bills Digest are correct as at October 2016.
Amendments relating to control orders (Schedules 2, 3, 4 and 15) .............................................................. 16
Lowering the minimum age for a control order to 14 years old (Schedule 2) ........................................... 17
Tracking devices (Schedule 3) .............................................. 20
Issuing courts (Schedule 4) .................................................. 21
New types of orders to protect national security information in control order proceedings (Part 1 of Schedule 15) ........................................................................................................ 21
Special advocates (Part 2 of Schedule 15) .................. 24

Monitoring, protective and preventative powers when a person is subject to a control order (Schedules 8, 9 and 10) .................................................................................................................. 30
Purposes for which powers would be available .................. 31
Thresholds for warrants authorising powers ......................... 31
Powers in relation to interim control orders and orders not yet in force ................................................................. 32
Use of things, information and documents obtained where control order is later declared void ......................... 33
Entry, search, seizure and related powers (Schedule 8) .... 33
Telecommunications interception warrants (Schedule 9) .... 37
Surveillance devices (Schedule 10) ........................................ 40

Preventative detention orders (Schedules 5 and 6) .......... 43

Offence of advocating genocide (Schedule 11) ................. 44

Offences relating to special intelligence operations (Schedule 18) ................................................................. 45
The special intelligence operations scheme ......................... 45
Section 35P—unauthorised disclosure offence ................... 45
Administrative requirements for the commencement or continuation of prosecutions ............................................. 48
Reviews of section 35P ......................................................... 49
INSLM findings and recommendations .......................... 49
Government response to the INSLM’s report .................. 52
Key amendments in Schedule 18 ........................................ 52
Disclosures by entrusted persons—proposed subsections 35P(1) and 35P(1B) (items 1-4) ................................. 52
Comments on the proposed offences for disclosures by entrusted persons .......................................................... 54
Offences for other disclosures—proposed subsections 35P(2) and 35P(2A) (item 4) ........................................... 57
Comments on the offences for ‘other disclosures’ ........... 58
New prior publication defence—proposed subsection 35P(3A) (item 6) ......................................................... 60
Comment on the “prior publication” defence .................. 60
Application of existing exceptions in subsection 35P(3) to the new offences (item 5) ........................................ 61
Extended geographical jurisdiction—subsection 35P(4) (item 7) ........................................................................................................... 61
Other issues—omissions from the 2016 Bill................................. 62

Other provisions .................................................................................. 63
Exemptions to terrorism organisation offences: funds for legal representation (Schedule 1) ................................................................. 63
Security assessments by ASIO (Schedule 12) ................................. 63
Classification of publications et cetera (Schedule 13)................. 64
Delayed notification search warrants (Schedule 14)...................... 65
Dealing with national security information in proceedings (Schedule 16) ......................................................................................... 65
Disclosures by taxation officers (Schedule 17) ............................... 65

Concluding comments ................................................................. 66
Measures previously included in the 2015 Bill.............................. 66
New measures .................................................................................. 66
### Glossary

<table>
<thead>
<tr>
<th>Abbreviation or acronym</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>2015 Bill</td>
<td>Counter-Terrorism Legislation Amendment Bill (No. 1) 2015</td>
</tr>
<tr>
<td>AAT</td>
<td>Administrative Appeals Tribunal</td>
</tr>
<tr>
<td>ACIC</td>
<td>Australian Criminal Intelligence Commission</td>
</tr>
<tr>
<td>ACLEI</td>
<td>Australian Commission for Law Enforcement Integrity</td>
</tr>
<tr>
<td>AFP</td>
<td>Australian Federal Police</td>
</tr>
<tr>
<td>AGD</td>
<td>Attorney-General’s Department</td>
</tr>
<tr>
<td>AHRC</td>
<td>Australian Human Rights Commission</td>
</tr>
<tr>
<td>ALHR</td>
<td>Australian Lawyers for Human Rights</td>
</tr>
<tr>
<td>ASIO</td>
<td>Australian Security Intelligence Organisation</td>
</tr>
<tr>
<td>ASIO Act</td>
<td>Australian Security Intelligence Organisation Act 1979</td>
</tr>
<tr>
<td>CDPP</td>
<td>Commonwealth Director of Public Prosecutions</td>
</tr>
<tr>
<td>COAG</td>
<td>Council of Australian Governments</td>
</tr>
<tr>
<td>IGIS</td>
<td>Inspector-General of Intelligence and Security</td>
</tr>
<tr>
<td>IS Act</td>
<td>Intelligence Services Act 2001</td>
</tr>
<tr>
<td>INSLM</td>
<td>Independent National Security Legislation Monitor</td>
</tr>
<tr>
<td>LCA</td>
<td>Law Council of Australia</td>
</tr>
<tr>
<td>MEAA</td>
<td>Media, Entertainment and Arts Alliance</td>
</tr>
<tr>
<td>NTEU</td>
<td>National Tertiary Education Union</td>
</tr>
<tr>
<td>NSI Act</td>
<td>National Security Information (Criminal and Civil Proceedings) Act 2004</td>
</tr>
<tr>
<td>NSLA Bill</td>
<td>National Security Legislation Amendment Bill (No. 1) 2014</td>
</tr>
<tr>
<td>PDO</td>
<td>Preventative Detention Order</td>
</tr>
<tr>
<td>PJCHR</td>
<td>Parliamentary Joint Committee on Human Rights</td>
</tr>
<tr>
<td>PJCIS</td>
<td>Parliamentary Joint Committee on Intelligence and Security</td>
</tr>
<tr>
<td>SD Act</td>
<td>Surveillance Devices Act 2004</td>
</tr>
<tr>
<td>SIO</td>
<td>Special Intelligence Operation</td>
</tr>
<tr>
<td>TIA Act</td>
<td>Telecommunications (Interception and Access) Act 1979</td>
</tr>
</tbody>
</table>
The Bills Digest at a glance

The Counter-Terrorism Legislation Amendment Bill (No. 1) 2016 (the 2016 Bill) is the latest in a series of reforms to national security and counter-terrorism laws since mid-2014. The Government states the Bill would address issues that have come to light through recent counter-terrorism investigations and operational activity.

The 2016 Bill is comprised mainly of measures included in a 2015 Bill that lapsed on prorogation of Parliament. Those measures have been amended to implement recommendations that the Parliamentary Joint Committee on Intelligence and Security (PJCIS) made on the 2015 Bill. It also includes two new measures recommended by the Independent National Security Legislation Monitor.

Many of the proposed amendments relate to control orders. Key amendments relating to control orders include:

- lowering the minimum age at which a control order may be imposed from 16 to 14 years of age (Schedule 2)
- where a person is required under a control order to wear a tracking device, requiring the court to impose a specific set of additional requirements on the person that is designed to ensure the device remains in good working order (Schedule 3)
- introducing new ‘monitoring powers’ that would allow police to use entry, search and seizure, telecommunications interception and surveillance device powers in relation to a person subject to a control order to monitor their compliance with the order and prevent terrorist related conduct (Schedules 8, 9 and 10)

Implementation of the PJCIS recommendations relating to those measures will increase safeguards and accountability but leave the scope of the actual measures unchanged.

The 2016 Bill will also allow courts to consider information that is not disclosed to the person subject to a control order or their representative for security reasons, in control order proceedings (Part 1 of Schedule 15) and introduce a system of special advocates to represent the interests of those people in proceedings from which they and their legal representatives have been excluded (Part 2 of Schedule 15—this is a new measure). The measure in the 2015 Bill raised significant concerns about procedural fairness that the introduction of a special advocates scheme is designed to address. However, it is suggested that the particular scheme proposed in the 2016 Bill has not been subject to sufficient scrutiny to provide the Parliament with a meaningful assurance that its provisions will be workable and effective in practice.

Also new in the 2016 Bill are proposed amendments to secrecy offences relating to special intelligence operations (Schedule 18). The amendments implement the Government’s response to recommendations of the Independent National Security Legislation Monitor made in October 2015. Overall, the proposed measures are reasonably consistent with those recommendations. However, a number of ambiguities and uncertainties are also apparent in the framing and drafting of the proposed provisions.

Schedule 11 of the Bill would introduce a new offence of advocating genocide. Stakeholders have questioned the need for the offence, which would appear to overlap with several existing offences, and raised concerns about the potential for the offence to limit legitimate discussions of genocide related topics. An amendment to implement a PJCIS recommendation may mitigate concerns about the implications for free speech.

Other measures in the Bill include amending the threshold for imposing a preventative detention order by moving the focus from the imminence of a possible terrorist act to the existence of the capability for, and possibility of, a terrorist act within 14 days (Schedule 5); amending how thresholds relating to the application and issue of delayed notification search warrants apply (Schedule 14); amending the definition of advocating the doing of a terrorist act for the purpose of refusing classification to a publication, film or computer game (Schedule 13); allowing the Australian Security Intelligence Organisation to provide security assessments directly to state and territory governments and authorities (Schedule 12); and allowing taxation officers to disclose protected taxation information to Australian Government agencies for national security-related purposes (Schedule 17).
History of the Bill

An earlier version of this Bill, the Counter-Terrorism Legislation Amendment Bill (No. 1) 2015 (the 2015 Bill) was introduced into the 44th Parliament on 12 November 2015. The 2015 Bill lapsed on prorogation of Parliament before being debated in either House of Parliament. This Bill contains amendments to implement committee recommendations and includes two new measures as identified below.

Purpose and structure of the Bill

The purpose of the Counter-Terrorism Legislation Amendment Bill (No. 1) 2016 (the 2016 Bill) is to:

- amend the Criminal Code Act 1995 (Criminal Code) to:
  - expand the control order regime, including by lowering the minimum age at which a control order may be imposed from 16 to 14 years of age (Schedules 2, 3, 4 and 7)
  - modify the preventative detention order regime, including by amending the threshold for imposing a preventative detention order (Schedules 5, 6 and 7)
  - introduce a new offence of advocating genocide (Schedule 11) and
  - include additional exemptions relating to legal representation for certain terrorist organisation offences (Schedule 1).
- amend the Crimes Act 1914 (Schedule 8), Telecommunications (Interception and Access) Act 1979 (Schedule 9) and Surveillance Devices Act 2004 (Schedule 10) to introduce new monitoring powers in relation to persons subject to control orders
- amend the Australian Security Intelligence Organisation Act 1979 (ASIO Act) and the Administrative Appeals Tribunal Act 1975 to allow the Australian Security Intelligence Organisation (ASIO) to provide security assessments directly to state and territory governments and authorities (Schedule 12)
- amend the Classification (Publications, Films and Computer Games) Act 1995 (Classification Act) to change the definition of advocating the doing of a terrorist act (for the purpose of refusing classification) to be the same as the definition in the Criminal Code (Schedule 13)
- amend the Crimes Act to change how thresholds relating to the application and issue of delayed notification search warrants apply (Schedule 14)
- amend the National Security Information (Criminal and Civil Proceedings) Act 2004 (NSI Act) and the Public Interest Disclosure Act 2013 to allow courts in control order proceedings to consider information that is not disclosed to the controlee or their representative for security reasons (Part 1 of Schedule 15)
- amend the NSI Act to:
  - introduce a system of special advocates to represent the interests of a person who is the subject of a control order proceeding where that person and their legal representative have been excluded from seeing or hearing sensitive national security information (Part 2 of Schedule 15; new in the 2016 Bill) and
  - provide that orders made by a court under that Act in relevant security related circumstances will override any disclosure requirements provided by the regulations (Schedule 16).
- amend the Taxation Administration Act 1953 to allow taxation officers to disclose protected taxation information to Australian Government agencies for national security-related purposes (Schedule 17), and
- amend the ASIO Act to replace offences for unauthorised disclosure of information relating to a special intelligence operation with separate offences for people employed by ASIO and others (Schedule 18; new in the 2016 Bill).
Background

The 2016 Bill and the Criminal Code Amendment (High Risk Terrorist Offenders) Bill 2016 are the latest in a series of national security and counter-terrorism laws introduced since mid-2014.8 Previous reforms have included new and expanded offences, additional and broader powers for law enforcement and intelligence agencies, and new grounds on which dual nationals may lose their Australian citizenship.9 The Attorney-General stated that the measures in the current Bill ‘reflect lessons learned from recent counter-terrorism investigations and operational activity’.10

On 12 September 2014, Australia raised its national terror threat level from medium to high.11 In November 2015, the revised National Terrorism Threat Advisory System altered this to ‘probable’, meaning that there is credible intelligence indicating individuals or groups have both the intent and capability to conduct an attack.12 Since the threat level was raised, there has been the stabbing of two police officers in Melbourne (September 2014), the Martin Place siege (December 2014), the murder of a police accountant in Parramatta (October 2015) and a knife attack on a man in Minto (September 2016).13 Over the same period, the Australian Federal Police (AFP) and state police have conducted 19 counter-terrorism operations, resulting in 48 people being charged with terrorism and other offences, including foreign incursions and firearms offences.14 As at June 2016, ASIO was managing around 400 high priority counter-terrorism investigations, the same as June 2015 but double the June 2014 figure.15

At the time of the 2016 Bill’s introduction, estimates indicated there were around 110 Australians fighting or engaged with terrorist groups in Iraq and Syria and 200 providing support or facilitation from Australia, and that at least 58 Australians had lost their lives in the conflict.16 Around 40 Australians had returned from the conflict, most of them some time ago.17 As at 1 September 2016, the Minister for Foreign Affairs had cancelled around 180 Australian passports, suspended 33, and refused 24 to prevent Australians travelling to Iraq and Syria to take part in the conflict.18

The increase in operational activity has meant that agencies are gaining experience with powers that have been available since 2005, but were rarely used, or not used at all, until recently. Four control orders were issued in the twelve months from December 2014 to December 2015, having previously been used only twice—one in 2006 and once in 2007.19 Preventative detention orders (PDOs) were used for the first time in September 2014 as part of Operation Appleby. Three men were detained under PDOs issued under New South Wales law on 18 September 2014 and released the next day, reportedly without charge.20 In April 2015, an 18 year old was...

---

11. T Abbott (Prime Minister) and G Brandis (Attorney-General), National terrorism public alert level raised to high, media release, 12 September 2014.
17. Ibid.; Council of Australian Governments (COAG), Australia’s Counter-Terrorism Strategy: Strengthening our resilience, Commonwealth of Australia, 2015, p. 3. The Strategy, published in July 2015, indicated that over 30 Australians had returned, none of whom had subsequently been involved in ‘activities of security concern’.
detained for several days under a PDO issued under Victorian law in relation to his alleged involvement with others in the Anzac Day plot. That PDO was revoked when he was charged with a terrorism offence.\textsuperscript{21} The prosecution for that charge was dropped in August 2015, but the man remained subject to a control order and was sentenced to a 12 month good behaviour bond without conviction for weapons offences in November 2015.\textsuperscript{22}

\textbf{Implementation of COAG and INSLM recommendations}

The Attorney-General also noted the 2016 Bill would give effect to ‘a number of recommendations from the Council of Australian Governments [COAG] Review of Counter-Terrorism Legislation’.\textsuperscript{23}

\textbf{Schedules 1} and \textbf{4} will partially implement recommendations 20 and 28 respectively, as outlined in the ‘Other provisions’ and ‘Control orders’ (see ‘Issuing court’) sections of this Digest below.

COAG’s recommendation that the Government give consideration to introducing a special advocacy system for control order proceedings, reiterated by the Parliamentary Joint Committee on Intelligence and Security (PJCIS) in November 2014, was not implemented in the 2015 Bill.\textsuperscript{24} The 2016 Bill (\textbf{Part 2 of Schedule 15}) now includes amendments to establish such a system in response to recommendations of the Independent National Security Legislation Monitor (INSLM) in January 2016 and the PJCIS in February 2016 (in its report on the 2015 Bill; see further ‘Committee consideration’ below).\textsuperscript{25}

COAG released its response to the COAG Review in October 2014.\textsuperscript{26} Of the 44 recommendations relevant to Commonwealth legislation, 15 were supported (five of which were for no change), four were supported in part, and six were supported in principle.\textsuperscript{27} While some recommendations were addressed through the \textit{Terrorism Legislation Amendment (Foreign Fighters) Act 2014}, several of the recommendations supported or partially supported would remain outstanding if the 2016 Bill is passed.\textsuperscript{28}

The INSLM’s report on an inquiry into whether the additional safeguards for the control order regime set out in the COAG Review should be introduced was tabled in May 2016.\textsuperscript{29} The INSLM supported recommendation 28 (which as noted above would be partially implemented by the 2016 Bill).\textsuperscript{30} The INSLM also supported recommendation 33, which was for amendments to make it explicit that a prohibition or restriction on a person being at specified areas or places must not constitute a relocation order.\textsuperscript{31} Despite also having been supported by COAG, that recommendation is not implemented in the 2016 Bill.

\begin{flushright}
\textit{Morning Herald}, 3 December 2014, p. 9. Little information is available on these orders due to a non-publication order: P Farrell, ‘\textit{Indefinite ban on reporting of counter-terrorism preventative detention order}’, \textit{The Guardian}, (online edition), 23 September 2014.
\end{flushright}

\begin{flushright}
\end{flushright}

\begin{flushright}
S Farnsworth, ‘Harun Causевич, arrested over Anzac Day terror plot, wins bid to remove tracking device’, \textit{ABC News} (online), updated 8 July 2016. The control order , which expired on 11 September 2016, is at Attachment 1 in the judgment (with redaction) in \textit{Gaughan v Causевич [No. 2] [2016] FCCA 1693}. Control orders may only be in place for up to 12 months, but successive orders may be made in relation to the same person: \textit{Criminal Code}, section 104.16. It is not clear whether police have sought a further order on Mr Causevic.
\end{flushright}

\begin{flushright}
\end{flushright}

\begin{flushright}
\end{flushright}

\begin{flushright}
\end{flushright}

\begin{flushright}
COAG, \textit{Communique}, COAG meeting, Canberra, 10 October 2014.
\end{flushright}

\begin{flushright}
\end{flushright}

\begin{flushright}
C Barker, M Biddington, M Coombs and M Klappdor, \textit{Counter-Terrorism Legislation Amendment (Foreign Fighters) Bill 2014}, Bills digest, 34, 2014–15, Parliamentary Library, Canberra, 2014. No amendments have been made to address recommendations 1–3, 5, 7, 9–10, 18, 24, or 33, despite a positive response from COAG.
\end{flushright}

\begin{flushright}
Gyles, \textit{Control order safeguards part 2}, op. cit.
\end{flushright}

\begin{flushright}
Ibid., p. 8.
\end{flushright}

\begin{flushright}
Ibid., p. 15. The INSLM’s views on the other outstanding COAG Review recommendations were more mixed, being that they should not be supported, were not necessary, or would be desirable but not urgent.
\end{flushright}
Schedule 18 of the 2016 Bill will replace the current offences for unauthorised disclosure of information relating to a special intelligence operation with separate offences for disclosures made by people employed by ASIO and disclosures by others. This will implement recommendations made by the INSLM in a report tabled in February 2016 on the impact of the offences on journalists. See further the ‘Offences relating to special intelligence operations’ section of this Digest below.

Committee consideration

At its 14 September 2016 meeting, the Senate Standing Committee for Selection of Bills deferred consideration of the 2016 Bill to its next meeting.

Parliamentary Joint Committee on Intelligence and Security

2015 Bill

The PJCIS inquired into the 2015 Bill and reported on 15 February 2016. The report included 20 substantive recommendations for amendments to the 2015 Bill and Explanatory Memorandum. The Government stated in July 2016 that following consultation with state and territory governments, it accepted all of the recommendations and would amend the Bill accordingly before reintroducing it early in the next Parliament.

The PJCIS’s recommendations are reflected in the 2016 Bill through changes relating to control orders and associated monitoring powers, control order proceedings (including the introduction of a special advocates scheme), preventative detention orders, the offence of advocating genocide, security assessments by ASIO and disclosure of certain tax information. Further detail is provided in the analysis of the Bill’s Schedules.

Special intelligence operations

The Attorney-General referred the National Security Legislation Amendment Bill (No. 1) 2014 (NSLA Bill) to the PJCIS for inquiry and advisory report in July 2014. This was further to the PJCIS’s inquiry into potential reforms to national security legislation, including a proposal to develop the SIO scheme, in the 43rd Parliament on the referral of the former Attorney-General in 2012.

In its 2013 report on the latter inquiry, the PJCIS recommended that the Government develop the SIO scheme, subject to comparable limitations and safeguards applying to the ‘controlled operations’ scheme in Part 1AB of the Crimes Act 1914. This scheme authorises the Australian Federal Police to conduct covert operations for the purpose of investigating and obtaining admissible evidence in relation to certain serious offences. Sections 15HK and 15HL of the Crimes Act contain offences for the unauthorised disclosure of information relating to a controlled operation, upon which section 35P of the ASIO Act is modelled.

In its report on the NSLA Bill in September 2014, the PJCIS did not recommend major amendments to the text of section 35P. It acknowledged concerns of stakeholders about the potential impacts of the offences on freedom of expression (including in relation to journalists and “whistleblowers”).

The PJCIS concluded, however, that interests in freedom of expression and protecting sensitive information could be managed adequately through the fault elements and criminal standard of proof applying to the offences, and administrative requirements under the Prosecution Policy of the Commonwealth which provide that the Commonwealth Director of Public Prosecutions (CDPP) must be satisfied that the commencement or continuation of a prosecution would be in the public interest. The PJCIS recommended some relatively minor

34. PJCIS, Advisory report on the Counter-Terrorism Legislation Amendment Bill (No. 1) 2015, op. cit.
35. M Turnbull (Prime Minister) and G Brandis (Attorney-General), Strengthening counter-terrorism legislation, media release, 25 July 2016.
38. Ibid., pp. 108-112 (recommendation 28).
40. Ibid., pp. 51, 55 and 61-63.
41. As to which, see: Commonwealth Director of Public Prosecutions (CDPP), ‘Prosecution policy of the Commonwealth: Guidelines for the making of decisions in the prosecution process’, CDPP website, pp. 5–6.
amendments, including to broaden the scope of exceptions to enable disclosures for the purpose of obtaining legal advice, and making complaints to the Inspector-General of Intelligence and Security (or staff). 42

**Senate Standing Committee for the Scrutiny of Bills**

The Senate Standing Committee for the Scrutiny of Bills (Scrutiny of Bills Committee) had not yet reported on the 2016 Bill as at the date of publication of this Digest. However, the Scrutiny of Bills Committee had concerns about several measures in the 2015 Bill43, some of which would be at least partly addressed by the implementation in the 2016 Bill of the PJCIS’s recommendations. Among the key concerns it raised that remain relevant to the 2016 Bill were:

- the impact of proposed restrictions on access to national security information in control order proceedings on access to natural justice, including the right to a fair hearing, and the potential need for further safeguards in these situations44
- in relation to preventative detention orders, the proposed shift in the test that applies to when a terrorist attack is considered imminent ‘from an expectation that an attack will occur to a conclusion about the capability for an attack to be carried out’45 and
- the ability to use things seized, information obtained or a document produced under the proposed monitoring powers for persons subject to control orders in certain circumstances where the relevant interim control order has been declared void by a court.46

The Scrutiny of Bills Committee was not persuaded by further information from the Attorney-General that the amendments relating to access to national security information now in Part 1 of Schedule 15 provide an appropriate balance between national security concerns and procedural fairness in control order proceedings.47 However, it did consider that implementing the PJCIS’s recommendations on those provisions ‘may represent an improvement to the Bill as currently drafted’.48

The Scrutiny of Bills Committee supported the PJCIS’s recommendation that for the proposed advocating genocide offence (in Schedule 11) to apply, a person must be reckless as to whether another person might act accordingly. It expressed some concern about the PJCIS’s recommendation to remove the requirement that the advocacy was engaged in ‘publicly’, but left the question of the most appropriate approach to the Senate as a whole.49 Both recommendations will be implemented by the 2016 Bill.

The Scrutiny of Bills Committee, in its consideration of the National Security Legislation Amendment Bill (No 1) 2014 (‘NSLA Bill’), identified section 35P as potentially trespassing unduly on personal rights and liberties (namely freedom of expression). It drew the provision to the attention of the Senate, together with the response of the Attorney-General.50

**Policy position of non-government parties/independents**

As at the time of writing this Digest, the Australian Labor Party did not appear to have publicly stated its support or otherwise for the 2016 Bill. However, it had stated that it will continue to work constructively with the Government on national security legislation.52 Implementation of all of the PJCIS’s recommendations on the

---

42. Ibid., pp. 61-63, recommendations 11-13.
44. Ibid., pp. 176–183.
45. Ibid., pp. 147–150.
46. Ibid., pp. 154–158.
47. Ibid., p. 180.
48. Ibid., pp. 181–182.
49. Ibid., pp. 168–171.
50. For information about the NSLA Bill and its enactment, see: Parliament of Australia, ‘National Security Legislation Amendment Bill (No. 1) 2014 homepage’, Australian Parliament website. The NSLA Bill was passed on 1 October 2014 and received the Royal Assent on 2 October 2014, as the National Security Legislation Amendment Act (No. 1) 2014, Schedule 3 (special intelligence operations, including section 35P) commenced on 30 October 2014. Also see C Barker and M Biddington, National Security Legislation Amendment Bill (No. 1) 2014, Bills digest, 19, 2014–15, Parliamentary Library, Canberra, 2014.
In October 2015, ahead of the 2015 Bill’s introduction, the Australian Greens questioned the need to lower the minimum age at which control orders may be imposed and called on the Government to provide evidence to support its proposal.\textsuperscript{53}

In the 44th Parliament, some members of the cross-bench opposed the enactment of section 35P of the ASIO Act (to be amended by Schedule 18) during the debate of the NSLA Bill. They moved various amendments to remove the provision from the NSLA Bill, or alternatively to include exceptions or defences, and ultimately voted against the NSLA Bill.\textsuperscript{54}

In addition, while Labor supported the enactment of section 35P as part of the NSLA Bill, some members have individually expressed their concern that the offences could have a harsh and oppressive effect on journalists and others seeking to report, or participate in public discussion, on national security matters.\textsuperscript{55} The Leader of the Opposition reportedly wrote to the Prime Minister on 29 October 2014, requesting the Prime Minister to refer section 35P to the INSLM for inquiry and report.\textsuperscript{56}

**Position of major interest groups**

The views of major interest groups, in particular law groups and legal experts, civil liberties and human rights organisations and the Inspector-General for Intelligence and Security (IGIS) on most of the measures in the 2016 Bill, are set out in their submissions and evidence to the PJCIS’s inquiry into the 2015 Bill and summarised in the PJCIS’s report on the inquiry. Some of the concerns raised by stakeholders about the 2015 Bill will be addressed in the 2016 Bill through implementation of the PJCIS’s recommendations on the 2015 Bill.

A summary is provided below, with stakeholder views also incorporated into the analysis of the Bill’s Schedules where relevant.

**Control orders**

Councils for civil liberties (in a joint submission), the Law Council of Australia (LCA), Gilbert + Tobin Centre of Public Law (Gilbert + Tobin), Amnesty International, and the Victorian Bar and Criminal Bar Association of Victoria (Victorian Bar and CBA) restated their ongoing opposition to the control order regime as a whole in their submissions to the PJCIS inquiry into the 2015 Bill.\textsuperscript{57}

---


56. L Bourke, *’Bill Shorten writes to Tony Abbott with concerns that terror laws could see journalists face jail’*, *Sydney Morning Herald*, (online edition) 30 October 2014. (The author also uploaded a copy of the letter.)

57. L Bourke, *’Bill Shorten writes to Tony Abbott with concerns that terror laws could see journalists face jail’*, *Sydney Morning Herald*, (online edition) 30 October 2014. (The author also uploaded a copy of the letter.)

---
Lowering the minimum age to 14 years old

The proposal to lower the minimum age for control orders attracted attention when it was formally announced in October 2015. 58

Several Muslim community representatives expressed concerns that extending control orders to people as young as 14 years of age could be counterproductive, further alienating already disaffected teenagers and damaging community-police relations. 59 Those concerns were shared by the National Children’s Commissioner, who also considered control orders had the potential to disrupt children’s education and participation in community life and argued it was preferable to work with communities to divert children from antisocial pathways. 60 Similar objections are set out in the submissions of the Muslim Legal Network (NSW), the Victorian Bar and CBA and councils for civil liberties to the PJCIS inquiry into the Bill. 61

The former INSLM, Bret Walker SC, stated that in terms of an appropriate minimum age, there is no ‘magic number’, but that there was no evidence on which to reasonably argue that this measure would make Australia safer. 62 The LCA and some other legal experts have raised similar questions about the likely efficacy of the measure. 63

Professor Greg Barton argued that control orders could play a legitimate role in diverting young people from a violent extremist path, but that they could only be effective if used alongside community-based solutions: ‘Control orders are a temporary measure, not a permanent solution, and if not used wisely can cause more harm than good. Working with family and community, however, they may just make a vital difference’. 64 Levi West considered control orders the ‘least bad’ option compared to alternatives such as lowering the evidentiary threshold for prosecution, and their application to some young people an ‘unfortunate necessity’. 65

Human rights and legal organisations and councils for civil liberties considered the amendments as introduced in 2015 did not properly implement Australia’s obligations under the United Nations Convention on the Rights of the Child, including ensuring the interests of the child are a primary consideration in all proceedings. 66 The 2016 Bill will implement recommendation 1 of the PJCIS’s report on the 2015 Bill by requiring the best interests of the child to be a primary consideration.

Several stakeholders opposed the court appointed advocate scheme in the 2015 Bill. 67 This has been removed in the 2016 Bill and replaced with amendments to explicitly provide that a young person has the right to legal representation in control order proceedings and a system of special advocates, implementing recommendations 2 and 5 of the PJCIS’s report on the 2015 Bill. 68

Monitoring powers

The Australian Human Rights Commission (AHRC) and the Muslim Legal Network (NSW) opposed the proposed monitoring powers in Schedules 8, 9 and 10. They did not consider persons subject to control orders should be...
subject to powers such as entry, search and seizure, telecommunications interception and surveillance devices in the circumstances proposed in the Bill. The Muslim Legal Network (NSW) considered Schedule 8 to go well beyond monitoring compliance with orders and to be ‘clearly designed to operate as an investigative extension of the control order provisions’. The INSLM took a similar view, stating ‘[t]he details of the potential monitoring blur, if not eliminate, the line between monitoring and investigation’. The INSLM further considered:

The case for control orders is weakened if control orders are of little utility without such far reaching surveillance. It is difficult to imagine such provisions being applied to an accused on bail. The significance for present purposes is to emphasise the seriousness of the impact upon a person of the grant of a control order if these changes come into force and the consequent necessity for proper safeguards of the interests of a potential controlee.

While not opposing the monitoring powers entirely, the LCA and Gilbert + Tobin considered the proposed thresholds at which they could be accessed to be too low and the powers themselves too broad, including in their potential impact on third parties. Councils for civil liberties raised similar concerns, and recommended the provisions not proceed in their current form.

Implementation of the PJCIS’s recommendations 9, 13 and 14 will go some way to addressing some of those concerns by requiring consideration to be given prior to authorisation to whether the exercise of powers would be likely to have the least interference with privacy (and in the case of search powers, also liberty) of any person. However, most of the PJCIS’s recommendations on Schedules 8, 9 and 10 (which will be implemented in the 2016 Bill) related to improved accountability for, and oversight of, the proposed powers, as opposed to the their scope and the thresholds at which they will be available.

Gilbert + Tobin also considered the amendments could make it more likely for a court to conceive of the control order regime as punitive and therefore unconstitutional.

National security information in control order proceedings

The AHRC, Gilbert + Tobin, the Muslim Legal Network, Australian Lawyers for Human Rights (ALHR) and the LCA also stated concerns with provisions now in Part 1 of Schedule 15 of the 2016 Bill. In particular, that withholding information from the defence in control order proceedings posed a threat to procedural fairness by not allowing a defendant to rebut allegations or otherwise adequately defend themselves.

The 2016 Bill will implement recommendations 4 (minimum standard of disclosure) and 5 (special advocates, also a recommendation of the COAG Review and the INSLM) of the PJCIS’s report on the 2015 Bill. This should largely address the concerns raised in relation to these provisions in the 2015 Bill. However, the 2016 Bill will not implement the INSLM’s recommendation that Part 1 of Schedule 15 not commence until a special advocates scheme has been implemented.

Following the introduction of the 2016 Bill, the LCA welcomed the inclusion of the special advocates scheme (Part 2 of Schedule 15). It also called for an immediate review of the special advocate scheme by the PJCIS.
Offences relating to special intelligence operations

At the time of writing, major interest groups do not appear to have made substantial public comments on the text of the proposed amendments to section 35P of the ASIO Act, as contained in Schedule 18 to the 2016 Bill.

However, major non-government stakeholders—including media organisations, civil liberties organisations, and members of the legal profession and academia—opposed the enactment of section 35P in 2014.80 Several interest groups and individuals continued to express their criticism after its enactment.81 They also made submissions to the INSLM’s inquiry into the provision in 2015, supporting its repeal or amendment.82

Some interest groups and individuals have commented on the INSLM’s recommendations to retain section 35P subject to several amendments.83 Some have argued that the recommendations do not go far enough to provide certainty to journalists and others to know what information may be disclosed without exposure to criminal liability, or protect journalists and ‘whistleblowers’ who seek to disclose allegations of wrongdoing in the course of an SIO.84

Other measures

Preventative detention orders

Some stakeholders raised concerns about the proposed change in the 2015 Bill to when a terrorist act is considered to be imminent for the purposes of the preventative detention order (PDO) regime. The AHRC, LCA and councils for civil liberties considered it would lower the threshold in such a way as to make PDOS available in a much broader range of circumstances, taking the scheme beyond the purpose for which it was enacted.85

As per recommendation 15 of the PJCIS’s report on the 2015 Bill, the word ‘imminent’ has been removed entirely in Schedule 5 of the 2016 Bill. However, the 2016 Bill will lower the threshold at which PDOS may be made in the same way as would the 2015 Bill.

Offence of advocating genocide

Stakeholders raised concerns that the offence of advocating genocide proposed in Schedule 11 may infringe on free speech and could limit legitimate discussions of related topics. Submissions also pointed out that several existing related offences appeared to adequately criminalise the behaviour and it was not clear what benefit the new offence would provide.86

Some stakeholders also considered that the threshold required for proving the offence was inappropriately low (particularly as the person need not intend that the genocide be committed), and should be in line with those for incitement and urging violence.87 This concern is addressed in the 2016 Bill through implementation of

---

82. See generally, INSLM, Submission—review into section 35P of the ASIO Act, INSLM website.
84. See, for example, MEAA, Journalists still face jail under ASIO Act changes, op. cit. (MEAA CEO Paul Murphy stated, ‘the Monitor’s report, while welcome, has not changed the fundamental intent of section 35P, which is to intimidate whistleblowers and journalists.’)
85. AHRC, Submission to PJCIS, op. cit., pp. 14–16; LCA, Submission to PJCIS, op. cit., pp. 15–16; Joint submission by Australian councils for civil liberties, Submission to PJCIS, op. cit., pp. 11–12. Gilbert + Tobin continued to object to the PDO regime as a whole, but did not oppose this amendment (Submission to PJCIS, op. cit., p. 7).
86. Muslim Legal Network (NSW), Submission to PJCIS, op. cit., pp. 35–38; Gilbert + Tobin, Submission to PJCIS, op. cit., pp. 11–12; AHRC, Submission to PJCIS, op. cit., pp. 20–22; LCA, Submission to PJCIS, op. cit., pp. 23–26; Joint Media Organisations, Submission to PJCIS, Inquiry into the Counter-Terrorism Legislation Amendment Bill (No. 1) 2015, 10 December 2015, p. 2; Joint submission by Australian councils for civil liberties, Submission to PJCIS, op. cit., p. 17.
87. Muslim Legal Network (NSW), Submission to PJCIS, op. cit., p. 36; Gilbert + Tobin, Submission to PJCIS, op. cit., p. 11.
recommendation 17 of the PJCIS’s report on the 2015 Bill. A person will now need to be reckless as to whether another person might engage in genocide on the basis of his or her advocacy for the offence to be proven.

Classification of publications
The LCA, Blueprint for Free Speech and councils for civil liberties raised concerns with the proposal to amend the definition of advocating the doing of a terrorist act in the Classification Act (for the purpose of refusing classification) to be the same as the broader definition in the Criminal Code. Concerns centred on the potential for the more expansive definition to limit freedom of expression by also restricting legitimate discussion of the issues. Blueprint for Free Speech also questioned whether the change would have the desired impact on public safety.

Financial implications
The Explanatory Memorandum states that the 2016 Bill will have ‘little financial impact on Government expenditure or revenue’, but provides no further explanation. The Explanatory Memorandum to the 2015 Bill stated that it would have no financial impact. It appears that either the Government has become more cautious about such statements or that it anticipates that the introduction of a special advocates system (Part 2 of Schedule 15), changes to offences relating to special intelligence operations (Schedule 18), or amendments to address the PJCIS’s recommendations (possibly additional oversight functions imposed on the Ombudsman) could have a small financial impact.

Special advocate scheme
The task of recruiting and security clearing a panel of lawyers who are available to perform the functions of special advocates is likely to be resource intensive. The need to ensure that special advocates have access to appropriate administrative support will also have resource implications.

The Government also does not appear to have provided any commitment or assurance that existing legal aid or legal assistance funding (or court funding) will not be diverted or otherwise effectively reduced to meet the establishment or operational costs of a special advocates scheme.

Statement of Compatibility with Human Rights
As required under Part 3 of the Human Rights (Parliamentary Scrutiny) Act 2011 (Cth), the Government has assessed the 2016 Bill’s compatibility with the human rights and freedoms recognised or declared in the international instruments listed in section 3 of that Act. The Government considers that the 2016 Bill is compatible.

Parliamentary Joint Committee on Human Rights
The Parliamentary Joint Committee on Human Rights (PJCHR) had not yet reported on the 2016 Bill as at the date of publication of this Digest. However, the PJCHR had some significant concerns in relation to parts of the 2015 Bill, some of which were allayed by further information provided by the Attorney-General, some of which would be mitigated by the implementation in the 2016 Bill of the PJCIS’s recommendations, and some of which would remain outstanding.

The PJCHR also considered section 35P of the ASIO Act, as part of the NSLA Bill, in the 44th Parliament. The PJCHR concluded that section 35P was incompatible with the right to freedom of expression in Article 19(2) of the International Covenant on Civil and Political Rights.

---

89. Explanatory Memorandum, Counter-Terrorism Legislation Amendment Bill (No. 1) 2015, p. 2.
90. Explanatory Memorandum, Counter-Terrorism Legislation Amendment Bill (No. 1) 2015, p. 2.
91. All of the other measures in the 2016 Bill were also in the 2015 Bill.
92. The Statement of Compatibility with Human Rights can be found at page 3 of the Explanatory Memorandum to the 2016 Bill.
Control orders
The PJCHR remained concerned about the compatibility of the control order regime more broadly with Australia’s human rights obligations. In relation to the 2015 Bill, following legal advice provided to the PJCHR and further information from the Attorney-General, disagreement remained between committee members as to whether or not the amendments allowing control orders to be imposed on people from the age of 14 years were compatible with international human rights law.

The PJCHR supported in principle the PJCIS’s recommendations to remove the role of court-appointed advocates and to expressly provide that young people have a right to legal representation in control order proceedings. Both recommendations will be implemented by the 2016 Bill.

Preventative detention orders
The PJCHR considered that removing the requirement for a terrorist act to be imminent before a PDO can be imposed may be incompatible with the right to liberty. Further, it was of the view that implementing the PJCIS’s recommendation on this amendment, rather than being an improvement, would actually ‘further weaken the nexus between PDOs and imminent threats to life’.

Monitoring powers in relation to people subject to control orders
The PJCHR had several concerns relating to the monitoring powers in relation to people subject to control orders, which include search and seizure, telecommunications interception and surveillance devices. It considered the PJCIS’s recommendations on those powers (which will be implemented in the 2016 Bill) would provide important safeguards and stated that it would welcome their implementation. However, some of the PJCHR’s concerns may not be fully addressed in the 2016 Bill:

The committee remains concerned that insufficient safeguards exist to protect the right to privacy. In particular, monitoring warrants can be issued without any reasonable suspicion that the relevant person is doing anything suspicious or unlawful; B-Party warrants involve a significant intrusion into non-suspect’s right to privacy; and the deferred reporting arrangements limit the transparency surrounding the use of such intrusive measures.

National security information
The PJCHR considered the proposed restrictions on access to national security information in control order proceedings would limit the right to a fair hearing. The PJCHR concluded that the implementation of the PJCIS’s recommendations would address its concerns if a special advocates scheme was in place before those restrictions commenced. In the 2016 Bill, the special advocates scheme in Part 2 of Schedule 15 could commence up to 12 months after the further restrictions on access to national security information in Part 1 of the same Schedule.

Amendments relating to control orders (Schedules 2, 3, 4 and 15)
Control orders have been part of the Australian anti-terrorism framework since December 2005. Reforms passed in 2014 expanded both the grounds on which orders may be sought and the purposes for which they may be granted. There are now several grounds on which an order may be sought, most of which relate not to what might be prevented by an order, but to what the police and the court are satisfied a person has already done (such as having trained with a terrorist organisation, having engaged in hostile activity in a foreign country

96. Ibid., pp. 94–105. It is not clear from the PJCHR’s report whether it sought advice separately or whether the legal advice to which it refers was provided by the Government.
97. Ibid., pp. 105–108.
98. Ibid., pp. 108–114.
99. Ibid., pp. 114–121.
100. Ibid., p. 123.
or provided support for someone else to do so).\textsuperscript{104} Further, while the obligations, prohibitions and restrictions to be imposed on a person under a control order must still serve some protective or preventative purpose, that now extends to preventing support for, or facilitation of, a terrorist act or engagement in hostile activity in a foreign country.\textsuperscript{105} The types of obligations, prohibitions and restrictions that may be imposed under a control order include a curfew at a particular address, wearing of an electronic tracking device, restrictions on use of telecommunications, prohibitions or restrictions on associating or communicating with certain people and regular reporting to police.\textsuperscript{106}

**Lowering the minimum age for a control order to 14 years old (Schedule 2)**

Currently, a control order may not be applied to anyone under 16 years of age.\textsuperscript{107} Schedule 2 of the Bill will lower the minimum age at which a control order may be imposed from 16 to 14 years of age.\textsuperscript{108}

**Policy position**

Australian security intelligence and law enforcement agencies have advised that terrorist organisations, particularly Islamic State, are targeting propaganda and recruitment activities at a younger audience than was previously the case.\textsuperscript{109} The Attorney-General told the Senate he had signed warrants under the ASIO Act in relation to people as young as 14 years of age ‘on more than one occasion’.\textsuperscript{110} The AFP Commissioner confirmed in October 2015 that a twelve year old boy was ‘on the police radar’ in relation to possible terrorist activity.\textsuperscript{111} While not previously on the agencies’ radar and therefore not a candidate for a control order, the shooter who killed NSW Police accountant Curtis Cheng, Farhad Jabar, was 15 years old.\textsuperscript{112} Another 15 year old was charged with conspiracy to conduct an act in preparation for a terrorist act on 10 December 2015.\textsuperscript{113}

The AFP considers that control orders have a role to play in diverting young people who are beyond the point where they might be receptive to voluntary intervention from contact with the formal criminal justice system:

Lower intensity interventions such as voluntary participation in community-based programs are appropriate where a person is not considered to pose a risk to public safety. However, as valuable as such programs are, they are not appropriate when a person is not willing to voluntarily change their behaviours, and their activities indicate that the person is further down the path of radicalisation and is at risk of engaging in terrorist activity. Control orders can play an important role in providing a mechanism to manage and mitigate the risk posed by an individual where laying charges is not justified by the evidence available at a particular point in time, and the person would otherwise be unwilling to take steps to change their behaviour.\textsuperscript{114}

The age of criminal responsibility under Australia federal law is generally set at 14 years of age (though a child aged 10 years or more may be held criminally responsible if it can be proven that the child knew his or her conduct was wrong).\textsuperscript{115}

**Counter-arguments**

As noted in the ‘Position of major interest groups’ section above, some stakeholders have questioned the efficacy of control orders generally, and therefore the expansion of the regime, and cautioned that using control orders against younger teenagers could be counter-productive.

\textsuperscript{104} [Criminal Code], subsection 104.2(2), section 104.3 and paragraph 104.4(1)(c).

\textsuperscript{105} Ibid., section 104.1 and subsection 104.4(1).

\textsuperscript{106} Ibid., subsection 104.5(3).

\textsuperscript{107} Ibid., subsection 104.28(1).

\textsuperscript{108} Item 30 of Schedule 2, amendment to subsection 104.28(1).

\textsuperscript{109} ASIO, Report to Parliament 2014–15, op. cit., pp. ix, 3–4; M Turnbull (Prime Minister) and M Keenan (Justice Minister), Prime Minister meets states and territories to address radicalisation of young people, 7:30, transcript, ABC, 15 October 2015; AAP, ‘Boy, 12, on terror list’, West Australian, 15 October 2015, p. 6; L Wilson, ‘Fresh-faced westerners are being lured into terrorism by ISIS propaganda’, News.com.au, 16 March 2015.

\textsuperscript{110} G Brands, ‘Answer to Question without notice: national security’, [Questioner: N McKim], Senate, Debates, 14 October 2015, p. 7626.

\textsuperscript{111} Turnbull and Keenan, Prime Minister meets states and territories to address radicalisation of young people, op. cit.

\textsuperscript{112} N Ralston, A Benny-Morrison and R Olding, ‘Teen shooter unknown to police’, The Sun Herald, 4 October 2015, p. 3.

\textsuperscript{113} AFP and NSW police, Two men charged in Operation Appleby investigation, joint media release, 10 December 2015.

\textsuperscript{114} AFP, Submission to PJCIS, Inquiry into the Counter-Terrorism Legislation Amendment Bill (No. 1) 2015, December 2015, p. 5.

\textsuperscript{115} Criminal Code, sections 7.1 and 7.2. Doli incapax will act as a rebuttable presumption in these circumstances.
In its report on the 2015 Bill, the PJCHR noted there is some doubt about whether control orders are an effective tool to begin with, but concedes there have been ‘significant recent developments in the counter-terrorism space’. Nonetheless, the PJCHR retained some doubt as to whether the extension of the scheme to children aged 14 and 15 years is a proportionate response, rationally connected to a legitimate objective. Concerns about the necessity and proportionality of imposing control orders on young people were also raised in submissions to the PJCIS by human rights and legal organisations, including the AHRC and the LCA.

PJCIS view on lowering the minimum age

The PJCIS noted concerns about proportionality raised by some stakeholders, but in light of recent events and evidence from law enforcement, found lowering the minimum age at which a control order may be imposed to be ‘justified and in principle, a reasonable and necessary measure for protecting the community from harm’.

Maximum period for control orders imposed on minors

The only additional protection currently in place for minors subject to a control order is the maximum time the order may be in effect, which is three instead of twelve months for persons 16 or 17 years of age. A maximum period of three months will continue to apply to control orders imposed on persons under 18 years of age. As is currently the case, this does not prevent the making of successive control orders in relation to the same person. Councillors for civil liberties recommended there be a limit of one successive control order able to be made against a person under 18 years of age, while the Muslim Legal Network (NSW) recommended they not be permitted at all in relation to young people. The Attorney-General’s Department (AGD) responded to those suggestions, stating that ‘[t]he function and purpose of control orders would be seriously hindered’ if successive orders could not be made when the relevant thresholds were met.

Consideration of the best interests of the child

A court imposing an interim control order on a person 14 to 17 years of age will be required to take into account the best interests of the child as a primary consideration when determining whether each proposed obligation, prohibition or restriction is reasonably necessary and reasonably appropriate and adapted to the purposes of a control order. It will need to take into account the objects of the control order regime as a paramount consideration, and the impact on the person’s circumstances as an additional consideration. In giving consideration to the best interests of the child, the court must consider particular rights and characteristics, including the right to receive an education and the benefit of meaningful relationships with family and friends, along with any other relevant matter. The 2016 Bill responds to recommendation 1 of the PJCIS report on the 2015 Bill, that the best interests of a young person be a primary consideration (not just ‘a consideration’) and the safety and security of the community a paramount consideration. This should go some way to addressing concerns about this aspect of the Bill raised by the PJCHR and echoed by the AHRC, LCA, Gilbert + Tobin, UNICEF Australia, ALHR and councils of civil liberties.

117. Ibid., pp. 94–100.
118. AHRC, op cit., pp. 9–10; LCA, Submission to PJCIS, op cit., pp. 6–7; Amnesty International, op. cit.; Victorian Bar and CBA, op. cit., p. 2; UNICEF Australia, op. cit.
119. PJCIS, Advisory report on the Counter-Terrorism Legislation Amendment Bill (No.1) 2015, op. cit., pp. 43–44.
120. Criminal Code, subsection 104.28(2).
121. Ibid., section 104.28(3).
122. Joint submission by Australian councils for civil liberties, op. cit., p. 8; Muslim Legal Network (NSW), op. cit., p. 11. It is unclear from the submission whether ‘young people’ is intended to refer only to 14 and 15 year olds, or also 16 and 17 year olds.
123. Attorney-General’s Department (AGD), Supplementary submission to the PJCIS, Inquiry into the Counter-Terrorism Legislation Amendment Bill (No.1) 2015, January 2016, p. 13.
124. Item 3 of Schedule 2, repeal and replacement of subsection 104.4(2) of the Criminal Code.
125. The objects of the control order regime are to allow a control order to be imposed on a person for one or more of the following purposes: 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—section 104.1 of the Criminal Code.
126. Item 3 of Schedule 2, proposed subsection 104.4(2A) of the Criminal Code.
128. PJCHR, Thirty-sixth report of the 44th Parliament, op cit., p. 92; AHRC, Submission to PJCIS, op cit., pp. 12–13; LCA, Submission to PJCIS, op. cit., p. 9; Gilbert + Tobin, Submission to PJCIS, op. cit., pp. 3–4; UNICEF Australia, Submission to PJCIS, op. cit., p. 2; Joint submission by Australian councils for civil liberties, Submission to PJCIS, op. cit., pp. 7–8; ALHR, Submission to PJCIS, op. cit., pp. 4–5.
The PJCHR also questioned the compatibility of the provisions in the 2015 Bill with children’s rights because those rights must be considered only in the context of the proposed obligations, prohibitions and restrictions, not the initial determination of whether the order is necessary. In a supplementary submission, AGD stated that the best interests of the child should not be a consideration in that initial determination, as it would ‘fundamentally change the purpose of the test.’

The requirements to give paramount consideration to the objects of the control order regime and primary consideration to the best interests of a young person will also be applied to variations that would add further obligations, prohibitions or restrictions to an existing control order.

Right to legal representation

The 2015 Bill would have introduced independent court appointed advocates for persons 14 to 17 years of age where an interim control order had been imposed. While it was intended to operate as a safeguard, the PJCHR, INSLM and submitters to the PJCIS inquiry into the 2015 Bill raised issues in relation to the proposed scheme, including that it could adversely impact the child instead of helping to protect his or her interests. Those concerns were shared by the PJCIS, which recommended the role of court appointed advocate be removed and amendments made instead ‘to expressly provide that a young person has the right to legal representation in control order proceedings’ (recommendation 2). There was nothing in the existing legislation to prevent a young person (or adult) seeking legal advice or representation in relation to a control order, but the PJCIS considered it desirable for those rights to be made explicit.

The PJCIS’s recommendation is reflected in the 2016 Bill and a proposed Government amendment to the 2016 Bill. Item 5 of Schedule 2 (proposed subparagraph 104.12(1)(b)(iii)) will require that an AFP member serving an interim control order on any person must inform them that he or she has a right to obtain legal advice and legal representation. A Government amendment would require an issuing court to appoint a lawyer to act for a person aged 14–17 years of age in control order proceedings if the young person does not already have one (proposed subsection 104.28(4)). The requirement will not apply to ex parte proceedings for an interim order or where the young person has refused a lawyer previously appointed under the proposed provisions (proposed subsection 104.28(5)).

Service of orders on parents and guardians

The 2016 Bill will implement recommendation 3 of the PJCIS’s report on the 2015 Bill by requiring an AFP member to take reasonable steps to personally serve copies of all documents relating to a control order imposed on a 14–17 year old on at least one parent or guardian (in addition to the young person), including interim and confirmed orders, revocation or variations of an order and associated applications.

Reporting

The Attorney-General is required to table an annual report detailing statistical information relating to control orders made in each financial year. The 2016 Bill will require that report to include those statistics specifically for control orders made in relation to persons 14 to 17 years of age.

Additional comment

130. AGD, Supplementary submission, op. cit., p. 7.
131. Item 26 of Schedule 2, repeal and replacement of subsection 104.24(2) and proposed subsection 104.24(2A).
134. Counter-Terrorism Legislation Amendment Bill (No. 1) 2016, Proposed amendment [sheet ZA417].
136. Criminal Code, section 104.29.
137. Item 34 of Schedule 2, proposed paragraph 104.29(2)(j).
While some additional safeguards are being provided in terms of the making of a control order in relation to someone 14 to 17 years of age, the ‘monitoring’ powers proposed in Schedules 8, 9 and 10 of the 2016 Bill and the offence for intentionally breaching a control order (with a maximum penalty of five years imprisonment) will apply to minors in the same way as adults.

**Tracking devices (Schedule 3)**

One of the obligations that may be imposed on a person under a control order is the wearing of a tracking device.\(^{138}\)

Schedule 3 of the Bill will provide that when a court requires a person subject to a control order to wear a tracking device, it must also impose a specific set of requirements on that person, and authorise an AFP member to do certain things, to ensure the device remains in good working order. It will also introduce new offences for interference with, or disruption or loss of function of, a tracking device.

**Proposed subsection 104.5(3A) lists the requirements to be imposed on a person required to wear a tracking device (including taking both steps specified in the control order and ‘reasonable steps’ to ensure the device and any related equipment remain in good working order). Intentionally contravening any of those requirements would constitute an offence punishable by up to five years imprisonment under existing section 104.27.**\(^{139}\)

**Proposed subsection 104.5(3B) requires the court to authorise an AFP member to take steps specified in the control order to ensure the device and associated equipment remain in good working order and to enter one or more premises specified in the order to install any necessary equipment. The two sets of requirements have been separated to address ambiguities in the 2015 Bill as per the first part of recommendation 8 of the PJCIS’s report on the 2015 Bill.**\(^{140}\)

**Stakeholder concerns**

The Queensland Government raised concerns about the application of this measure to 14–17 year olds in its submission on the 2015 Bill. In particular, it did not consider it appropriate that a court not have the discretion to amend the requirements to take account of the particular circumstances of a child.\(^{141}\) In response, AGD stated that given the requirement for a court to be satisfied that all the obligations imposed in an order are reasonably necessary, appropriate and adapted, a court would only require a child to wear a tracking device if it was satisfied that all of those supplementary requirements met that threshold.\(^{142}\)

The LCA and Gilbert + Tobin had concerns about the lack of clarity around what constitutes ‘reasonable steps’.\(^{143}\) Muslim Legal Network (NSW) and Gilbert + Tobin also objected to the requirement to alert the AFP if a person becomes aware that the device or any associated equipment is not in good order within four hours, arguing that a person may not have the technical knowledge to fulfil such a requirement.\(^{144}\) Gilbert + Tobin suggested that if the amendments are proposed to address concerns about devices being disabled, the more appropriate solution would be a clear prohibition on interference with the device.\(^{145}\)

**PJCIS view**

The PJCIS recommended amendments to the Explanatory Memorandum to include examples of what would constitute reasonable steps. Examples have been included in the Explanatory Memorandum to the 2016 Bill, including notifying the AFP if the device becomes too loose to wear or makes uncommon sounds.\(^{146}\)

The PJCIS also recommended inclusion of ‘a clear prohibition on interfering with a tracking device required to be worn by the subject of a control order’ (the second part of recommendation 8).

---

139. *Criminal Code*, section 104.27 (offence) and subsection 5.6(1) (default fault element for a physical element consisting of conduct is intent).
144. Gilbert + Tobin, *Submission to PJCIS*, op. cit., p. 6; Muslim Legal Network (NSW), *Submission to PJCIS*, op. cit., p. 12.
New offences
The Government has responded to that PJCIS recommendation by introducing two new offences (item 3 of Schedule 3).

The first offence will apply if a person subject to a control order is required to wear a tracking device, and that person engages in conduct that results in interference with, or disruption or loss of function of, the tracking device.\(^{147}\) The offence will only apply where the person engages in the conduct intentionally and is reckless as to whether it will have that result specified in the offence.\(^{148}\) The conduct can be an act or an omission.\(^{149}\) The second offence is an equivalent offence for a person other than the subject of a control order interfering with the tracking device.\(^{150}\)

The maximum penalty for each of the offences is five years imprisonment, the same as for the existing offence of contravening a control order. The Explanatory Memorandum states that this ‘is appropriate given that all of the offences are directed to similar sorts of wrongdoing that frustrate and undermine the efficacy of the control order regime’.\(^{151}\)

Issuing courts (Schedule 4)
Schedule 4 of the Bill will remove the Family Court from the list of courts authorised to make control orders. This will partially implement a recommendation of the COAG Review. Recommendation 28 was that both the Family Court and the Federal Circuit Court of Australia be removed, leaving the Federal Court as the only issuing court.\(^{152}\) Gilbert + Tobin supported the amendment, but argued the Government should adopt the COAG Recommendation in full.\(^{153}\) AGD stated that doing so ‘would limit the geographic locations for making applications and could delay consideration of a control order application, resulting in ongoing risk to the community’.\(^{154}\)

The INSLM suggested a compromise whereby COAG’s recommendation is implemented in full, but the Federal Court is given the power to remit an application for a control order to the Federal Circuit Court.\(^{155}\)

New types of orders to protect national security information in control order proceedings (Part 1 of Schedule 15)
Part 1 of Schedule 15 of the Bill will amend the NSI Act to introduce new provisions providing courts with the power to make three new types of orders in control order proceedings (under Division 104 of the Criminal Code), allowing the court to consider information that is not disclosed to the subject of the control order or their representative for national security reasons.

As outlined separately below, Part 2 of Schedule 15 will introduce a system of special advocates to represent the interests of a person who is the subject of a control order proceeding where that person and their legal representative have been excluded from seeing or hearing sensitive national security information.

The Explanatory Memorandum states:

> The objective of the NSI Act is to prevent the disclosure of information in federal criminal proceedings and civil proceedings where disclosure is likely to prejudice national security, except to the extent that preventing the disclosure would seriously interfere with the administration of justice. ‘National security’ means ‘Australia’s defence, security, international relations or law enforcement interests’ (section 8).\(^{156}\)

\(^{147}\) Proposed subsection 104.27A(1).

\(^{148}\) Criminal Code, Division 5 of Part 2.2, particularly section 5.6 (default fault element for a physical element consisting of conduct is intent; default fault element for a physical element consisting of a result is recklessness).

\(^{149}\) Criminal Code, section 4.1.

\(^{150}\) Proposed subsection 104.27A(2).


\(^{152}\) COAG, COAG Review, op. cit., p. 58.

\(^{153}\) Gilbert + Tobin, Submission to PJCIS, op. cit., pp. 6–7.

\(^{154}\) AGD, Supplementary submission to PJCIS, op. cit., p. 15.

\(^{155}\) Gyles, Control order safeguards part 2, op. cit., pp. 7–8.

\(^{156}\) Explanatory Memorandum, 2016 Bill, op. cit., p. 142.
The NSI Act already contains protections for sensitive information, such as the closed hearing requirements in existing section 38I, non-disclosure certificates under section 38F and witness exclusion certificates under section 38H. However, if a court determines to exclude information under the existing provisions, under section 38L, such information cannot be used as evidence in the substantive hearing.

The Explanatory Memorandum states that it may be necessary to present such sensitive material to a court in order for a control order to be obtained, that the existing protections may be inadequate in some circumstances and that these issues, combined with the speed of counter-terrorism investigations, necessitate the proposed changes:

In some circumstances, information will be so sensitive that existing protections under the NSI Act are insufficient. For example, critical information supporting a control order may reveal law enforcement or intelligence sources, technologies and methodologies associated with gathering and analysing information. The inadvertent or deliberate disclosure of such material may endanger the safety of individuals as well as the general public, or jeopardise sources and other intelligence methods. However, the inability to provide such information to a court may mean that a control order is unable to be obtained.

… in order for control orders to be effective, law enforcement need to be able to act quickly, and be able to present sensitive information (which is in the form of admissible evidence) to a court as part of a control order proceeding without risking the integrity, safety or security of the information or its source.

Amendments

Item 21 of Schedule 15 will repeal and replace section 38J of the NSI Act.

Proposed subsection 38J(1) will set out the circumstances in which one of the orders in proposed section 38J may be made. Specifically, the orders may be made when certain hearings have been held relating to a control order, the Attorney-General or his or her legal representative has requested such an order, and the court is satisfied that the person to whom the control order proceeding relates ‘has been given sufficient information about the allegations on which the control order request was based to enable effective instructions to be given in relation to those allegations’. This last aspect has been modified from the 2015 Bill in accordance with recommendation 4 of the PJCIS’s report on the 2015 Bill, which recommended a higher standard of disclosure.

Proposed subsection 38J(2) of the NSI Act will set out what the court may order to control information in documents in non-disclosure certificate hearings required by existing subsection 38G(1) (civil non-disclosure certificates). It provides courts with the power to order the non-disclosure of the information to anyone but the court and impose closed hearing requirements as set out in existing section 38I. This subsection will permit redacted versions of the documents to be disclosed if ordered. An addition in the 2016 Bill is that the court may order that the person to whom the control order proceeding relates and that person’s legal representative are not entitled to be present for any part of a hearing in the proceeding in which the information is disclosed to the court (proposed paragraph 38J(2)(e)). Where such an order is made, the court may appoint a special advocate under proposed section 38PA (see further the analysis of Part 2 of Schedule 15 below).

Proposed subsection 38J(3) will provide similar powers relating to information in any form, and so does not deal with redacting information from documents as provided in subsection 38J(2). The 2016 Bill includes an equivalent addition to that in proposed subsection 38J(2) and a special advocate may be appointed.

Proposed subsection 38J(4) will provide that where a hearing is required under subsection 38H(6) (regarding an Attorney-General’s civil witness exclusion certificate), the court has the ability to order that a witness not be called by a person or their representative, or that the closed hearing requirements in 38I must apply. The 2016 Bill includes an equivalent addition to that in proposed subsection 38J(2) and a special advocate may be appointed.

In making these decisions, proposed subsection 38J(5) will require the court to consider whether there would be a prejudice to national security if information was disclosed or a witness called, or if an order would have a

157. NSI Act.
158. Ibid.
159. PJCIS, Advisory report on the Counter-Terrorism Legislation Amendment Bill (No.1) 2015, op. cit., pp. 74–75.
substantial adverse effect on the substantive hearing. The court may also consider any other matter it considers relevant. The Explanatory Memorandum notes that there is no requirement in proposed section 38J for the court to give the greatest weight to the need to protect national security. \textsuperscript{160}

Noting that the object of the NSI Act is ‘to prevent the disclosure of information in federal criminal proceedings and civil proceedings where the disclosure is likely to prejudice national security, except to the extent that preventing the disclosure would seriously interfere with the administration of justice’, section 3 of the Act also provides that courts must have regard to this object when exercising powers or performing functions under the Act. \textsuperscript{161} This requirement would continue to operate in guiding the court’s exercise of its discretion under the proposed changes.

**Reporting**

Item 31 of Schedule 15 will amend section 47 of the NSI Act to require the Attorney-General to include, in annual reports on the NSI Act, how many orders were made under proposed section 38J and identify the types of proceedings to which they related. This will implement recommendation 6 of the PJCIS’s report on the 2015 Bill. \textsuperscript{162}

**Procedural fairness issues relating to new section 38J**

An article in *The Conversation* referred to proposed section 38J of the 2015 Bill as ‘the Bill’s most concerning aspect’. \textsuperscript{163} The article went on to point out the inherent threats to procedural fairness, claiming that allowing the court to consider evidence that is not provided to the defence and cannot be challenged is unfair and the Bill does not provide sufficient safeguards to ensure a fair hearing. As noted in the ‘Position of major interest groups’ section of this Digest, many stakeholders voiced similar concerns.

**COAG, INSLM and PJCIS view**

The COAG Review considered this situation, and recommended that special advocates should be provided to assist in cases where sensitive information must be withheld from the accused in control order hearings, and that as a minimum standard ‘the applicant must be given sufficient information about the allegations against him or her to enable effective instructions to be given in relation to those allegations.’ \textsuperscript{164}

The INSLM also supported that position, and recommended that proposed section 38J should not come into force until a system of special advocates had been established for the control order regime. The INSLM noted that this provision of the Bill, given its focus on withholding information from the accused, would have the most direct relation to the role of a special advocate. \textsuperscript{165}

The INSLM stated that a system of special advocates would be a reasonable means to address the information imbalance the proposed court orders would create, and the consequent threats to ‘the principles of open justice, a fair trial, a fair hearing and the equality of arms’. \textsuperscript{166}

The PJCIS recommended COAG’s recommendation on the minimum standard of disclosure be implemented (Recommendation 4, implemented in proposed subsection 38J(1)) and that a system of special advocates be introduced (Recommendation 5). \textsuperscript{167}

Unlike the INSLM, the PJCIS considered this measure ‘should proceed without delay’. \textsuperscript{168} In the 2016 Bill, the special advocates scheme in Part 2 of Schedule 15 could commence up to 12 months after the further

\textsuperscript{160} Explanatory Memorandum, 2016 Bill, op. cit., p. 146.

\textsuperscript{161} NSI Act, section 3.

\textsuperscript{162} PJCIS, Advisory report on the Counter-Terrorism Legislation Amendment Bill (No.1) 2015, op. cit., pp. 81-82.

\textsuperscript{163} T Tulich and J Blackburn, ‘National security bill opens the door to expanded control orders and secret evidence’, *The Conversation*, 13 November 2015.

\textsuperscript{164} COAG, COAG Review, op. cit., pp. 59-60 (Recommendations 30 and 31).

\textsuperscript{165} Gyles, Control order safeguards—special advocates and the Counter-Terrorism Legislation Amendment Bill (No. 1) 2015, op. cit., p. 10.

\textsuperscript{166} Ibid., pp. 3-5.

\textsuperscript{167} PJCIS, Advisory report on the Counter-Terrorism Legislation Amendment Bill (No.1) 2015, op. cit., pp. 74-81.

\textsuperscript{168} Ibid., p. 81.
restrictions on access to national security information in Part 1, and further details of the scheme may be set out in regulations.\(^\text{169}\)

**Special advocates (Part 2 of Schedule 15)**

Special advocates (Part 2 of Schedule 15) Part 2 of Schedule 15 establishes a scheme of special advocates, where an order is made or sought under proposed new section 38J of the *NSI Act*, with the result that a person who is subject to an application for a control order (‘the party’) and his or her legal representative has sensitive information withheld from them, and are excluded from parts of the hearing when the relevant information is considered by the court.

**Background to the proposed scheme**

In its report on the 2015 Bill, the PJCIS described the role of a ‘special advocate’ in the following terms:

> Special advocates are security cleared lawyers who represent individuals in proceedings where the individual and their legal representative have been excluded. In the context of the proposed amendments to the *NSI Act*, the special advocate would represent the subject of the control order application in closed proceedings where both the subject and their legal representative have been excluded.\(^\text{170}\)

The PJCIS endorsed a recommendation of the INSLM that such a scheme should be established, although deviated from the INSLM’s view that the proposed amendments to the *NSI Act* (now in Part 1 of Schedule 15 to the 2016 Bill) should not come into force until a special advocates regime was established.\(^\text{171}\)

The PJCIS stated that ‘special advocates provide a valuable, additional safeguard in the judicial process’\(^\text{172}\) and appeared to place weight on the following view and reasoning of the INSLM:

> My experience as defence counsel is that it is possible to play a useful role in testing the prosecution case where no positive defence can be put forward on behalf of an accused. My experience as counsel, Royal Commissioner and judge is that a contradictor plays a vital role in any decision making, particularly judicial or quasi-judicial decision making. A special advocate can make submissions, for example: as to the extent to which the information needs to be protected if at all; the most helpful way of redacting the information and providing summaries or particulars of it; and the admissibility of the information and the lack of, or limited, probative value the information might have to support the case for the orders. The special advocate will have access to all of the evidence and can put the withheld evidence into context ... The involvement of a special advocate in the *NSI Act* proceedings should not introduce any undue delay in control order proceedings as special advocates will only be involved in those cases where proposed s 38J of the *NSI Act* is invoked and should not require any additional steps to be taken.\(^\text{173}\)

**Overview of the proposed scheme**

The key provision in Part 2 of Schedule 15 is item 41 which establishes the regime by inserting a new Subdivision C in Division 3 of Part 3A of the *NSI Act*.

**Proposed Subdivision C** provides a broad framework under which the court may exercise its discretion to appoint special advocates. It also prescribes the functions of special advocates and the nature of their relationship with the party, as well as the circumstances and manner in which the special advocate, the party and the party’s lawyer may communicate (with criminal penalties for contravention). Proposed Subdivision C also confers an extremely broad regulation-making power to settle matters of detail, including the terms on which a person serves as a special advocate, in subordinate legislation. Some key aspects of the scheme are summarised below.\(^\text{174}\)

\(^{169}\) Clause 2 (commencement); proposed section 38PI, Part 2 of Schedule 15.

\(^{170}\) PJCIS, *Advisory report on the Counter Terrorism Legislation Amendment Bill (No. 1) 2015*, op cit., pp. 68. Readers are referred to the PJCIS report on the 2015 Bill for more detailed information about the proposal to establish the scheme (including summary information about comparable schemes in the United Kingdom and Canada and some stakeholders’ views about the respective advantages or disadvantages of such a scheme).

\(^{171}\) Ibid., pp. 78-81 and recommendation 5. See also, R Gyles, *Control order safeguards—[INSLM report] special advocates and the Counter-Terrorism Legislation Amendment Bill (No 1) 2015*, Independent National Security Legislation Monitor, Canberra, January 2016, p. 10 (recommendations 1 and 2).

\(^{172}\) PJCIS, *Advisory report on the Counter Terrorism Legislation Amendment Bill (No. 1) 2015*, op cit., p. 79.


\(^{174}\) Readers are also referred to the overview of the special advocates scheme at pp. 156–159 of the Explanatory Memorandum.
Delayed commencement

Section 2 of the 2016 Bill provides that the proposed scheme will commence on the earlier of a date to be fixed by Proclamation, or 12 months after Royal Assent. The Explanatory Memorandum states that this is necessary to operationalise the scheme, including appointing a pool of special advocates and making regulations. This means that the proposed arrangements in new section 38J (inserted by item 21 in Part 1 of Schedule 15) will be in force for up to 12 months without a statutory special advocates scheme in place.

The Explanatory Memorandum states, however, that a court could decide to exercise its inherent powers to appoint a special advocate in the interim. While technically accurate, the practical implications of this position should also be acknowledged. In particular, the court, in exercising inherent jurisdiction, may not have access to the same degree of administrative support and resourcing as may accompany a statutory scheme, which may be necessary for a special advocate to be appointed and perform his or her functions effectively.

This raises the question of whether the Government is supporting the courts to develop any interim arrangements that may need to be implemented until such time as a statutory special advocates regime is operational. (Such arrangements might need to include, for example, arranging for the security clearance of a pool of lawyers who are available to act as special advocates, if appointed under the court’s inherent jurisdiction.) Such administrative support may help ensure that the potential to appoint special advocates under inherent jurisdiction is a realistic option for courts considering control order applications in which section 38J (if enacted) is invoked.

An alternative is to revert to the approach recommended by the INSLM, to the effect that the commencement of proposed section 38J should be tied to the establishment of a special advocates scheme, and therefore deferred.

Appointment of a special advocate (proposed section 38PA)

Appointment of a special advocate is at the court’s discretion. The court must provide parties (and the Attorney-General and his or her legal representative) with an opportunity to make submissions about who to appoint. If the party or his or her lawyer nominates a person to be appointed as special advocate, the court must generally appoint that person, unless it is satisfied there would be some adverse consequence in the nature of unreasonable delay, conflict of interest, or a risk of inadvertent disclosure of sensitive information.

Potential concern—delegation of legislative power

One matter of potential concern is that regulations made under the proposed enactment may prescribe the requirements that a person must meet in order to be appointed as a special advocate. The effect of proposed paragraph 38PA(2)(a) is that the court has no discretion to appoint a person who does not comply with whatever requirements the Executive may choose to set in the regulations at any given point in time. The regulation-making power is entirely open-ended, in that the provisions of proposed Subdivision C do not appear to impose any statutory limits on the types of eligibility requirements that may be prescribed by regulation.

Leaving the mandatory eligibility requirements for the appointment of special advocates entirely to subordinate legislation may be undesirable. For example, it could result in arbitrariness in the setting and amending of requirements. At least hypothetically, if the requirements set in the regulations are overly prescriptive, there may be no special advocates available—either at all, or in a particular geographical region—to represent the person’s interests. To better manage this risk, consideration could be given to fixing, in primary legislation, the basic qualifications a special advocate must hold, and conferring a more limited regulation-making power to prescribe supplementary, technical or more detailed eligibility requirements in subordinate legislation.

175. Explanatory Memorandum, 2016 Bill, p. 159.
176. Ibid.
177. Gyles, Control order safeguards, op. cit., p. 10 (recommendation 2).
178. Proposed subsection 38PA(1).
179. Proposed subsection 38PA(2).
180. Proposed subsection 38PA(3).
Functions of a special advocate (proposed section 38PB)

Proposed section 38PB provides that the function of the special advocate is to represent the interests of the party to a proceeding by:

- making submissions to the court at any part of a hearing in the proceeding where the party and his or her legal representative are not entitled to be present
- adducing evidence and cross-examining witnesses at such a part of a hearing in the proceeding, and
- making written submissions to the court.

Proposed section 38PB should also be read in conjunction with proposed subsection 38PC(3), which states that the special advocate is not a party to proceedings. Therefore, the special advocate cannot perform activities such as appealing procedural orders made as part of the proceedings such as orders under proposed section 38J (see item 21 in Part 1 of Schedule 15 to the 2016 Bill). It is open to question whether there is a sufficiently clear demarcation between a special advocate’s functions in proposed 38PB, and the activities that are peculiar to a party to the proceedings, and are therefore excluded by proposed subsection 38PC(3).

Relationship of special advocate and relevant person (proposed section 38PC)

Absence of lawyer-client relationship

Proposed subsection 38PC(1) makes clear that there is no lawyer-client relationship between the party and the special advocate. This appears to be consistent with the role and functions of special advocates as representative of the interests of the party in closed proceedings, not as the party’s lawyer.181

Legal professional privilege

Importantly, proposed subsection 38PC(2) provides that legal professional privilege applies to communications between the party (or his or her lawyer) and the special advocate.182 However, this privilege is not absolute, as a result of the communication arrangements prescribed by proposed section 38PF, under which the court—and in some instances the Attorney-General or his or her representatives—is privy to the communications from a special advocate to the party or legal representative. (This is discussed below).

Disclosure of information to special advocate by the Attorney-General (proposed section 38PE)

Proposed section 38PE provides a framework through which the Attorney-General must disclose the sensitive information to the special advocate. Proposed subsection 38PE(1) provides that, at the same time the court appoints a special advocate, it must also make an order fixing a date on which the Attorney-General must disclose the relevant information to the special advocate. Proposed subsection 38PE(2) provides that the Attorney-General must comply with the order. There are no provisions dealing with the consequences of non-compliance. Proposed subsection 38PE(3) places limitations on the circumstances in which the special advocate may disclose this information.183

Communication by special advocate and parties—conditions and restrictions (proposed sections 38PD, 38PF and 38PG)

Proposed sections 38PD, 38PF and 38PG prescribe the circumstances and manner in which the special advocate and parties may communicate. In broad terms, the special advocate will be able to communicate with the party

181. See also, Explanatory Memorandum, 2016 Bill, op. cit., pp. 157, 164.
182. By way of background explanation, legal professional privilege (sometimes referred to as client legal privilege) protects certain confidential communications between a lawyer and client from compulsory production in court or other proceedings. As the Australian Law Reform Commission (ALRC) has summarised, its rationale is to 'enhance the administration of justice and the proper conduct of litigation, by promoting free disclosure between clients and lawyers, to enable lawyers to give proper advice and representation to their clients'. The ALRC has noted that 'the privilege may also be considered a human right'. ALRC, Uniform Evidence Law, Report, 102, ALCR, Canberra, December 2005 at [14.44].
and his or her legal representative, without restriction, before receiving the sensitive information, unless the court makes an order restricting or prohibiting communication.\textsuperscript{184}

Once the special advocate has received the sensitive information, he or she will only be able to communicate with the party in writing \textit{and} with the approval of the court.\textsuperscript{185} The special advocate must not disclose the sensitive information he or she has received to the party or the party’s legal representative.\textsuperscript{186} Similarly, the party will only be able to communicate with the special advocate via the party’s legal representative, who must make such communications in writing only.\textsuperscript{187} The restrictions on communication continue to apply even if the control order proceeding has ended or the special advocate has ceased acting for the party.\textsuperscript{188} The Explanatory Memorandum states that these restrictions are considered necessary to protect national security information, including minimising the risk of inadvertent disclosure by the special advocate (via the court’s supervision of communications).\textsuperscript{189}

\textbf{Will the proposed communication arrangements be practicable?}

These restrictions, if adhered to, would seem to provide a reasonable safeguard against the possibility of inadvertent disclosure of sensitive information by the special advocate. However, it is not clear whether the proposed arrangements would also be workable, from a practical perspective, to enable the special advocate to obtain necessary information from a party in order to perform his or her role effectively and efficiently.

As discussed subsequently in this Bills Digest (see the "key issue" heading below) it is difficult to arrive at an informed conclusion on the practicality of the proposed arrangements without the benefit of consultation with the relevant issuing courts and members of the legal profession with experience in security related proceedings or analogous litigation. The extrinsic materials to the 2016 Bill do not provide information on what, if any, efforts have been made to consult with the legal profession or the courts on the proposed scheme (and whether these stakeholders are supportive of the proposed scheme).\textsuperscript{190} There does not appear to have been a public consultation process on the proposed scheme, in the nature of an exposure draft, prior to the introduction of the Bill.

\textbf{Abrogation of legal professional privilege}

\textbf{Proposed subsection 38PF(5)} may result in the abrogation of legal professional privilege in the communications between the special advocate and the party. This is because the court is responsible for on-forwarding communications from the special advocate to the party, in accordance with the requirements of \textbf{proposed subsection 38PF(4)}. If the court is satisfied that the communication is not likely to prejudice national security (in the sense of not raising a real, rather than remote, possibility of causing such prejudice) it must forward the communication. It the court is not satisfied that the communication is not likely to prejudice national security, it must amend the communication to remove the concern, or must decline to forward the communication if it cannot be so amended.

\textbf{Proposed subsection 38PF(5)} provides that the court may, in making a decision under proposed subsection 38PF(4), consult with the Attorney-General or the Attorney-General’s legal representative or any other representative of the Attorney-General. The Explanatory Memorandum indicates that this “reflects the fact that the Attorney-General, and agencies under his or her portfolio, have intimate knowledge of national security considerations and could provide the court with guidance in relation to why a proposed communication is likely to prejudice national security (or not likely to prejudice national security).”\textsuperscript{191}

\textsuperscript{184} Proposed section 38PD.

\textsuperscript{185} Proposed subsections 38PF(2)-(7).

\textsuperscript{186} Proposed subsection 38PF(2). See also \textit{proposed subsection 46H(3)} which creates an offence for contravening this prohibition, punishable by a maximum penalty of two years’ imprisonment (item 42 refers).

\textsuperscript{187} Proposed subsections 38PF(8)-(10). See also \textit{proposed subsections 46H(4) and 5} which create offences for contravening these prohibitions, punishable by a maximum penalty of two years’ imprisonment (item 42 refers).

\textsuperscript{188} Proposed section 38PG.

\textsuperscript{189} Explanatory Memorandum, 2016 Bill, op. cit., p. 168.

\textsuperscript{190} As discussed below, some stakeholders have called for further review of the proposed scheme before it is enacted to enable stakeholder consultation. See, for example: LCA, \textit{Special advocate regime a vital inclusion in new counter-terrorism bill, but further parliamentary scrutiny necessary}, op. cit. See also: AHRC, \textit{Supplementary submission} to the PJCIS, \textit{Inquiry into the Counter-Terrorism Legislation Amendment Bill (No. 1) 2015}, December 2015, p. 5.

\textsuperscript{191} Ibid., p. 169.
However, this consultation may operate to abrogate legal professional privilege in the communication. The Explanatory Memorandum acknowledges this possibility and states that this is expected to occur only in ‘rare circumstances’ and in any event only ‘following a careful balancing of the competing interests by the court’. While the second part of that statement is evidently correct, there does not appear to be any rational basis upon which to predict the frequency with which a court may consider it necessary to consult with the Attorney-General about the potential impact on national security that a particular proposed communication may have.

Further, the abrogation of legal professional privilege over the relevant information may have broader, detrimental consequences for the party’s interests, since the Bill does not contain any explicit prohibitions on the secondary use of any information that is provided to the Attorney-General or his or her representatives. Such information may be prejudicial to a party’s interests (either in the extant control order proceedings or more broadly). To better balance the party’s interests in being able to have ‘frank and honest communication’ with the special advocate, consideration might be given to enacting a further provision to place an express prohibition on the Attorney-General and his or her legal representatives making subsequent use of that information, and a requirement that the document is returned to the court after inspection (or deleted or destroyed securely).

**Regulation-making power (proposed section 38PI)**

**Proposed 38PI** confers a broad regulation-making power, stating that the regulations ‘may determine matters relating to special advocates’. It states that such matters may include, but are not limited to, remuneration, conflicts of interest and immunity. The Explanatory Memorandum acknowledges the significant breadth of the proposed regulation-making power, but states that it is considered necessary to ensure that ‘Parliament has the requisite authority to make such regulations as necessary to ensure the effective operation of the special advocates role’ and that regulations would be ‘established as soon as practicable in order to operationalise the special advocates role swiftly’.

It is unclear from this limited explanation why a regulation-making power needs to be entirely open-ended, presumably covering any matter relating to the operation of the proposed scheme. In particular, it is unclear why it is necessary or appropriate for matters of special advocates’ immunity to be dealt with via regulation, rather than fixed in primary legislation. (In addition to promoting transparency and certainty, the use of primary legislation to set the scope and limits of a person’s legal liability or immunity would ensure that these matters are not made unduly dependent upon administrative discretion.)

**Offences relating to unauthorised disclosures and communications (item 42, proposed section 46H)**

**Proposed section 46H** contains four offences, which variously apply to unauthorised disclosures of information by special advocates; and unauthorised communications by the party or his or her lawyer after the Attorney-General discloses the sensitive information to the special advocate. All of the offences are punishable by a maximum penalty of two years’ imprisonment. In all of the offences, the person making the disclosure or communication must be reckless as to whether the Attorney-General has disclosed the information to the special advocate. This means that the person must be aware of a substantial risk that the Attorney-General had made the communication, and acted unreasonably in the circumstances by taking that risk and making the communication or disclosure.

It may be questioned whether it is necessary or appropriate for the special advocates regime to incorporate a punitive dimension at all and, if so, whether a harm element should be included in the offences; or whether the

---

192. Ibid., pp. 164–165. See also p. 169 (‘the court would likely try to ensure that legal professional privilege is protected to the greatest extent possible when consulting with the Attorney-General (or the Attorney-General’s legal representative or any other representative of the Attorney-General)’).
193. Ibid., p. 164.
194. Ibid., p. 172. (The reference to ‘Parliament’ is presumably a typographical error, since the regulations made under section 49 of the NSI Act are made by the Governor-General, consistent with the delegated nature of legislative power, and are subject to Parliamentary disallowance,)
195. Proposed subsections 46H(1) and (3).
196. Proposed subsections 46H(4) and (5).
197. A detailed overview is provided at pp. 172–176 of the Explanatory Memorandum to the 2016 Bill.
defendant should be required to know that the Attorney-General has disclosed the relevant information. The prospect of exposure to legal liability for an inadvertent or technical contravention of these provisions may create a disincentive for legal practitioners to serve as special advocates, or to provide legal representation of controlees; and may have a harsh or oppressive impact on a controlee who may not fully understand his or her obligations.

Reporting requirement (item 43, proposed paragraphs 47(e)-(f))

Item 43 amends the annual reporting requirement in section 47 of the NSI Act to require the annual reports on the operation of the Act to include details of the use of the special advocates scheme. In particular, the reports must provide the number of special advocates appointed in the reporting period, and the proceedings in relation to which they were appointed. This will help to provide transparency about the use of the scheme.

Possible explicit oversight function for the PJCIS in relation to the special advocates scheme

In addition to the proposed annual reporting of unclassified information about the special advocates scheme, Parliamentary oversight could be enhanced further by amending section 29 of the Intelligence Services Act 2001 (IS Act) to make explicit that the statutory oversight functions of the PJCIS include the special advocates scheme.199

The PJCIS has oversight functions under paragraphs 29(1)(baa)-(bac) and subparagraph 29(1)(bb)(iii) of the IS Act in relation to the performance by the AFP of its functions under Part 5.3 of the Criminal Code (which includes the control order regime in Division 104). The PJCIS’s functions in relation to Part 5.3 might be argued to encompass the operation of the proposed special advocates scheme, given that it is specific to control order proceedings. Nonetheless, making this explicit in the IS Act would ensure that there is a clear and enduring mandate for the PJCIS to perform oversight in relation to the scheme, which is not open to contrary interpretation.

For completeness, it is worth noting that the NSI Act is within the statutory oversight remit of the INSLM, with the result that the proposed scheme would, if enacted, be subject to ongoing review by the INSLM.200

Issue: need for further scrutiny of, and consultation on, the details of the scheme

Shortly after the introduction of the Bill on 15 September 2016, the President of the Law Council of Australia, Stuart Clark, stated:

A special advocate regime provides a significant safeguard. The special advocate will be able to see the sensitive information that has been withheld from the subject of a control order and make representations on behalf of that person. This is essential, given that a person’s legal representative will also be excluded from accessing certain information.

For full accountability, however, the scheme must be immediately reviewed by the PJCIS. The exact relationship and level of interaction between the special advocate and the subject of the control order, and their legal representatives requires careful consideration.201

The Australian Human Rights Commission, in its submission to the PJCIS inquiry into the 2015 Bill also urged the consultative development and careful pre-legislative scrutiny of any proposed scheme, stating that:

In the Commission’s view, the precise form of a Special Advocate regime should be the result of careful consideration, following consultation with appropriately qualified experts, including legal practitioners with experience in criminal and control order proceedings where national security information has been put before the court.202

200. Independent National Security Legislation Monitor Act 2010 (INSLM Act), subparagraph 6(1)(a)(i) and section 4 (per paragraph (f) of the definition of ‘counter-terrorism and national security legislation’).
201. LCA, Special advocate regime a vital inclusion in new counter-terrorism bill, but further parliamentary scrutiny necessary, op. cit.
Indeed, it is difficult to comment meaningfully on the appropriateness or practicality of the provisions of Part 2 of Schedule 15 in the abstract, without knowing the perspectives of members of the legal profession who would be required to operate under the scheme, or the views of the courts upon which jurisdiction would be conferred. This is particularly evident in relation to the regulation of communication between the special advocate and parties (proposed sections 38PD, 38PF, 38PG and 38PH) and the provisions governing the disclosure by the Attorney-General of the relevant information to the special advocate (proposed section 38PE).

The Explanatory Memorandum does not provide an indication of what, if any, consultation the Government has undertaken in developing the proposed scheme; or whether the procedural and technical details of the proposed scheme have the support of the courts or legal profession (or other stakeholders).

The proposed scheme is complex and prescriptive. It operates in the context of an application for an order to place potentially significant restrictions on the liberty of a controlee. The scheme would expose controlees, their lawyers and special advocates to criminal liability in the event that its complex procedures for communications are not followed precisely. In this context, there is a risk that an absence of public consultation on the details of the proposed legislation may result in the enactment of measures that are practically unworkable. This may create a disincentive for legal practitioners to offer their services as special advocates or as the legal representatives of controlees. Such an outcome may, in turn, serve as a disincentive to the use of the special advocates scheme in individual cases, and may further place an unnecessary impost on the Parliament’s time to pass amending legislation correcting oversights that could have been identified in pre-legislative consultation.

The referral of Part 2 of Schedule 15 to a Parliamentary committee for inquiry and report to the Parliament, in advance of the Bill being debated, would therefore appear to be a sensible and prudent course of action to avoid unintended consequences, and support informed deliberations on the proposed scheme.

Possible trial arrangements and alignment with the sunsetting of the control order scheme

In its submission to the INSLM’s inquiry into control order safeguards in September 2015, the Law Council of Australia expressed its support for an incremental approach to the establishment of a special advocates scheme:

If a special advocates model is to be adopted, the Law Council considers that it should be trialed on a limited basis only, within narrow parameters (for example, in relation to a single area of the law such as the control order regime) and a finite timeframe. A comprehensive independent review should then take place before it is adopted on a permanent basis.  

The 2016 Bill proposes to enact the scheme in Part 2 of Schedule 15 on a permanent basis. In view of the discussion above, the merits of this approach are open to debate.

Monitoring, protective and preventative powers when a person is subject to a control order (Schedules 8, 9 and 10)

As noted above, the purpose of the control order regime is preventative. Obligations, prohibitions or restrictions are imposed so as to protect the public and mitigate the likelihood of a person engaging in terrorism-related activity. However, police do not currently have access to specific powers to monitor the compliance of someone subject to a control order with the obligations, prohibitions or restrictions it imposes.

Schedules 8, 9 and 10 will provide access to powers normally used to investigate offences—entry, search and seizure; telecommunications interception; and use of surveillance devices—for the purpose of determining whether the conditions of a control order have been, or are being, complied with. This will support enforcement of control orders, including through the existing offence of contravening a control order and the proposed offences in Schedule 3 of the Bill for interfering with a tracking device worn as a condition of a control order.

However, as outlined below, those Schedules will also provide for the use of those powers in relation to a person subject to a control order for broader protective and preventative purposes. Information and evidence derived from the use of those powers can also be used for a range of purposes beyond monitoring compliance with the control order and combating terrorism, even when a control order to which the relevant warrant is linked is later declared void.

---

203. LCA, ‘Adequacy of safeguards relating to the control order regime.’ Submission to the INSLM, 30 September 2015, p. 15.
Some issues common to all three Schedules are outlined first below, followed by further detail on each Schedule.

**Purposes for which powers would be available**

The justification for the introduction of the powers proposed in Schedules 8, 9 and 10 in the Explanatory Memorandum and AGD’s and the AFP’s submissions to the PJCIS inquiry into the 2015 Bill focuses largely (in the case of the AFP, solely) on the need to ensure police have adequate powers to properly monitor compliance with control orders. However, that justification concerns only one of four purposes for which the powers will be available.

The new powers proposed for the *Crimes Act, Telecommunications (Interception and Access) Act 1979* (*TIA Act*) and *Surveillance Devices Act 2004* (*SD Act*) will also be available in relation to a person subject to a control order for the purpose of:

- protecting the public from a terrorist act
- preventing the provision of support for, or the facilitation of, a terrorist act and/or
- preventing the provision of support for, or the facilitation of, the engagement in a hostile activity in a foreign country.

In a law enforcement context, entry, search and seizure powers are provided either in the context of determining compliance with legislative requirements (monitoring powers, generally granted to regulatory agencies) or investigating a criminal offence, and telecommunications interception and surveillance device powers only for the purposes of investigating criminal offences. The amendments proposed by the Bill will expand the purposes for which such powers may be used beyond investigations and compliance, to uses that are largely preventative in nature. Making those powers available to police to protect the public from, or prevent commission of, a terrorist act or offence, albeit in the limited context of persons subject to control orders, would be a new development. The appropriateness or otherwise of the proposed powers for the four purposes set out in the 2016 Bill cannot be properly assessed where the justification put forward addresses only one of those four purposes.

**Thresholds for warrants authorising powers**

A related but somewhat separate issue is the particular threshold that must be satisfied before the powers in Schedules 8, 9 and 10 may be used for one or more of the four purposes outlined in the preceding section of this Digest.

Under proposed sections 3ZZOA and 3ZZOB of the *Crimes Act* in Schedule 8, a monitoring warrant may be issued for one or more of the four purposes where the issuing officer is satisfied that a search is ‘reasonably necessary’ for one of those purposes. The provisions were modelled on the monitoring warrant provisions in the *Regulatory Powers (Standard Provisions) Act 2014*, which were developed for monitoring compliance with legislative requirements.

Under changes to the *TIA Act* and the *SD Act* in Schedules 9 and 10 respectively, a control order warrant may be issued where the relevant issuing authority is satisfied that information to be obtained under a warrant ‘would be likely to substantially assist’ in connection to one of those purposes.

---


205 The same purposes apply throughout many provisions of Schedules 8, 9 and 10. See for example proposed sections 3ZZKA, 3ZZLA, 3ZZOA and 3ZZOB of the *Crimes Act* (Schedule 8), items 21 and 24 of Schedule 9 (*TIA Act*) and items 1, 8, 11 and 13 of Schedule 10 (*SD Act*).

206 AGD, Guide to framing Commonwealth offences, infringements notices and enforcement powers, AGD, Canberra, September 2011, Chapters 7 and 10 and p. 87; *TIA Act*, Part 2-5, particularly Division 4; *SD Act*, Parts 2 and 4.

207 Search warrants, telecommunication interception and surveillance devices could all be sought in the context of an investigation for the preparatory offences in sections 101.4 (possessing things connected to terrorist acts), 101.5 (collecting or making documents likely to facilitate terrorist acts) and 101.6 (any act in preparation for, or planning, a terrorist act) of the *Criminal Code*, and the offence of breaching a control order in section 104.27 of the *Criminal Code*.


209 Items 21 and 24 of Schedule 9, amending sections 46 and 46A of the *TIA Act* respectively and item 11 of Schedule 10, amending subsection 16(1) of the *SD Act*.
Several stakeholders considered the proposed thresholds to be too low. The LCA suggested that before a warrant could be issued under Schedule 8, 9 or 10 in relation to a person subject to a control order, there should ‘as a minimum be a reasonable suspicion that the order is not being complied with or that the individual is engaged in terrorist related activity’.\(^{210}\) Gilbert + Tobin and the AHRC also suggested amendments to make the thresholds more stringent.\(^{211}\)

AGD responded to the LCA’s and Gilbert + Tobin’s suggestions, stating that requiring ‘reasonable suspicion’ would effectively bring the threshold into line with that required to access powers for the purpose of an investigation, meaning the provisions would no longer fill the gap they are being proposed to address.\(^{212}\) While that argument is appropriate to the context of availability of the powers to monitor compliance with a control order, it highlights the difficulties associated with extending the proposed scheme to other purposes. In particular, introducing powers to serve a purpose somewhere in between the two well established purposes of monitoring compliance with conditions and investigating a suspected offence makes it difficult to establish an appropriate threshold at which they should be available.

The PJCIS noted stakeholder concerns but did not recommend any changes to the thresholds in the 2015 Bill, which are replicated in the 2016 Bill.\(^ {213}\)

**Powers in relation to interim control orders and orders not yet in force**

The powers in Schedules 8, 9 and 10 will be available in relation to a person subject to an interim control order or a confirmed control order.\(^{214}\) An interim control order is made by a court in ex parte proceedings at which the person in relation to whom the order is proposed is not represented. Once an interim order is made, an AFP member must serve the order on the person and inform the person of various matters, including the person’s right to attend court for the court to decide whether to confirm, void or revoke the order.\(^ {215}\) The person and one or more of their representatives is entitled to adduce evidence and make submissions in relation to confirmation of the order at a hearing held to determine whether the order should be confirmed.\(^ {216}\)

Accordingly, allowing the powers outlined below to be exercised before a control order is confirmed means those powers may be exercised before the person subject to the order has a chance to contest it. Further, while an AFP member is required to serve the person with the interim control order ‘as soon as practicable’ the Bill would allow the proposed telecommunications interception and surveillance device powers to be exercised even before that occurs, so before the person is aware they are subject to an interim control order.\(^ {217}\)

The court making the interim order must specify a day on which the person may attend court for the court to decide whether to confirm, void or revoke the order. That day must be ‘as soon as practicable, but at least 72 hours, after the order is made’.\(^ {218}\) The interim control order imposed on Ahmad Naizmand on 5 March 2015 was not confirmed until 30 November 2015.\(^ {219}\) The interim control order imposed on Harun Causevic in September 2015 was not confirmed until July 2016.\(^ {220}\)

---

210. LCA, Submission to PJCIS, op. cit., p. 17.
212. AGD, Supplementary submission to PJCIS, op. cit., pp. 18–19.
214. Schedule 8, proposed section 3ZZJ(b) of the Crimes Act; Item 1 of Schedule 9, proposed amendments to subsection 5(1) of the TIA Act; Item 3 of Schedule 10, proposed amendments to subsection 6(1) of the SD Act.
215. Criminal Code, subsection 104.5(1) and section 104.12.
216. Ibid., subsection 104.14(1).
217. The monitoring powers in Schedule 8 are premised on the control order being in force (proposed subsections 3ZZOA(5) and 3ZZOB(5)). Under paragraph 104.5(1)(d) of the Criminal Code, a control order only enters into force once it is served on the person. Proposed sections 6T of the TIA Act (item 9 of Schedule 9) and proposed section 6C of the SD Act (item 7 of Schedule 10) displace that particular provision of the Criminal Code.
218. Criminal Code, subsections 104.5(1) and (1A).
**Use of things, information and documents obtained where control order is later declared void**

Schedules 8 (monitoring powers), 9 (telecommunications interception) and 10 (surveillance devices) each make provision for how things, information and documents obtained through the use of those powers may be dealt with if the relevant interim control order is declared void by a court. The Bill limits, but does not prevent, the use of those things, information and documents. Things, information and documents obtained under the powers in Schedule 8 may still be used or shared by a person if:

- the person reasonably believes that doing so is necessary to assist in preventing, or reducing the risk of the commission of a terrorist act, serious harm to a person or serious harm to property or
- the person does so for purposes connected with the performance of a function or duty, or exercise of a power, by a person, court, tribunal or other body under, or in relation to a matter arising under, specific legislation so far as it relates to a preventative detention order (under Commonwealth, state or territory law).\(^{221}\)

Similar provisions are set out in Schedules 9 and 10 with respect to information obtained under a telecommunications interception warrant and the use of a surveillance or tracking device in relation to an interim control order respectively.\(^{222}\)

These provisions have attracted some criticism, with the Muslim Legal Network (NSW) stating that allowing information and evidence to be used in the manner proposed is a ‘violation of the principle requiring that only legally obtained information may be used as evidence against an individual’.\(^{223}\)

These provisions also attracted the attention of the PJCHR and the Scrutiny of Bills Committee, both of which asked the Attorney-General for information outlining the rationale and providing further justification in light of the implications for peoples’ rights and liberties.\(^{224}\) On receipt of that information and following further consideration, the PJCHR assessed that the provisions are ‘likely to be compatible’ with the right to a fair trial, while the Scrutiny of Bills Committee declined to finalise its comments pending the Government’s response to the PJCIS’s recommendations on the monitoring powers. While the PJCIS recommended several amendments to Schedules 8, 9 and 10 (which are reflected in the 2016 Bill), none of them were specific to use of information where an order is later declared void.

**Entry, search, seizure and related powers (Schedule 8)**

This section of the Digest should be read in conjunction with those on issues common to Schedules 8, 9 and 10 above, which provide commentary on the purposes for which the powers below will be available, the threshold at which they will be available and other issues.

**Powers**

Schedule 8 will insert proposed Part IAAB into the Crimes Act to provide a scheme under which Commonwealth and state or territory police may exercise certain powers in relation to a person subject to a control order, or a premises to which the person has a ‘prescribed connection’ for the purpose of:

- 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 and/or
- determining whether the control order has been, or is being, complied with.\(^{225}\)

‘Prescribed connection’ with premises will be defined in proposed section 3ZZJC. It will include, for example, the person’s residence, (paid or voluntary) workplace, business or educational institution. The Explanatory

---

221. Proposed section 3ZZTC of the Crimes Act in Schedule 8.
222. Proposed section 299 of the TIA Act at item 58 of Schedule 9 and proposed section 65B of the SD Act at item 45 of Schedule 10.
223. Muslim Legal Network (NSW), Submission to PJCIS, op. cit., p. 30. See also pp. 26–27 and 34.
225. Proposed sections 3ZZJA, 3ZZKA, 3ZZLA, 3ZZOA and 3ZZOB of the Crimes Act.
Memorandum states that the definition is designed to capture even temporary connections between premises and a person subject to the control order ‘for example, where the person is merely staying with friends for a short period of time’.\(^{226}\) The definition would not generally capture other premises the person regularly visits, such as the homes of friends or family members or frequently visited public places. However, searches of premises and powers exercisable thereon, such as questioning people, potentially impact many third parties, including colleagues and fellow students and depending on the nature of the person’s employment (for example retail or hospitality), members of the public.

Broadly, the powers included under proposed Part IAAB are:

- entry to premises and exercise of ‘monitoring powers’, including a search, either by consent or under a monitoring warrant\(^{227}\)
- conducting an ordinary or frisk search of a person subject to a control order, either by consent or under a monitoring warrant\(^{228}\)
- searching any recently used conveyance and recording fingerprints, and taking samples, from things found in a search, without the need to obtain further consent or an additional warrant\(^{229}\)
- powers to ask questions and request or require documents following entry to premises\(^{230}\)
- powers to seize things believed to be evidential material, tainted property or seizable items following a search of a person or premises under a warrant\(^{231}\) and
- the ability to use and share things seized, documents produced and answers provided for certain purposes.\(^{232}\)

More extensive powers are available under a warrant than by consent. A monitoring warrant can only be issued by a magistrate, as is the case with a search warrant under Part IAA of the Crimes Act for offence-related search warrants.\(^{233}\) A magistrate must be satisfied that a warrant is reasonably necessary for one or more of the purposes outlined above.\(^{234}\)

**Safeguards**

The safeguards in the 2015 Bill have been supplemented in the 2016 Bill to address recommendations made by the PJCIS in its report on the 2015 Bill. Proposed safeguards include:

- explicit preservation of legal professional privilege and the privilege against self-incrimination\(^{235}\)
- a requirement for police to notify a person required to answer questions or produce documents of their rights to claim those privileges, implementing recommendation 10 of the PJCIS\(^{236}\)
- an obligation on issuing officers to consider whether allowing access to the powers available under a warrant would be ‘likely to have the least interference with any person’s liberty and privacy that is necessary in the circumstances’ (in response to recommendation 9 of the PJCIS)\(^{237}\)
- a prohibition on strip searches and searches of a person’s body cavities\(^{238}\)

\(^{226}\) Explanatory Memorandum, 2016 Bill, op. cit., p. 79.

\(^{227}\) Proposed sections 3ZZKA, 3ZZKB and 3ZZKC of the Crimes Act.

\(^{228}\) Proposed sections 3ZZLA and 3ZZLB of the Crimes Act.

\(^{229}\) Ibid.

\(^{230}\) Proposed section 3ZZKE of the Crimes Act.

\(^{231}\) Proposed sections 3ZZKF and 3ZZLC of the Crimes Act.

\(^{232}\) Proposed Division 8, Part IAAB of the Crimes Act.

\(^{233}\) Proposed section 3ZZJB and Division 5, Part IAAB of the Crimes Act.

\(^{234}\) Proposed sections 3ZZOA and 3ZZOB of the Crimes Act.

\(^{235}\) Proposed 3ZZJD of the Crimes Act. An exception is provided only in relation to information sought by the Ombudsman in the exercise of inspection powers.

\(^{236}\) Proposed subsections 3ZZKE(4) and (5) of the Crimes Act; PJCIS, Advisory report on the Counter-Terrorism Legislation Amendment Bill (No.1) 2015, op. cit., pp. 111–114.

\(^{237}\) Proposed paragraphs 3ZZOA(4)(g) and 3ZZOB(4)(g) of the Crimes Act; PJCIS, Advisory report on the Counter-Terrorism Legislation Amendment Bill (No.1) 2015, op. cit., pp. 111–113.

\(^{238}\) Proposed section 3ZZOC of the Crimes Act.
• a general prohibition on executing a monitoring warrant and exercising consequential powers if the control order is revoked, declared void or varied to remove one or more obligations, prohibitions or restrictions239
  – note: if a warrant is executed in breach of the prohibition, evidence, information and documents seized are not admissible in criminal proceedings (other than those concerning misconduct or corruption). However, the Bill does not provide such material is not admissible in civil proceedings.240

• procedural protections outlined in proposed Division 4, Part IAAB, including that consent must be informed and voluntary, and may be limited or withdrawn; compensation for damage to electronic equipment; and the occupier of premises and the person subject to the control order being entitled to be present and observe searches of premises241

• requirements for the AFP to keep certain documents connected to the issue of monitoring warrants, notify the Commonwealth Ombudsman within six months of a warrant issued in response to an AFP application, and notify the Ombudsman of any contraventions of proposed Part IAAB of the Crimes Act or of a monitoring warrant as soon as practicable (all implementing parts of recommendation 11 of the PJCIS)242

• powers for the Ombudsman to conduct inspections and report on the compliance of the AFP and AFP members and special members with the provisions of proposed Part IAAB of the Crimes Act and of a monitoring warrant (also implementing part of recommendation 11 of the PJCIS)243 and

• a requirement for the Attorney-General to include information on the number of monitoring warrants issued and executed, and the Ombudsman’s annual report on compliance, in annual reports to Parliament on control orders (partially implementing recommendation 12 of the PJCIS).244

There were two other pieces of information required by recommendation 12 of the PJCIS: complaints made or referred to the Ombudsman relating to the exercise of the monitoring powers, and certain information about AFP conduct and practice issues that related to the exercise of the monitoring powers. Annual reports on control orders must already include those types of information where it is ‘related to control orders’. It is unclear whether the exercise of monitoring powers would fall within those existing obligations or whether further amendments would be required to fully implement the recommendation.

Use, sharing and return of things, documents and information obtained

Proposed Division 8, Part IAAB makes different provision for the use, sharing and returning of things seized, documents obtained and answers to questions obtained under the Part. The Explanatory Memorandum does not explain why each is to be treated differently, or why the purposes for which it is proposed material may be used, shared and retained are appropriate.

Things seized

Things seized under proposed Part IAAB will be able to be used, shared and retained as if they had been seized under a search warrant issued for investigation of an offence (under Division 2 of Part IAA of the Crimes Act).245 This will mean things seized can be used or made available to constables, Commonwealth officers, state and territory police and anti-corruption agencies and foreign law enforcement, intelligence and security agencies for a broad range of purposes, including:

• preventing, investigating or prosecuting an offence under Commonwealth or state or territory law
• use in various types of proceedings (such as proceeds of crime and forfeiture proceedings) under Commonwealth or state or territory law or

239. Proposed section 3ZZOD of the Crimes Act.
240. Proposed subsections 3ZZOD(2), (3) and (4) of the Crimes Act.
244. Items 2 and 3 of Schedule 8, amending section 104.29 of the Criminal Code; Part IAAB of the Crimes Act; PJCIS, Advisory report on the Counter-Terrorism Legislation Amendment Bill (No.1) 2015, op. cit., pp. 111–115.
• when use or sharing of the things is required or authorised by a state or territory law.  

**Documents obtained**

Documents obtained under **proposed Part IAAB** will be able to be used, shared and retained as if they had been obtained under notice to produce provisions used for investigation of serious offences (under Division 4B of Part IAA of the **Crimes Act**). This will mean they can be used and shared with the same persons and agencies, and for the same purposes, as outlined above in relation to things seized.

In addition, documents may also be shared with constables, Commonwealth officers, state and territory police and anti-corruption agencies and foreign law enforcement, intelligence and security agencies for the purposes of:

• 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 and/or

• determining whether the control order has been, or is being, complied with.

These additional purposes considerably expand the circumstances in which a document may be shared. The existing preventative ground is specific to preventing a Commonwealth or state or territory offence. The proposed additional grounds are framed instead around the broader concepts of ‘terrorist act’ (for which the definition is independent of the offence of committing a terrorist act) and ‘engaging in a hostile activity’ (for which the definition is independent of the foreign incursions offences). Given documents may be shared with foreign law enforcement, intelligence and security agencies, the breadth of purposes for which documents may be shared, and lack of any requirement that the conduct to be prevented constitute an Australian offence, is significant.

**Answers given**

Answers given to questions asked under **proposed Part IAAB** will only be able to be used for the purposes of:

• 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

• determining whether the control order has been, or is being, complied with and/or

• preventing, investigating or prosecuting an offence.

As with the document use provisions, the first three purposes are not defined by reference to preventing conduct that would constitute an offence.

The scope of **proposed section 3ZZRD** is unclear in several other respects. It lists the purposes for which an answer may be used, but does not specify who may use them, whether they may be shared, and if so, with whom. Under **proposed section 3ZZKE**, questions may be asked by a constable who has entered premises by consent or under a warrant. However, given answers may be used in a prosecution for an offence, it appears there is some intention that answers be used by officers other than constables (and, accordingly, that they may be shared). It is also unclear how retention of information obtained from answers is governed.

---

246. **Crimes Act**, section 3ZQU.
247. **Proposed section 3ZZRC** of the **Crimes Act**.
248. **Crimes Act**, section 3ZQU.
249. **Proposed subsection 3ZZRC(2)** of the **Crimes Act**; **Crimes Act**, section 3ZQU.
250. **Crimes Act**, section 3C. The definition of offence for the purposes of Part IAA will apply because **proposed section 3ZZRC** will apply Division 4C of that Part to documents obtained under **proposed Part IAAB**.
251. **Crimes Act**, section 3; **Criminal Code**, subsection 100.1(1).
252. **Proposed section 3ZZLB** of the **Crimes Act**; **Criminal Code**, subsections 100.1(1) and 117.1(1).
253. **Proposed section 3ZZRD** of the **Crimes Act**.
Issue: breadth of use and sharing provisions, including with foreign agencies

As is clear from the descriptions above, things seized and information obtained under proposed Part IAAB, especially documents, may be used and shared for a broad range of purposes and with a broad range of domestic and foreign agencies, well beyond the purpose for which the monitoring powers are available. The Explanatory Memorandum contains no rationale for, or justification of, the breadth of the proposed provisions. Consideration could be given to whether the provisions should be framed more narrowly so as to better accord with the particular aims and purposes of the Bill. Amendments might, for example, limit use and sharing for protective or preventative purposes to circumstances where the conduct to be prevented would constitute an offence under Australian law, and clarify how answers given to questions may be used and shared.

Telecommunications interception warrants (Schedule 9)

This section of the Digest should be read in conjunction with those on issues common to Schedules 8, 9 and 10 above, which provide commentary on the purposes for which the powers below will be available, the threshold at which they will be available and other issues.

Powers

The amendments in Schedule 9 will allow ‘control order warrant agencies’ to obtain both B-party and Named person warrants to intercept and monitor the telecommunications of a person subject to a control order or a telecommunications service likely to be used by someone else to communicate with the subject of a control order for the purpose of:

- 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 and/or
- determining whether the control order has been, or is being, complied with (such as breaches of a prohibition on communicating with certain individuals).

‘Control order warrant agency’ will include the AFP, the Australian Commission for Law Enforcement Integrity (ACLEI) and the Australian Criminal Intelligence Commission (ACIC) and a state agency declared by the Minister under section 34 of the TIA Act. The types of state agencies the Minister may declare include police forces and crime and corruption commissions.

The amendments will also allow intercepted telecommunications information to be used in any proceedings associated with that control order and any proceedings related to serious offences (be they terrorism or non-terrorism related offences). The amendments will also introduce new ‘deferred reporting’ arrangements that will permit the chief officer of an agency to defer public reporting on the use of a warrant relating to a control order in certain circumstances. Finally, the amendments will also permit the use of intercepted telecommunications in connection with PDOs made under state and territory laws to support a nationally consistent prevention scheme.

---

254. The key items are items 21 and 24 of Schedule 9, amending sections 46 and 46A of the TIA Act respectively. B-party warrants allow the interception of a telecommunications service likely to be used by another person (a non-suspect) to communicate with a suspect. Named person warrants allow the interception of more than one telecommunications service used or likely to be used by the suspect: TIA Act, paragraphs 9(1)(a)(ia) and 46(1)(d)(ii), sections 9A and 46A. Law enforcement agencies may obtain a warrant by applying to an eligible judge or a nominated member of the Administrative Appeals Tribunal (AAT).

255. Proposed definition of ‘Control order warrant agency’ in item 1 of Schedule 9, in conjunction with existing definitions of ‘Commonwealth agency’ and ‘eligible authority’ in subsection 5(1) of the TIA Act.

256. Definition of ‘eligible authority’ in subsection 5(1) of the TIA Act.

257. Proposed subsection 139B(1) (which links to existing subsections 139(2), 139(4A) and 139A(2) of the TIA Act).

258. Proposed section 103B of the TIA Act.

259. Proposed section 139B and amendments to definitions of ‘permitted purpose’ and ‘preventative detention order’/‘preventative detention order law’ in subsection 5(1) of the TIA Act.
Privacy protections

The amendments propose a privacy-balancing test and other restrictions on the issuing of those warrants that reflect those currently in place under the TIA Act[^260^], with an additional factor included to implement recommendation 13 of the PJCIS’s report on the 2015 Bill (concerning whether interception represents the least interference with any person’s privacy, see further below).

The effectiveness of the privacy protections included in the 2015 Bill was questioned by several stakeholders, including the AHRC, LCA and councils for civil liberties[^261^]. The LCA noted that the amendments ‘would significantly broaden the circumstances in which innocent parties may be subjected to surveillance by reason of association’[^262^]. Of particular concern is the impact on the privacy of people other than those subject to control orders whose communications are intercepted under a B-party warrant, as outlined below.

The changes proposed to section 67 of the TIA Act by item 35 of Schedule 9 appear to provide that agencies can only use intercepted information obtained under a control order warrant for purposes relating to the control order regime (that is, broadly speaking, purposes related to preventing and protecting the public from terrorism) or a Commonwealth, state and territory law related to PDOs. However, proposed section 139B allows lawfully intercepted information to be used for a broader range of purposes.

**Proposed subsection 139B(1)** will allow an officer of the AFP or a state or territory police force to:

- communicate lawfully intercepted information to another person and
- make use of lawfully intercepted information.

For ‘one or more of the purposes referred to in subsection (2), and for no other purpose (other than a purpose referred to in subsection 139(2) or (4A) or 139A(2), if applicable’ (emphasis added).

Importantly, subsections 139(2), (3)[^263^], and (4A) and 139A(2) of the TIA Act encompass much broader purposes than those provided by section 67 (as proposed to be amended). Those purposes include:

- investigating a serious offence[^264^]
- investigating an offence punishable by imprisonment for a period, or a maximum period, of at least 12 months or a fine of at least 60 penalty units[^265^]
- prosecuting the offences referred to above[^266^]
- providing information to a foreign country in relation to a mutual assistance request[^267^] and
- undertaking certain integrity investigations and related proceedings[^268^].

Of particular note, **proposed section 139B** allows an officer or staff member of the AFP or a state or territory police force who intercepts the communications of a third party under a B-party warrant to use that information to investigate or prosecute that person (or others) for a range of criminal offences attracting a term of imprisonment greater than 12 months, despite that person not having been previously suspected of doing anything unlawful.

[^260^]: For B-party warrants, see proposed subsections 46(4)-(6) item 21 and in particular proposed paragraphs 46(4)(d)(ii), (5)(a), (c) and (6)(a).

[^261^]: These are based on existing paragraph 46(1)(d)(ii), 46(2)(a) and (c) and subsection 46(3) of the TIA Act. ‘The Judge or nominated AAT member must not issue a warrant in a case in which subparagraph (1)(d)(ii) applies unless he or she is satisfied that... (a) the agency has exhausted all other practicable methods of identifying the telecommunications services used, or likely to be used, by the person involved in the offence or offences referred to in paragraph (1)(d), or (b) interception of communications made to or from a telecommunications service used or likely to be used by that person would not otherwise be possible.’ (emphasis added). For named person warrants, items 22–25 will make equivalent amendments to section 46A of the TIA Act.

[^262^]: LCA, Submission to PJCIS, op. cit., p. 18.

[^263^]: TIA Act, paragraph 139(2)(b): ‘... the purposes are purposes connected with ... an investigation by the agency or by another criminal law-enforcement agency of a contravention to which subsection (3) applies ...’.

[^264^]: TIA Act, paragraph 139(3)(a).

[^265^]: TIA Act, paragraph 139(3)(b).

[^266^]: TIA Act, paragraph 139(2)(b) and (4).

[^267^]: TIA Act, subsection 139(4A).

[^268^]: TIA Act, subsection 139A(2).
Further, an amendment included in the Criminal Code Amendment (High Risk Terrorist Offenders) Bill 2016 would, if passed, amend proposed section 139B to also allow information obtained under a control order warrant to be used for the purposes of the proposed continued detention scheme. 269

As noted above, the 2016 Bill includes amendments to implement recommendation 13 of the PJCIS’s report on the 2015 Bill. The amendments will impose an obligation on eligible judges and AAT members to consider whether allowing interception under a control order warrant would be ‘the method that is likely to have the least interference with any person’s privacy’. 270 This will go some way towards addressing concerns about privacy implications.

**Proposed section 79AA of the TIA Act, at item 37 of Schedule 9, requires agencies to destroy information obtained under a control order warrant before the control order to which it relates came into force, if that warrant was issued for the purpose of, or for purposes that include, monitoring compliance with a control order. The amendments contain several exceptions to the obligation to destroy such information. Those exceptions will ensure that any information that could assist in preventing terrorism (broadly speaking) can be retained and used, thus reflecting the ‘preventative’ thrust of many of the amendments. Of note, this destruction obligation will not apply at all if a control order warrant was issued for purposes that did not include monitoring compliance with a control order (broadly speaking, preventing terrorism).**

**Record-keeping and oversight by the Ombudsman**

Part 2–7 of the TIA Act imposes requirements for records relating to applications for and issue of interception warrants to be kept by Commonwealth agencies (AFP, ACLEI and ACIC), and for the Commonwealth Ombudsman to inspect those records and report on agencies’ compliance.

The 2015 Bill included amendments to Part 2–7 to extend those existing requirements to capture records relating to control order warrants. In order to implement recommendation 11 of the PJCIS’s report into the 2015 Bill, the amendments to Part 2–7 in the 2016 Bill are more comprehensive. 271

Agencies will be required to keep records relating to applications for and issue of control order warrants. They will also need to keep records relating to decisions to defer the publication of information about control order warrants in annual public reports. The Ombudsman will have powers to conduct inspections to determine agencies’ compliance with record keeping and information destruction requirements (including proposed section 79AA) and the TIA Act more broadly, and report on its findings. 272

In addition, in accordance with recommendation 11 of the PJCIS’s report, proposed section 59B will require Commonwealth agencies to notify the Ombudsman of:

- each control order warrant issued in response to a Commonwealth agency application, within six months of issue and
- any contraventions by an officer of a Commonwealth agency of TIA Act provisions relating to control order warrants as soon as practicable.

The Ombudsman will also have the power to conduct inspections in response to notice of contraventions and to report on any breaches. 273

**Items 12 and 13** will amend section 35 and insert **proposed section 38A** respectively, so that the Minister may only declare a state agency to be a control order warrant agency if he or she is satisfied that the agency will be subject to record keeping obligations and oversight equivalent to that imposed on Commonwealth agencies. The Minister will also be able to revoke a declaration if satisfied that state requirements, or compliance with those requirements, is no longer satisfactory.

270. Proposed paragraphs 46(5)(f) and 46A(2B)(f) of the TIA Act (Items 21 and 24 of Schedule 9 to the Bill).
273. Items 45–47, amending sections 83–85 of the TIA Act and inserting proposed section 85A.
Reporting requirements

Part 2–8 of Chapter 2 of the TIA Act deals with the reporting of information related to interception warrants. As control order warrants will be a type of interception warrant, those provisions will automatically apply in relation to control order warrants.

Item 49 of Schedule 9 will insert proposed section 103B to require that the public reporting of control order warrants is deferred until a subsequent report if the chief officer of a control order warrant agency is satisfied that the information, if made public, could reasonably be expected to enable a reasonable person to conclude that:

• a control order warrant is likely to be, or is not likely to be, in force in relation to a telecommunications service used, or likely to be used, by a particular person or

• a control order warrant is likely to be, or is not likely to be, in force in relation to a particular person.

The Government argues that this is necessary because, due to the low number of control orders in existence at any time, public reporting during the period in which a control order warrant is in operation would undermine the purpose and effectiveness of such warrants (for example, by effectively revealing that a particular person who is subject to a control order is or is not also subject to covert surveillance).

Surveillance devices (Schedule 10)

This section of the Digest should be read in conjunction with those on issues common to Schedules 8, 9 and 10 above, which provide commentary on the purposes for which the powers below will be available, the threshold at which they will be available and other issues.

Currently the SD Act provides that surveillance device warrants are available where an eligible judge or nominated member of the AAT is satisfied that one or more ‘relevant offences’ (usually serious offences) have been, are being, are about to be, or are likely to be, committed. Use of tracking devices can also be authorised by certain senior officers of law enforcement agencies, and less intrusive types of surveillance devices may be used without special authorisation.

Powers

Schedule 10 will amend the SD Act to allow Commonwealth and state and territory law enforcement agencies to obtain a warrant to install and use a surveillance device in relation to a person who is subject to a control order for the purpose of:

• 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 and/or

• determining whether the control order has been, or is being, complied with (such as curfew requirements or visiting a prohibited place).

The amendments will also extend the circumstances in which law enforcement agencies may use less intrusive types of surveillance devices without a warrant to include the purposes noted above.

As with the amendments to the TIA Act, Schedule 10 will also introduce new ‘deferred reporting’ arrangements that will permit the chief officer of an agency to defer public reporting on the use of a surveillance device relating to a control order in certain circumstances.

275. SD Act, sections 11–14 and 16. Surveillance devices include data surveillance devices, listening devices, optical surveillance devices and tracking devices, as well as devices that combine any two or more of those functions: SD Act, subsection 6(1).
276. Ibid., sections 37 (optical surveillance devices), 38 (listening and recording devices) and 39 (tracking devices under authorisation).
277. Items 1 (amending section 3 of the TIA Act), 8–10 (amending section 14), 11–15 (amending section 16) and 16 (amending section 17).
278. Items 19 (amending section 17 of the TIA Act), 20 and 21 (amending section 38), 22–24 (amending section 39) and 25 (amending section 40).
279. Items 35 to 37 (amendment to section 50 and insertion of proposed section 50A of the SD Act).
Privacy protections

In relation to surveillance device warrants, the amendments propose a balancing test and other restrictions on the issuing of those warrants that reflect those currently in place under the SD Act, with an additional factor included to implement recommendation 14 of the PJCIS’s report on the 2015 Bill. Implementation of that recommendation will impose an obligation on eligible judges and nominated AAT members to consider whether allowing use of a surveillance device would be the means of obtaining information ‘that is likely to have the least interference with any person’s privacy’.

The 2016 Bill would not, however, impose an equivalent requirement on law enforcement officers to consider whether use of a surveillance device without a warrant would be likely to result in the least interference with any person’s privacy.

The existing offences related to the unlawful use, recording, communication or publication of ‘protected information’ will automatically include information obtained via control order surveillance warrants and tracking device authorisations in respect of a person subject to a control order. Item 29 will add to the exceptions to those offences so that information obtained under a surveillance device warrant or tracking device authorisation relating to a control order can be used for the purposes of determining whether the relevant control order has been, or is being, complied with. However, the application of existing exceptions to those offences will also mean that information obtained under a surveillance device warrant or tracking device authorisation relating to a control order can be used in a broad range of circumstances beyond investigating compliance with a control order, preventing terrorism or prosecuting breaches of control orders and terrorism offences. Those purposes include:

- investigating or prosecuting a ‘relevant offence’
- providing information to a foreign country in relation to a mutual assistance request
- undertaking certain integrity investigations and related proceedings

Proposed section 46A of the SD Act, at item 32 of Schedule 10, purports to ensure that agencies must destroy information obtained under a control order warrant or tracking device authorisation before the control order to which it relates came into force, if that warrant or authority was issued for the purpose of, or for purposes that include, monitoring compliance with a control order. The amendments contain several exceptions to the obligation to destroy such information. Those exceptions will ensure that any information that could assist in preventing terrorism (broadly speaking) can be retained and used, thus reflecting the ‘preventative’ thrust of many of the amendments. Of note, this destruction obligation will not apply at all if a control order warrant or tracking device authorisation was issued for purposes that did not include monitoring compliance with a control order (broadly speaking, preventing terrorism).

Further, as noted above in relation to issues common to Schedules 8, 9 and 10, proposed section 65B will allow information obtained through a surveillance device as permitted by the amendments in Schedule 10 to be used in certain circumstances even where the relevant control order is later declared void.

Record-keeping and oversight by the Ombudsman

Division 2 of Part 6 of the SD Act requires Commonwealth and state and territory law enforcement agencies to keep records relating to applications for and issue of surveillance device warrants and tracking device authorisations. Division 3 of Part 6 requires the Commonwealth Ombudsman to inspect those records and report on agencies’ compliance.

281. Proposed paragraph 16(2)(ec) of the SD Act at item 13 of Schedule 10.
282. SD Act, section 44 (meaning of ‘protected information’) and subsections 45(1) and (2) (offences).
283. Proposed paragraphs 45(5)(j) and (k).
284. SD Act, subsections 45(3)-(6). Paragraph 45(4)(b) allows protected information to be used, disclosed and published where a person ‘believes on reasonable grounds that the use or communication is necessary to help prevent or reduce the risk of serious violence to a person or substantial damage to property’. Likewise paragraphs 45(5)(a)-(c) allow protected information to be used, communicated and published ‘if it is necessary’ for the investigation or prosecution of a ‘relevant offence’ or for a ‘relevant proceeding’. As such, protected information can be used for a wider set of purposes than investigating or prosecuting terrorism related offences or breaches of control orders.
285. Ibid., paragraph 45(4)(f).
286. Ibid., paragraphs 45(5)(d), (e), (h) and (i). See also: section 45A.
The 2015 Bill included amendments to Divisions 2 and 3 of Part 6 to extend those existing requirements to capture records relating to warrants and authorisations related to control orders. In order to implement recommendation 11 of the PJCIS’s report into the 2015 Bill, the amendments to those Divisions in the 2016 Bill are more comprehensive.\(^\text{287}\)

Agencies will be required to keep records relating to applications for and issue of surveillance device warrants and tracking device authorisations. They will also need to keep records relating to decisions to defer the publication of related information in annual public reports. The Ombudsman will have powers to conduct inspections to determine agencies’ compliance with record keeping and information destruction requirements (including \textit{proposed section 46A}) and the \textit{SD Act} more broadly, and report on its findings.\(^\text{288}\)

In addition, in accordance with recommendation 11 of the PJCIS’s report, \textit{proposed section 49A} will require agencies to notify the Ombudsman of:

- each surveillance device warrant and tracking device authorisation related to a control order issued in response to an agency application, within six months of issue and
- any contraventions by an officer of an agency of \textit{SD Act} provisions about use of a surveillance device associated with a control order as soon as practicable.

The Ombudsman will also have the power to conduct inspections in response to notice of contraventions and to report on any breaches.\(^\text{289}\)

\textbf{Reporting requirements}

Division 2 of Part 6 of the \textit{SD Act} also deals with the reporting of information relating to surveillance device warrants and tracking device authorisations. Those provisions will automatically apply in relation to warrants and authorisations issued in relation to control orders. Among those provisions is section 49, which requires the chief officer of each law enforcement agency to provide certain details and documents to the Minister as soon as practicable after a warrant or authorisation ceases to be in force. \textit{Items 33 and 34 of Schedule 10} will amend section 49 to require specific details to be included in such reports if a warrant was issued in relation to a control order, specifically the benefit of the use of the device in determining compliance with the control order or preventing terrorism, and the general use to made of any information obtained. However, the amendments will not require those same details to be reported for tracking authorisations issued in relation to a control order.

\textit{Item 37} will insert \textit{proposed section 50A} to require that inclusion of information about surveillance devices in a public annual report is deferred until a subsequent report if the chief officer of a law enforcement agency is satisfied it is ‘control order information’. This will be information that, if made public, could reasonably be expected to enable a reasonable person to conclude that a control order warrant is likely to be, or is not likely to be, in force, authorising the use of a surveillance device:

- on particular premises
- in or on a particular object or class of object or
- in relation to the conversations, activities or location of a particular person.

Information that might reveal those same matters in relation to a tracking device authorisation does not fall within the definition of control order information, so reporting of it may not be deferred in the same way. This appears to be an oversight.

The Government has advanced essentially the same arguments for the need to defer reporting as made in relation to the interception warrants.\(^\text{290}\)

\textbf{Footnotes:}

\(^{287}\) PJCIS, \textit{Advisory report on the Counter-Terrorism Legislation Amendment Bill (No.1) 2015}, op. cit., p. 114.

\(^{288}\) \textit{Items 33, 34, and 38–41}, amending sections 49 and 51–53 of the \textit{SD Act}.

\(^{289}\) \textit{Items 42 and 44}, amending section 55 of the \textit{SD Act} and inserting \textit{proposed section 61A}.

\(^{290}\) \textit{Explanatory Memorandum, 2016 Bill, op. cit., p. 126.}
Preventative detention orders (Schedules 5 and 6)

There are currently two purposes for which preventative detention orders (PDOs) may be made if relevant thresholds are met: to prevent an imminent terrorist act, and to preserve evidence of or relating to a terrorist act that has already occurred.

Schedule 5 will replace the first of these (prevention of an imminent terrorist act). Instead of being able to be made to prevent a terrorist act that is imminent and expected to occur within the next 14 days, a PDO will be able to be made if a terrorist act is capable of being carried out, and could occur, within the next 14 days’ (emphasis added).

Before making a PDO, the issuing authority will still be required to be satisfied:

• making the order would substantially assist in preventing a terrorist act occurring and
• detaining the person for the proposed period is reasonably necessary for the purpose of preventing that terrorist act.

The Explanatory Memorandum states that law enforcement agencies may be aware of individuals with the capability and intent to carry out a terrorist act, but no clear timeframe in mind:

The terrorist act could potentially occur within hours, weeks or months. 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. In other circumstances, a person may become aware that they are the subject of law enforcement surveillance and accordingly change the timing of the planned attack to evade attention. In such instances, law enforcement agencies may not be able to obtain a PDO as the issuing authority may not be satisfied that there is an expectation the act will occur within precisely 14 days, despite the clear and ongoing threat posed by the individual.

The Explanatory Memorandum also characterises the change as a clarification that ‘still captures the essence of the original imminent test by having both a preparedness component and a temporal component’. However, as the Scrutiny of Bills Committee pointed out, the change in emphasis from an expectation that a terrorist attack will occur to a determination that it realistically could occur, represents a significant shift that would mean PDOs were available in a broader range of circumstances. The Scrutiny of Bills Committee and the PJCHR both sought additional explanation from the Attorney-General. Having received that, the Scrutiny of Bills Committee left the question of the amendment’s appropriateness to the Senate as a whole, while the PJCHR remained concerned and considered the amendment ‘may be incompatible with the right to liberty’.

While objecting to the PDO regime as a whole, Gilbert + Tobin did not oppose this amendment. However, the AHRC, LCA and councils for civil liberties considered the proposed new threshold to be too low.

The PJCIS considered the amendment in the 2015 Bill, which would have had the same effect as that in the 2016 Bill, but was differently worded. The PJCIS accepted the change to the threshold, but recommended the word ‘imminent’ not be used, as the revised threshold ‘stretches beyond the common understanding of the term “imminent”’ (recommendation 15). Schedule 5 has been amended in the 2016 Bill accordingly.

Schedule 6 will make a minor amendment so that neither a person’s past nor current service as a judge in the Family Court will make them eligible to be appointed as an issuing authority for continued preventative

291. Criminal Code, paragraphs 105.4(4)(c) and (d).
293. Ibid., pp. 71–72.
298. AHRC, Submission to PJCIS, op. cit., pp. 14–16; LCA, Submission to PJCIS, op. cit., pp. 15–16; Australian councils for civil liberties, Submission to PJCIS, op. cit., pp. 11–12.
detention orders. The same Schedule in the 2015 Bill would only have excluded past service. The 2016 Bill will implement recommendation 16 of the PJCIS’s report on the 2015 Bill by also excluding current service.\(^{300}\)

**Offence of advocating genocide (Schedule 11)**

Division 80 of the *Criminal Code* contains offences for treason and related conduct, urging violence and advocating terrorism. Schedule 11 will insert *proposed section 80.2D* to introduce a new offence of ‘advocating genocide’, with a maximum penalty of seven years imprisonment.

*Proposed subsection 80.2D(3)* contains definitions for the purposes of the proposed offence.

- ‘Advocate’ will mean ‘counsel, promote, encourage or urge’. This is consistent with the definition used in the offence of advocating terrorism.\(^ {301}\)
- ‘Genocide’ will mean the commission of an offence (other than an ancillary offence such as attempt or conspiracy) against Subdivision B of Division 268 of the *Criminal Code*, accordingly, genocide by: killing; causing serious bodily or mental harm; deliberately inflicting conditions of life calculated to bring about physical destruction; imposing measures intended to prevent births; or forcibly transferring children. These offences are essentially aligned with the definition provided in the 1948 *United Nations Convention on the Prevention and Punishment of the Crime of Genocide* (Article II).\(^ {302}\)

As noted in the ‘Position of major interest groups’ section of this Digest, some stakeholders were concerned that the proposed offence may infringe on free speech and could limit legitimate discussions of genocide related topics, and that the threshold required for proving the offence was inappropriately low. They also questioned the need for an additional offence, given the apparent overlap with existing offences (such as other offences in Division 80) and the availability of section 11.4 of the *Criminal Code*, which provides for an extension of criminal liability for incitement that could be applied to the existing genocide offences.

The PJCIS considered those issues and concerns raised about a lack of clarity around certain terms used in the offence in the 2015 Bill. It made two recommendations for amendments, both of which are reflected in the 2016 Bill.

The revised offence in *proposed subsection 80.2D(1)* will apply to someone if:

- the person (intentionally\(^ {303}\)) advocates genocide and
- the person does so reckless as to whether another person will engage in genocide.

The second part of the offence was added to implement recommendation 17 of the PJCIS’s report on the 2015 Bill, and should go some way to addressing concerns about the breadth of the offence.\(^ {304}\) The requirement in the 2015 Bill that the advocacy be engaged in ‘publicly’ has been removed in the 2016 Bill in accordance with recommendation 18 of the PJCIS’s report.\(^ {305}\) Implementation of these recommendations brings the way the offence is framed into closer alignment with the existing offence of advocating terrorism.\(^ {306}\)

The PJCIS noted the potential overlap of the proposed offence and existing offences, but was persuaded of its necessity:

> Some participants in the inquiry argued that such existing offences mean that the proposed ‘advocating genocide’ offence is unnecessary. However, the Committee recognises that the new offence is targeted at behaviour that does not meet the thresholds for prosecution under existing legislation. Evidence from the AFP was that such tools are needed to enable police to intervene earlier in the radicalisation process to prevent and disrupt further engagement in genocide offences.\(^ {307}\)

\(^{300}\) Ibid., p. 154.

\(^{301}\) *Criminal Code*, section 80.2C.

\(^{302}\) *Genocide Convention Act 1949*.

\(^{303}\) *Criminal Code*, subsection 5.6(1) (default fault element for a physical element consisting of conduct is intent).


\(^{305}\) Ibid.

\(^{306}\) *Criminal Code*, section 80.2C.

The proposed offence includes a note referring to the existing defence in section 80.3 for acts done in good faith. The Explanatory Memorandum claims that ‘(t)his defence protects the implied freedom of political communication.’\textsuperscript{308} This defence may be particularly necessary in the Australian domestic context in view of ongoing debates over current Indigenous policies, and the statements in the Bringing Them Home report and elsewhere asserting that Indigenous assimilation may be considered to fall within the definition of genocide.\textsuperscript{309}

The proposed offence also includes a double jeopardy safeguard in proposed subsection 80.2D(2) to prevent trial for such an offence where the person has already been convicted or acquitted by the International Criminal Court for an offence based on the same conduct.

**Offences relating to special intelligence operations (Schedule 18)**

Schedule 18 contains proposed amendments to the secrecy offences in section 35P of the ASIO Act, which implement the Government’s response to recommendations of the INSLM made in October 2015.\textsuperscript{310}

Section 35P contains offences for the unauthorised disclosure of information relating to a particular type of covert intelligence operation, known as a Special Intelligence Operation (SIO).

The key amendments are in item 4 (new offences) and item 6 (an exception to new offences which apply to persons who are not involved in the conduct of an SIO, if the information disclosed was already published).

An understanding and analysis of the proposed amendments requires an appreciation of the SIO scheme, the existing offences, the administrative arrangements governing their enforcement, and the INSLM’s inquiry.

These matters are outlined below, followed by analysis of the provisions in Schedule 18.

**The special intelligence operations scheme**

The SIO scheme was enacted in October 2014, as part of the Government’s first tranche of amendments to national security legislation, which was introduced and enacted in the 44th Parliament.\textsuperscript{311}

In broad terms, the SIO scheme enables the Attorney-General to authorise ASIO to conduct certain covert intelligence collection operations.\textsuperscript{312} The effect of authorisation is to confer upon authorised participants a limited immunity from civil and criminal liability in relation to authorised conduct carried out as part of the SIO.\textsuperscript{313}

The Inspector-General of Intelligence and Security (IGIS) has oversight of ASIO’s activities in relation to SIOs, including applications for authorisation and the conduct of operations, under the Inspector-General of Intelligence and Security Act 1986 (IGIS Act).\textsuperscript{314}

**Section 35P—unauthorised disclosure offence**

Section 35P, as currently in force, contains two offences—a ‘basic offence’ and an ‘aggravated offence’. These offences are capable of applying to all persons, including:

\textsuperscript{308} Explanatory Memorandum, 2016 Bill, op. cit., p. 131. The defence is available for all offence in Division 80.


\textsuperscript{310} Explanatory Memorandum, Counter-Terrorism Legislation Amendment Bill (No 1) 2016, p. 2; G Brandis, Second reading speech, Counter-Terrorism Legislation Amendment Bill (No 1) 2016, op. cit., p. 38; G Brandis (Attorney-General), Government response to INSLM report on the impact on journalists of section 35P of the ASIO Act 1979, media release, 2 February 2016.

\textsuperscript{311} National Security Legislation Amendment Act (No 1) 2014, Schedule 3 (which enacted a new Division 4 in Part III of the ASIO Act). The legislative history of the SIO scheme, including its policy objectives, is summarised in in R Gyles, Report on the impact on journalists of section 35P of the ASIO Act 1979, media release, 2 February 2016.

\textsuperscript{312} ASIO Act, section 35B (applications by ASIO for SIO authorities), section 35C (granting of SIO authorities by the Attorney-General), section 35D (contents of SIO authorities).

\textsuperscript{313} ASIO Act, section 35K.

\textsuperscript{314} Inspector-General of Intelligence and Security Act 1986 (IGIS Act). In addition to the functions and powers conferred under the IGIS Act (including the inspection of agencies’ records, the consideration of complaints and the commencement of inquiries) the ASIO Act requires ASIO to provide certain notifications and reports to the IGIS in relation to the commencement and conduct of SIOs: section 35PA and section 35Q. A summary of oversight arrangements is contained in Gyles, Report on the impact on journalists of section 35P of the ASIO Act, op cit., Appendix G, pp. 81–86.
• so-called ‘insiders’—persons who are in some way involved in an SIO (such as participants in an SIO, and ASIO personnel and others supporting the conduct of an SIO)

• so-called ‘outsiders’—persons who have no involvement in, or connection with, an SIO (such as journalists seeking to report on security operations, or community members who are aggrieved or adversely affected by activities carried out as part of an SIO).

The offences in section 35P are modelled on corresponding offences in Part 1AB of the Crimes Act, for unauthorised disclosures of information relating to controlled operations.315 (Controlled operations are covert law enforcement operations in which one or more persons are authorised to engage in otherwise unlawful conduct in order to obtain evidence of a serious criminal offence.)

The debate about section 35P, and the proposed amendments arising from the INSLM’s recommendations, turns heavily on an understanding and analysis of the technical elements of the offences. Awareness of these issues is, therefore, essential to an analysis of the proposed amendments. To this end, details of the existing offences and the application of general principles of criminal law in relation to the elements of offences are provided below.

The basic offence—subsection 35P(1)
The basic offence in subsection 35P(1) is punishable by a maximum penalty of five years’ imprisonment and applies to a person who:

• intentionally discloses information, and

• is reckless as to whether the information disclosed relates to an SIO.

The aggravated offence—subsection 35P(2)
The aggravated offence in subsection 35P(2) is punishable by a maximum penalty of 10 years’ imprisonment, and applies to a person who:

• intentionally discloses information

• is reckless as to whether the information disclosed relates to an SIO, and

– intends to endanger the health or safety of any person, or prejudice the effective conduct of an SIO, or

– is reckless as to whether the disclosure will cause the endangerment or prejudice mentioned above.

Exceptions to the offences—subsection 35P(3)
Subsection 35P(3) contains exceptions for persons who make disclosures in specified circumstances. These include disclosures for the purposes of legal proceedings arising out of or in relation to an SIO or any report of such proceedings,316 disclosures for the purpose of obtaining legal advice in relation to the SIO,317 and disclosures to the Inspector-General of Intelligence and Security (or staff).318

Explanation of fault elements applying to both offences
Chapter 2 of the Criminal Code Act 1995 (Criminal Code) provides that Commonwealth offences comprise two types of elements—physical elements and fault elements—both of which must be established beyond reasonable doubt in order for a person to be convicted.319

The physical elements of an offence are prescribed in each individual offence provision. The Criminal Code provides that there are three main types of physical elements, being: conduct, a circumstance in which conduct occurs, and the result of conduct.320

315. Crimes Act 1914, sections 15HK and 15HL. The controlled operations scheme, including the secrecy offences, is based on model national legislation. A summary is provided in Gyles, Report on the impact on journalists of section 35P of the ASIO Act, op cit., pp. 117–130, Appendix K).

316. ASIO Act, paragraph 35P(3)(b).

317. ASIO Act, paragraph 35P(3)(e).

318. ASIO Act, paragraph 35P(3)(f). See also paragraph 35P(3)(g) which authorises disclosures by IGIS officials to one another for the purpose of performing functions and exercising powers under the Inspector-General of Intelligence and Security Act 1986.


The *Criminal Code* also applies a **fault element** (or a ‘mental element’) to each physical element of an offence. The standard fault elements are intention, knowledge, recklessness and negligence.\(^{321}\) The *Criminal Code* prescribes general rules about the specific fault element that will apply to each type of physical element if the law creating the offence does not specify a fault element.\(^{322}\)

**Intentional disclosure of information**

As **subsections 35P(1) and 35P(2)** do not specify fault elements, the *Criminal Code* applies the fault element of **intention** to the physical element of disclosing information (being a form of conduct).\(^{323}\) A person has intention in relation to conduct if he or she means to engage in that conduct.\(^{324}\)

Other than in cases in which a person inadvertently discloses information (for example, if a document was released in an administrative error) the element of intention is unlikely to be in serious contention in alleged contraventions of section 35P. A media organisation that publishes a story, and an individual journalist who files a story for publication, would clearly mean to do so, and therefore engage in an intentional disclosure. A ‘whistleblower’ who provides comment, or hands documents, to a journalist would also clearly mean to do so.

**Recklessness that information relates to a special intelligence operation, or that disclosure will cause harm**

The *Criminal Code* applies the fault element of **recklessness** to the physical element in both offences that the information disclosed relates to an SIO (being a circumstance in which conduct, namely disclosure, occurs).\(^{325}\)

The *Criminal Code* also applies the fault element of recklessness to the physical element in the aggravated offence that the disclosure ‘will’ cause harm in the form of endangering health or safety, or prejudicing the effective conduct of an SIO (since this is also a circumstance in which conduct, namely disclosure, occurs).\(^{326}\)

The *Criminal Code* provides that a person will be reckless about a circumstance in which conduct occurs if, at the time of engaging in the relevant conduct, the person satisfies two requirements:

- **the person is aware of a substantial risk that the circumstance exists**—in this case:
  - in the basic offence—awareness of a substantial risk that the information relates to an SIO
  - in the aggravated offence—awareness of a substantial risk that the disclosure of the information would endanger health or safety, or prejudice the effective conduct of an SIO.

- **the person, unjustifiably in the circumstances known to him or her at the time, takes the risk by engaging in the relevant conduct**—in this case, engaging in the conduct that is the disclosure of the information (for example, publishing the story or filing it for publication, or making a comment to the media).\(^{327}\)

Proof that a person had actual knowledge of a circumstance will also satisfy the requirements of proof in relation to recklessness.\(^{328}\). (Given the covert nature of SIOs, however, it seems highly unlikely that persons who are not officially involved in these operations would have actual knowledge of them.)

**What amounts to a ‘substantial risk’ and acting ‘unjustifiably’ for the purpose of criminal recklessness?**

There are no statutory criteria for determining whether a risk is ‘substantial’ or whether the taking of a risk was ‘unjustifiable’ in the circumstances known to the person. These are questions of fact to be determined at trial. However, it is generally accepted that the task of proving that a person was aware of a substantial risk requires, in broad terms, proof that the person was consciously aware of a real and not remote possibility that the circumstance existed.\(^{329}\)

\(^{321}\) *Criminal Code*, section 5.1.

\(^{322}\) *Criminal Code*, section 5.6.

\(^{323}\) *Criminal Code*, subsection 5.6(1). (Note that the fault element of intention also applies to the physical element in subparagraph 35P(2)(c)(i) of the aggravated offence, that the person intended that the disclosure would endanger health or safety of any person, or prejudice the effective conduct of the SIO. This is because the fault element is prescribed expressly by the provision. The general rules about the application of fault elements under 5.6 of the *Criminal Code* can be displaced or overridden by specific offence provisions).

\(^{324}\) *Criminal Code*, subsection 5.2(1).

\(^{325}\) *Criminal Code*, subsection 5.6(2).

\(^{326}\) Ibid.

\(^{327}\) *Criminal Code*, subsection 5.4(1).

\(^{328}\) *Criminal Code*, subsection 5.4(4).
It is also generally accepted that proof that the taking of a risk was ‘unjustifiable’ requires a moral or value judgment based on the circumstances as the person believed them to be, and can involve the consideration of factors such as the degree of risk, the social utility of the person’s conduct and the social harm of the danger inherent in the risk, and the practicability of eliminating the risk.\(^{330}\)

**Government’s rationale for applying the fault element of recklessness, not knowledge**

The Government provided the following explanation of its rationale for selecting recklessness, rather than knowledge, as the applicable fault element to the circumstance that the information ‘relates to’ an SIO:

The policy justification for adopting recklessness, rather than knowledge, as the applicable fault element is ... that the wrongdoing targeted by ... s 35P is that the disclosure of information about an SIO will, by its very nature, create a significant risk to the integrity of that operation and the safety of its participants. The fault element of recklessness gives expression to the policy imperative to deter such conduct by clearly placing an onus on persons contemplating making a public disclosure of such information to consider whether or not their actions would be capable of justification to the criminal standard. In the event that there is doubt, and the proposed disclosure relates to suspected wrongdoing by ASIO, consideration should be given to making an appropriate internal disclosure, such as to the Inspector-General of Intelligence and Security, or to the Australian Federal Police if the commission of a criminal offence is suspected. \(^{331}\)

**How would the fault element of recklessness apply to journalists and others who report on operations?**

This question was the subject of significant Parliamentary and public debate on the NSLA Bill, and after its enactment, including in the INSLM’s inquiry in 2015.

In short, the Government also contended that the fault element of recklessness meant it was unlikely a journalist who adhered to ‘the usual practices of responsible journalism in the reporting of operational matters relating to national security’ (such as checking facts and consulting ASIO’s media liaison unit) would be exposed to prosecution. \(^{332}\) The basis for this position was that such actions would tend to suggest that a journalist and media organisation who proceeded to publish a story after making such inquiries (and presumably acting consistently with any information or advice received in response) had acted justifiably. In addition, it was said that a journalist who was entirely unaware of the possibility that the information might relate to an SIO would not be reckless, since he or she would not have adverted to a risk of any kind. \(^{333}\)

In contrast, media organisations and others argued that this did not provide adequate certainty about their potential exposure to legal liability in advance of publishing a story—including if ASIO declined to provide a substantive response to any attempts by the journalist to check facts (for example, by refusing to confirm or deny matters). The prospect of exposure to liability may therefore create a disincentive to publication. \(^{334}\)

**Administrative requirements for the commencement or continuation of prosecutions**

**Attorney-General’s direction to the Commonwealth Director of Public Prosecutions**

The Attorney-General issued a direction to the Commonwealth Director of Public Prosecutions (CDPP) on 30 October 2014 under section 8 of the *Director of Public Prosecutions Act 1983*.

---

329. See, for example, the commentary in S Odgers, *Principles of federal criminal law*, 3rd edn., Thomson Reuters, Pyrmont, 2015, pp. 69–71, paragraphs [5.4.120]–[5.4.150].

330. Ibid., p. 71, paragraphs [5.4.170]–[5.4.180].


332. A summary of the reasoning in support of this position is provided in R Gyles *Report on the impact of journalists of section 35P of the ASIO Act*, op cit., Appendix F, pp. 73-82 (the quoted phrase appears at p. 80).

333. Ibid., especially, pp. 79–80.

334. A summary of the reasoning in support of this position is provided in the INSLM report: Ibid., Appendix D, pp. 63–65.
This direction relevantly requires the CDPP to obtain the Attorney-General’s consent to proceed with a prosecution of a person for an alleged offence against section 35P 'where the person is a journalist and the facts constituting the alleged offence relate to the work of the person in a professional capacity as a journalist'.

**Commonwealth Director of Public Prosecutions National Legal Direction**

The CDPP has issued a National Legal Direction, which requires prosecutors to obtain the consent of the Director to any proposed prosecutions for offences against section 35P, in advance of seeking the Attorney-General’s consent to a prosecution of a person who is a journalist. The direction also provides guidance to prosecutors about the application of the public interest test in the *Prosecution Policy* of the Commonwealth in relation to potential prosecutions for offences against section 35P.\(^{336}\)

Some have criticised the adequacy of these mechanisms as safeguards against the prosecution of legitimate journalism or other disclosures in the public interest, because they involve the exercise of executive discretion rather than a legal immunity that would apply as of right.\(^{337}\) Others have advocated for the extension of the Attorney-General’s direction to persons other than journalists.\(^{338}\)

**Reviews of section 35P**

In conjunction with the appointment of Roger Gyles as Acting INSLM on 11 December 2014, the Prime Minister referred the matter of ‘the impact on journalists of section 35P of the *ASIO Act*’ to the (then) Acting INSLM for inquiry and report.\(^{339}\)

It is also worth noting that the Australian Law Reform Commission (ALRC) briefly considered section 35P in its inquiry into the encroachment by Commonwealth laws upon traditional rights and freedoms in 2014-15.\(^{340}\) The ALRC identified section 35P as a law that interferes with freedom of speech, and recommended that it was reviewed further to determine whether it imposed an unjustifiable limitation on the freedom. The ALRC noted that the provision was within the oversight remit of the INSLM and the PJCIS, and that the INSLM was undertaking such a review.\(^{341}\)

**INSLM findings and recommendations**

The INSLM provided his report to the Prime Minister on 1 October 2015, which was tabled on 2 February 2016.\(^{342}\) In broad terms, the INSLM recommended the retention of section 35P, subject to several amendments to modify the application of the offences to so-called ‘outsiders’ or third parties such as journalists who are not involved in, or connected with, the conduct of an SIO.\(^{343}\)

**Impact of section 35P on journalists**

The INSLM considered that section 35P had two main impacts on journalists, which are as follows:

---


336. CDPP, *Prosecuting offences for the unauthorised disclosure of information relating to controlled operations, special intelligence operations or delayed notification search warrants*, National Legal Direction, 1 December 2014, p. 4 (public interest test and consent of Attorney-General) and p. 5 (consent of Director).

337. For example, G Williams, ‘*Anti-terrorism laws threat to democracy*’, *The Sydney Morning Herald*, 3 November 2014, p. 16; S Breheny, ‘*George Brandis’s solution a cure worse than the disease*’, *The Australian*, (online edition), Institute of Public Affairs website, 7 November 2014, T Blackburn, ‘*Big flaws in security laws*’, *Courier-Mail*, 27 November 2014, p. 46.

338. JT Kwok (National Tertiary Education Union (NTEU)), ‘*Attorney-General to consider further protections for academics from s 35P*’, NTEU website, 30 March 2015.

339. T Abbott (Prime Minister), *Appointment of Independent National Security Legislation Monitor*, media release, 7 December 2014; Gyles, *Report on the impact of journalists of section 35P of the *ASIO Act*, op. cit., p. 5. (Note that this report also indicates Mr Gyles was appointed substantively as INSLM during the course of the inquiry on 20 August 2015 for a two-year term.)


341. Ibid., pp. 126–127 at paragraph [4.251].


A. It creates uncertainty as to what may be published about the activities of ASIO without fear of prosecution. The so-called chilling effect of that uncertainty is exacerbated because it also applies in relation to disclosures made to editors for the purpose of discussion before publication.

B. Journalists are prohibited from publishing anywhere at any time any information relating to an SIO, regardless of whether it has any, or any continuing, operational significance and even if it discloses reprehensible conduct by ASIO insiders.\textsuperscript{344}

Need for a secrecy offence applying to special intelligence operations

The INSLM stated that, in his view, an offence for the unauthorised disclosure of information relating to an SIO was ‘not inappropriate’.\textsuperscript{345} However, section 35P did not contain ‘adequate safeguards for protecting the rights of outsiders’ and was ‘not proportionate to the threat of terrorism or the threat to national security’.\textsuperscript{346}

Problems with section 35P

The INSLM identified ‘three basic flaws’\textsuperscript{347} in section 35P in support of this conclusion, which are as follows:

- the basic offence in subsection 35P(1)—the absence of a requirement in the basic offence in subsection 35P(1) to prove that a disclosure caused harm
- the aggravated offence in subsection 35P(2)—the application of the fault element of recklessness to the physical element that the disclosure will cause harm (in the form of endangering life or safety, or prejudicing the effective conduct of an SIO)
- both offences—the application of both offences to the disclosure of information already in the public domain.\textsuperscript{348}

The INSLM considered that these flaws meant that section 35P is ‘arguably invalid’ on the basis it infringes the implied freedom of political communication, and is arguably incompatible with Australia’s obligations under Article 19(2) of the \textit{International Covenant on Civil and Political Rights} with respect to freedom of expression.\textsuperscript{349}

Central to the INSLM’s conclusion was his rejection of the Government’s position that harm was implicit in the disclosure of any information relating to an SIO at any time. He opined this was ‘simply not sustainable’ as a rationale for exposing so-called ‘outsiders’ to criminal liability.\textsuperscript{350} He stated that ‘unless good cause is shown’ persons who do not have means of knowledge of the existence or nature of an SIO, or obligations of confidentiality, should not be exposed to prosecution.\textsuperscript{351}

The fundamental policy question is what—if anything—the Parliament should recognise, in legislation, as being a ‘good cause’ to justify the imposition of criminal sanctions upon so-called ‘outsiders’. The INSLM’s recommended amendments to enact discrete ‘outsider’ offences give expression to the INSLM’s opinion on this issue (discussed below).

Form of recommended amendments

To address the above issues, the INSLM recommended the enactment of two discrete categories of offences—one applying to unauthorised disclosures of information by ‘insiders’ who are involved in the conduct of an SIO, and the other applying to ‘outsiders’ who are not so involved.\textsuperscript{352}

New ‘outsider’ offences

The INSLM’s recommended amendments would attach a higher threshold of criminality to the offences applying to “outsiders”. In particular, these offences would require proof that:

\textsuperscript{344}. Ibid., p. 2 and pp. 12–13.
\textsuperscript{345}. Ibid., pp. 2 and 21.
\textsuperscript{346}. Ibid., pp. 2 and 23.
\textsuperscript{347}. Ibid., pp.3 and 23.
\textsuperscript{348}. Ibid.
\textsuperscript{349}. Ibid., p. 3. See also, Appendix J at pp. 102–116, which provides a brief analysis of constitutional and human rights issues.
\textsuperscript{350}. Ibid., p. 22.
\textsuperscript{351}. Ibid., p. 23.
\textsuperscript{352}. Ibid., pp. 3–4 and pp. 23–25.
• the ‘outsider’ disclosed information relating to an SIO (and was reckless as to that relationship), and
• the ‘outsider’ either:
  – was reckless that the disclosure would endanger the health or safety of any person, or would prejudice the effective conduct of an SIO, or
  – knew or intended that the disclosure would have the harmful effect described in the above point.\(^{353}\)

The INSLM recommended that a maximum penalty of five years’ imprisonment should apply to the offence for the disclosure of information, where the discloser is \textit{reckless} as to whether their disclosure would cause the harm described above.\(^{354}\)

He recommended that a maximum penalty of 10 years’ imprisonment should apply to the offence for the disclosure of information \textit{intending} to cause such harm, or \textit{knowing} that the disclosure would cause such harm.\(^{355}\)

\textbf{Exception to ‘outsider’ offences—prior publication}

The INSLM also recommended the enactment of an exception (an offence-specific defence) of “prior publication” which would apply only to the “outsider offences”.\(^{356}\)

He recommended that the exception apply to persons who disclose information relating to an SIO that has previously been published, subject to the following conditions:

\begin{itemize}
  \item having regard to the nature and extent of that prior publication and the place where it occurred, the defendant had reasonable grounds to believe that the second publication was not damaging, and
  \item the defendant was not in any way directly or indirectly involved in the prior publication.\(^{357}\)
\end{itemize}

\textbf{New ‘insider’ offences}

The INSLM recommended that offences applying only to ‘insiders’ should retain the general structure of, and maximum penalties applicable to, the offences as originally enacted.\(^{358}\) That is, they should require:

\begin{itemize}
  \item proof that a person disclosed information, reckless as to whether it related to an SIO (punishable by a maximum penalty of five years’ imprisonment) or
  \item proof of the above element, as well as proof that the person knew, or intended, that the disclosure would endanger the health or safety of any person, or prejudice the effective conduct of an SIO (punishable by a maximum penalty of 10 years’ imprisonment).\(^{359}\)
\end{itemize}

This was said to reflect that ‘insiders’ had specific obligations of confidentiality in relation to information obtained in the course of their duties, and that such persons have a greater knowledge or capacity to obtain knowledge of the risks of harm arising from unauthorised disclosures of information relating to SIOs.\(^{360}\)

The INSLM stated that he considered ‘insiders’ to include ‘ASIO employees, contractors and people who have entered into an agreement or arrangement with ASIO’.\(^{361}\)

\textbf{Measures not supported by the INSLM}

The INSLM considered briefly, but did not support, other potential amendments to section 35P suggested by inquiry participants.\(^{362}\) One such amendment was a ‘public interest defence’. The INSLM considered that the case for enacting a public interest defence ‘is not sufficient if section 35P is amended as recommended’.\(^{363}\)
In particular, the INSLM stated that ‘the judiciary should not lightly be involved in binding value judgments about issues of national security’. In the INSLM’s view, a preferable way of taking public interest considerations into account in the design and application of the offences in section 35P would be the combination of the harm element in the ‘basic outsiders offence’ together with the exercise of executive discretion in prosecutorial decision-making (including the Attorney-General’s consent to the prosecution of journalists, and the application by the CDPP of the public interest test under the Prosecution Policy of the Commonwealth.)

**Government response to the INSLM’s report**

The Attorney-General announced on 2 February 2016 that the Government supported all of the INSLM’s recommendations.

The Attorney-General also indicated that the Government intended to apply a modification to the recommended prior publication defence to the ‘outsiders offences’ by adding a further condition, namely:

The Government considers that prior to any secondary publication, an individual must take reasonable steps to ensure the proposed publication is not likely to cause harm. The Government will work with stakeholders to amend section 35P to include a defence of prior publication.

The extrinsic materials to the 2016 Bill do not appear to identify whether the Government consulted with stakeholders on the ‘prior publication defence’ prior to its introduction (and, if so, which stakeholders were consulted); or whether the Government intends to undertake consultations before the 2016 Bill is debated.

**Key amendments in Schedule 18**

The key proposed amendments are contained in item 4 (offences) and item 6 (prior publication defence).

Item 4 repeals the offences in subsections 35P(1) and 35P(2) and replaces them with the four new offences recommended by the INSLM, which are contained in new subsections 35P(1), (1B) (2) and (2A).

The headings to the offences apply two broad categorisations, which correspond to the INSLM’s labels of ‘insider’ and ‘outsider’ offences. These are:

- ‘Disclosures by entrusted persons’—covering the offences in proposed subsections 35P(1) and 35P(1B)
- ‘Other disclosures’—covering the offences in proposed subsections 35P(2) and 35P(2A).

Item 6 inserts the new prior publication defence, which applies to the ‘other disclosures’ offences.

Items 1-3, 5 and 7 are consequential to the key amendments in items 4 and 6.

**Disclosures by entrusted persons—proposed subsections 35P(1) and 35P(1B) (items 1-4)**

Item 4 inserts proposed subsections 35P(1) (basic offence) and 35P(1B) (aggravated offence), which correspond to the offences described by the INSLM as ‘insider offences’. These offences are stated to apply to a person who is, or who has been, an ‘entrusted person’.

This term is used instead of the INSLM’s label of ‘insider’.

Items 1-3 define the term ‘entrusted person’ and make other consequential amendments.

**Who are entrusted persons?**

Item 1 inserts a definition of the term ‘entrusted person’ in the general definitions in section 4 of the ASIO Act, and includes three classes of persons, by reference to the specific type of relationship they have with ASIO:

- an ‘ASIO employee’—defined in section 4 to mean a person who is employed under the two main machinery type provisions of the ASIO Act governing employment, namely section 84 (employment by the Director-General of Security) and section 90 (employment under regulations)

---

364. Ibid., p. 27.
365. Ibid.
367. Ibid.
368. Proposed paragraphs 35P(1)(a) and 35P(1B)(a).
• an ‘ASIO affiliate’—defined in section 4 to mean a person other than an ASIO employee who performs functions or services for ASIO in accordance with a contract, agreement or other arrangement. (It includes, for example, secondees, consultants, contractors and sources.)

• a person who has entered into a contract, agreement or arrangement with ASIO other than an ASIO affiliate—this covers people who do not fall within the definition of ‘ASIO affiliate’ because they are not performing functions or services for ASIO. (For example, this could conceivably cover staff members of other departments, agencies or entities with whom ASIO has shared information relating to an SIO—on conditions of confidentiality, and other limitations on use—for the purpose of the recipient performing functions or services for their agency, department or entity.)

The term ‘entrusted person’ is already used (and defined identically) in other offences in the ASIO Act, which apply to unauthorised dealings with intelligence-related information, and unauthorised recordings of such information. Accordingly, items 2 and 3 make consequential amendments to repeal the separate, identical definitions in these offence provisions, so that the definition in section 4 applies to them.

It is also worth noting that another offence in subsection 18(2) of the ASIO Act applies to the classes of persons covered by the definition of an ‘entrusted person’ although it does not use the defined term. This offence applies to persons who engage in an unauthorised disclosure of intelligence-related information. (The issue of its overlap with the proposed new offences is discussed in the “comments” section below.)

The ‘basic entrusted persons offence’—proposed subsection 35P(1) (item 4)

Proposed subsection 35P(1) creates the basic offence with respect to ‘entrusted persons’. Broadly, it applies to a disclosure of information relating to an SIO by a person who is, or who has been, an ‘entrusted person’ and who obtained that information in his or her capacity as an entrusted person. The offence is punishable by a maximum penalty of five years’ imprisonment, which is consistent with the ‘basic offence’ as currently in force.

The standard fault elements under the Criminal Code (discussed above) apply to all but one of these physical elements. (The exception is discussed separately below, in relation to strict liability elements.)

As with the ‘basic offence’ in current subsection 35P(1), the person must intend to engage in the conduct constituting the disclosure of information, and the person must be reckless that the information disclosed relates to an SIO. The person must also be reckless that the information came to his or her knowledge, or came into his or her possession, in the person’s capacity as an ‘entrusted person’.

The ‘aggravated entrusted persons offence’—proposed subsection 35P(1B) (item 4)

Proposed subsection 35P(1B) contains the ‘aggravated offence’ for unauthorised disclosures by ‘entrusted persons’. The elements of aggravation are set out in proposed paragraph 35P(1B)(e). The person must intend to endanger the health or safety of any person, or prejudice the effective conduct of an SIO; or he or she must be reckless that the disclosure will do so. The maximum penalty is 10 years’ imprisonment.

Strict liability elements in the ‘entrusted persons offences’—proposed subsections 35P(1A) and 35P(1C)

Proposed subsections 35P(1A) and 35P(1C) provide that strict liability applies to the physical elements in proposed paragraphs 35P(1)(a) (basic offence) and 35P(1B)(a) (aggravated offence). These physical elements are that the person is, or has been, an entrusted person.

The key legal effect of strict liability is that no fault element applies to these offences. Hence, the prosecution need only prove the relevant physical element. In this case, the physical element of a person’s status as an entrusted person might be satisfied by adducing documentary evidence such as the person’s contract of employment, or the contract or agreement the person has entered into with ASIO, or another document

369. Section 18A (unauthorised dealings with records, such as removal, retention and copying) and section 18B (unauthorised recording of information or matter). Note that ‘intelligence related information’ is a short-hand reference to the specific types of information (or records or other matter) covered by these offences, being information, matter or records of information (as applicable) that are acquired or prepared by ASIO in connection with its functions, or which relate to the performance by ASIO of its functions.

370. Criminal Code, subsection 6.1(2). A modified form of the defence of mistake of fact (in section 9.2) also applies to the elements of offences which are subject to strict liability.
recording an arrangement. If strict liability did not apply, the prosecution would be required to prove that the person was reckless as to his or her status as an ‘entrusted person’. 371

The Explanatory Memorandum states that proof of recklessness ‘would not be appropriate’ and that proof of the fact the person had entered into a contract, agreement or arrangement ‘should be sufficient’. 372 It does not point to any reasons in support of this opinion.

**Comments on the proposed offences for disclosures by entrusted persons**

Two questions arise in relation to the proposed “entrusted persons offences”:

- **First**, is it appropriate to apply strict liability to the physical element that the person is an entrusted person?
- **Secondly**, are these offences necessary or appropriate in light of the general unauthorised disclosure offence in subsection 18(2) of the ASIO Act? In particular, could the overlap create unintended consequences?

**Is strict liability appropriate in relation to a person’s status as an entrusted person?**

The INSLM did not make any comment about the application (or removal) of the fault element accompanying the physical element of a person’s status as an “insider”.

Other offences in the ASIO Act that apply to entrusted persons (or persons within the categories forming the definition of an ‘entrusted person’) do not apply strict liability to this element. 373

The absence of reasons in the Explanatory Memorandum makes it difficult to assess the appropriateness of proposed subsections 35P(1A) and 35P(1C). However, two relevant considerations are as follows.

**Potential policy grounds**

One possible ground for applying strict liability is a policy position that it is reasonable to hold an ‘entrusted person’ to a high standard of conduct, by presuming him or her to have read and understood, and be cognisant at all times, of his or her obligations and responsibilities under the relevant contract, agreement or arrangement with ASIO.

This position, on first blush, seems reasonable. However, it assumes that everyone who enters into a contract, agreement or arrangement with ASIO has the capacity to understand the obligations placed upon them, and are given an adequate opportunity to understand those obligations. While this may be a reasonable assumption to make on a wholesale basis for ASIO employees and certain ASIO affiliates who are in an employment-like relationship with ASIO, it may be questioned whether it is reasonable in relation to other categories of entrusted persons, who may only have a tangential relationship to ASIO.

The reasonableness of this assumption in relation to the latter category of entrusted persons depends on the existence of effective practical arrangements—both at the point of entry into a contract, agreement or arrangement, and throughout its administration—to ensure that entrusted persons are aware of, and understand, their status and consequent obligations. Two particularly important obligations are the limits on the person’s authority to disclose information, and any obligations placed upon the person that will continue after he or she ceases to be an entrusted person (for example, when the person’s contract ends). The Explanatory Memorandum does not contain any information about practical arrangements that could provide an assurance of this matter.

**Potential practical grounds**

Another possibility is that the proposed use of strict liability might help prevent the risk that prosecutions may not commence (or may not succeed) due to difficulties in proving that a person was reckless as to his or her status as an entrusted person.

---

371. As this physical element is a circumstance in which conduct occurs, subsection 5.6(2) of the Criminal Code would otherwise have applied.
373. See, for example, the following offences, which do not apply strict liability to this physical element: section 18A (offence of unauthorised dealing with records) and section 18B (offence of unauthorised recording of information or matter). See also subsection 18(2) (offence of unauthorised communication of intelligence-related information. The physical element in paragraph (b) provides that the person must be in one of the classes of persons which are incorporated in the definition of ‘entrusted person’ although it does not use this defined term).
For example, a defendant or prospective defendant might maintain that they were unaware of the risk they might have been an ‘entrusted person’. For example, there may be some suggestion that the person had not read or understood, or had forgotten about, the relevant contract, agreement or arrangement which established his or her status as an ‘entrusted person’. (As mentioned above, it is open to question whether this is likely to occur with people who are not ASIO employees or ASIO affiliates who are in an employment-like relationship with ASIO.) The prosecution would need to negate this possibility beyond reasonable doubt. Given that recklessness requires proof of a person’s subjective state of mind regarding his or her awareness of a substantial risk, it may be difficult to obtain admissible evidence that is sufficient to do so.

**Potential ineffectiveness of strict liability**

Even if it was accepted that the use of strict liability is appropriate as a matter of policy, it is questionable whether proposed subsections 35P(1A) and 35P(1C) will be effective in relieving the prosecution of a requirement to prove that a person was reckless as to his or her status as an entrusted person.

This is because the elements in proposed paragraphs 35P(1)(b) and 35P(1B)(b) do not apply strict liability. They require proof that the relevant information came into the person’s knowledge or possession in his or her capacity as an entrusted person, and that the person was reckless as to this circumstance.

Arguably, the task of proving that a person was aware of a substantial risk that information came into his or her knowledge or possession in a specific capacity or status (such as that of an ‘entrusted person’) will necessarily require some degree of proof that the person adverted to the possibility that he or she possessed that capacity or held that status. If this proposition is accepted, it would seem to neutralise any perceived policy or practical benefit sought to be gained from applying strict liability to paragraphs 35P(1)(a) and 35P(1B)(a).

**Are the proposed ‘entrusted persons’ offences necessary in light of subsection 18(2) of the ASIO Act?**

The conduct constituting the offences in proposed subsections 35P(1) and 35P(1B) appears to be covered by the existing offence for the unauthorised communication of intelligence-related information in subsection 18(2).

The Explanatory Memorandum states that the offence in subsection 18(2) is intended to be available ‘in addition to the offences in section 35P’. It does not indicate why it is considered appropriate to have two sets of offences that appear capable of applying to the same conduct, but adopt different maximum penalty structures and are inconsistent in their approaches to requiring proof of harm. In this regard, the internal offence and penalty structure within the ASIO Act is different to that applying to controlled operations under Part IAB of the Crimes Act. (For example, the general secrecy offence in section 60A of the Australian Federal Police Act 1979 is punishable by a maximum penalty of two years’ imprisonment. The general secrecy offences in Part VI and Part VII of the Crimes Act also apply lesser maximum penalties and take a different approach to harm elements.)

**Do proposed subsections 35P(1) and 35P(1B) duplicate the existing offence in subsection 18(2)?**

As mentioned above, subsection 18(2) is an offence for the unauthorised disclosure of intelligence-related information, and is subject to a maximum penalty of 10 years’ imprisonment.

Subsection 18(2) contains the following elements:

(a) the person makes a communication of any information or matter

(b) the information or matter has come into the person’s knowledge or possession by reason of the person being (or having been) an ASIO employee, ASIO affiliate, or having entered into a contract, agreement or arrangement with ASIO (otherwise than as an ASIO affiliate)

---

375. Australian Federal Police Act 1979, section 60A.
376. For example, section 70 of the Crimes Act (offence of disclosure of information by Commonwealth officers in contravention of a duty of non-disclosure) does not require proof of harm and is punishable by a maximum penalty of two years’ imprisonment. The general official secrets offence in subsection 79(3) (unauthorised communication of, or enabling of unauthorised access to, certain matter) is also punishable by a maximum penalty of two years’ imprisonment. An unauthorised communication offence with a higher maximum penalty in subsection 79(2) (seven years’ imprisonment) require proof of the person’s intention to cause a specific form of harm, namely intention to prejudice the security or defence of the Commonwealth (which may not be co-extensive with the specific forms of harm in the aggravated offence in section 15HL).
(c) the information or matter was acquired or prepared by or on behalf of ASIO in connection with its functions, or relates to the performance by ASIO of its functions

(d) the communication was not made to the Director-General, an ASIO employee, or an ASIO affiliate, by:
   – an ASIO employee, in the course of the person’s duties of employment, or
   – an ASIO affiliate, in accordance with the person’s obligations under the relevant contract, agreement or arrangement with ASIO
   – a person other than an ASIO affiliate, in accordance with the person’s obligations under the relevant contract, agreement or arrangement with ASIO.

(e) the communication was not made by a person acting within the limits of authority conferred by the Director-General

(f) the communication was not made with the approval of the Director-General (or another person authorised to provide approval).

Subsection 18(2A) contains an exception for information already in the public domain with the authority of the Commonwealth. Subsection 18(2B) contains an exception for communications to the IGIS (or the IGIS’s staff).

While there are differences in wording between the relevant provisions, it is not apparent that there are any elements of proposed subsection 18(2) that would make the task of prosecuting an unauthorised disclosure more difficult, in practical terms, than the task of prosecuting offences under proposed subsections 35P(1) and 35P(1B).

Accordingly, it seems likely that the value in the offences in proposed subsections 35P(1) and 35P(1B) may lie in their denunciatory effect rather than filling a substantive gap in the coverage of the criminal law. That is, they explicitly communicate the Parliament’s condemnation of the actions of entrusted persons who disclose information relating to an SIO in breach of the limits of their authority, and the trust reposed in them. However, this benefit is arguably outweighed by the risks of unintended consequences (discussed below).

**Risk of enacting offences which overlap significantly with subsection 18(2)**

**Inconsistent penalty structure**

The penalty structure between subsection 18(2) and proposed subsections 35P(1) and 35P(1B) is inconsistent. Subsection 18(2) and the aggravated offence in proposed subsection 35P(1B) have the same maximum penalty of 10 years’ imprisonment.

Unlike proposed subsection 35P(1B), subsection 18(2) does not require proof that the person intended to cause harm, or knew or was reckless that the disclosure would cause harm. This reflects a policy judgment that the harm is implicit in the combination of the person’s status as an authorised recipient of intelligence-related information, their breach of trust by acting in excess of their authority, and the nature of the information.

In contrast, the Explanatory Memorandum states that the maximum penalty applying to proposed subsection 35P(1B) ‘maintains parity’ with that applying to subsection 18(2). Yet it also states that the penalty applying to proposed subsection 35P(1B) is specifically intended to punish the wrongdoing arising from the aggravating elements of that offence, which relate to the harmful effects of disclosure.

This approach seems anomalous, particularly as subsection 18(2) applies to the unauthorised disclosure of a broader range of information than the offences in section 35P. Some information caught by subsection 18(2) might feasibly be less sensitive than information relating to an SIO, and potentially less harmful to security if disclosed without authorisation. Yet there is no requirement for the prosecution to prove harm.

**Risk of perverse incentives to prosecute offences under subsection 18(2)**

Subsection 18(2) covers conduct that could be prosecuted under the basic offence in proposed subsection 35P(1) but applies a maximum penalty double that of proposed subsection 35P(1). This could create a perverse incentive to rely upon subsection 18(2) in preference to proposed subsection 35P(1).

379. Ibid.
In addition, the parity of maximum penalties as between subsection 18(2) and proposed subsection 35P(1B) might create a perverse incentive to rely upon subsection 18(2) to avoid the potentially onerous task of proving the harm elements in proposed paragraph 35P(1B)(e).

**Potential application of the principle in The Queen v De Simoni in relation to sentencing**

The above risk may be mitigated, to an extent, by the possible application of the common law principle of sentencing recognised in *The Queen v De Simoni* (the ‘*De Simoni* principle’). This principle provides that a sentencing court cannot take into account, as an aggravating factor, a circumstance that would have warranted the person’s conviction for a more serious offence.

The potential application of the *De Simoni* principle to subsections 18(2) and proposed subsection 35P(1B) is not beyond argument. However, it might be argued that proposed subsection 35P(1B) amounts to a “more serious” offence than subsection 18(2) by reason of the harm element in proposed paragraph 35P(1B)(e) and its specific application to information relating to SIOs.

If this contention was accepted, then a person who is convicted of an offence against subsection 18(2) could not be sentenced on the basis of his or her advertence to the harmful impacts of disclosure, or intention to cause harm, to the extent that these factors are covered by proposed paragraph 35P(1B)(e).

The Government has not identified its policy position on the intended interaction of subsection 18(2) with proposed subsection and 35P(1B). On one hand, the potential application of the *De Simoni* principle may be viewed in a positive light, as a safeguard against the perverse incentives mentioned above. On the other hand, it might be inconsistent with the Government’s policy intention about the interaction of the respective offence provisions, and therefore could produce unintended consequences from a policy perspective.

**Confused or unintended signal to sentencing courts about the nature and gravity of wrongdoing**

Separately to the *De Simoni* principle, there is a risk that an internally inconsistent penalty structure within the *ASIO Act* may send a confused or an unintended signal to sentencing courts about the Parliament’s assessment of the nature and relative gravity of the wrongdoing involved in the various disclosure offences in the *ASIO Act*.

There is also a risk that this inconsistency could send a confused or an unintended message to the Parliament, and the wider community, about the policy underlying the relevant offences. This may complicate the task of developing and gaining support for any proposed amendments in future.

**Possible solution to the risks of overlap with subsection 18(2)**

One way of managing the risks of unintended legal and legal policy consequences arising from the overlap of proposed subsections 35P(1) and 35P(1B) with existing subsection 18(2) would be to omit subsections 35P(1) and 35P(1B) from the 2016 Bill. The result would be that subsection 18(2) alone would cover unauthorised disclosures of information relating to SIOs. This may require consequential amendments to some provisions of section 18.

An alternative solution may be to include new provisions in the 2016 Bill, giving express effect to the intended relationship between subsection 18(2) and proposed subsections 35P(1) and 35P(1B). (For example, new provisions could expressly exclude or apply the *De Simoni* principle, or otherwise provide guidance to sentencing courts.)

**Offences for other disclosures—proposed subsections 35P(2) and 35P(2A) (item 4)**

Proposed subsections 35P(2) and 35P(2A) correspond to the INSLM’s recommended category of outsider offences. With the exception of two matters (discussed below) they appear to implement faithfully the INSLM’s recommendations.

Proposed subsection 35P(2) contains the basic outsiders offence. It applies to a person who intentionally discloses information, reckless as to the circumstance that it relates to an SIO, and reckless as to the

---


381. It might be said that SIOs are more sensitive than other types of intelligence operations or activities of ASIO which generate information covered by subsection 18(2). This is supported by the onerous authorisation requirements applying to SIOs, and the unusual legal effects of authorisation in the form of immunity from civil and criminal liability (which departs from the fundamental principle that all people are subject to the law, which applies consistently to all persons).
circumstance that the disclosure will endanger the health or safety of any person, or will prejudice the effective conduct of an SIO. The maximum penalty is five years’ imprisonment.

Proposed subsection 35P(2A) contains the aggravated outsiders offence. It is punishable by a maximum penalty of 10 years’ imprisonment. The elements of aggravation are contained in proposed paragraph 35P(2A)(c), which requires proof of one, or both, of the following:

- **subparagraph 35P(2A)(c)(i)**—the person intends to endanger the health or safety of any person, or prejudice the effective conduct of an SIO
- **subparagraph 35P(2A)(c)(ii)**—the person knows that the disclosure will have either of the above harmful effects.

**Comments on the offences for ‘other disclosures’**

Two issues are apparent in relation to the offences in proposed subsections 35P(2) and 35P(2A). The first issue relates to unexplained differences to the INS LM’s recommendations.

The second issue relates to stakeholder concerns about the INS LM’s recommendation that the basic offence, now contained in proposed subsection 35P(2), should apply the fault element of recklessness to the circumstance that the information related to an SIO, and to the circumstance that the disclosure would cause harm.

**Application of proposed subsections 35P(2) and 35P(2A) to ‘entrusted persons’**

The INS LM’s recommendations appeared to support a complete separation between the two categories of so-called ‘insider’ and ‘outsider’ offences.

However, the proposed “outsider” offences in subsections 35P(2) and 35P(2A) do not expressly exclude ‘entrusted persons’. The Explanatory Memorandum states that this reflects a deliberate intention that these offences should not be ‘limited only to persons who are not and have never been an entrusted person’. 382

The Explanatory Memorandum suggests that ‘an entrusted person could still be subject to prosecution under subsection 35P(2) or (2A) if it was not demonstrated that they received the relevant information in their capacity as an entrusted person, although it is envisaged that this situation would be highly unusual’. 383

The Explanatory Memorandum does not address why it is considered necessary to prosecute an entrusted person under the so-called “outsider” offences, or provide details about the types of situations in which it is contemplated this course of action might be necessary. Presumably, the Government may be contemplating the scenario in which an entrusted person comes into contact with information relating to an SIO entirely outside his or her capacity as an entrusted person (for example, in a social setting). However, it is not clear whether the outsider offences are intended to apply to entrusted persons in a wider range of circumstances.

**Should proposed subsections 35P(2) and 35P(2A) be capable of applying to entrusted persons?**

It is possible that this approach may reflect an intention that proposed subsections 35P(2) and 35P(2A) should provide some kind of ‘safety net’ in the event that a prosecution of an offence against proposed subsection 35P(1) or 35P(1B) may fail, or a potential prosecution may not be open, for evidentiary reasons.

This risk might arise if, for example, there is insufficient admissible evidence to establish that:

- the person was an ‘entrusted person’ for the purpose of proposed paragraphs 35P(1)(a) and 35P(1B)(a). This could arise from lapses in record keeping, or in the event that the relevant contract, agreement or arrangement was not in writing, or if some irregularity is discovered in a written instrument
- the person was reckless as to whether the information came into his or her knowledge or possession in the person’s capacity as an entrusted person for the purpose of proposed paragraphs 35P(1)(b) and 35P(1B)(b).

The policy merits of allowing a prosecution to be brought under proposed subsections 35P(2) and 35P(2A) in these circumstances are debatable. However, the higher thresholds of criminality applied to these offences (particularly the harm elements) arguably provide a safeguard against the risk of abuse.

382. Ibid., p. 184.
383. Ibid.
The potential availability of a prosecution under proposed subsection 35P(2) or 35P(2A) may also help ensure that otherwise culpable conduct does not go unpunished as a result of an evidentiary limitation in establishing a potential defendant’s status as an ‘entrusted person’.

**Risk that the intended interpretation may not be supported by proposed subsections 35P(2) and 35P(2A)**

The proposed amendments do not include an express provision stating that an entrusted person may be prosecuted for an offence against proposed subsections 35P(2) and 35P(2A).

In the absence of such a provision, there may be some doubt that the proposed amendments are capable of supporting the Government’s desired interpretation.

It may be arguable that the word “person” as used in proposed subsections 35P(2) and 35P(2A) could be interpreted to mean “a person who is not an entrusted person”, having regard to the text and context of these provisions.

In particular, the existence of two separate categories of offences, and the use of the headings ‘disclosures by entrusted persons’ for the offences in proposed subsections 35P(1) and 35P(1B) and ‘other disclosures’ for the offences in proposed subsections 35P(2) and 35P(2A) (emphasis added) may tend against the interpretation suggested in the Explanatory Memorandum, despite its statement of subjective intention.

**Potential amendments to reduce the risk of an interpretation contrary to the intended meaning**

This Bills Digest does not advance a concluded view on the above question of statutory interpretation. The key issue is, arguably, managing the potential risk that ambiguity in the provisions could be exploited in a challenge to a prosecution of an entrusted person under proposed subsection 35P(2) or 35P(2A).

This risk could be removed through the enactment of a provision containing an express statement to the effect that nothing in proposed subsections 35P(1)-(1C) prevents a person who is an entrusted person from being prosecuted under proposed subsection 35P(2) or 35P(2A).

A further, complementary measure may be the inclusion of “alternative verdict provisions” as between subsections proposed 35P(1B) and proposed subsections 35P(2) and (2A).

**Stakeholder criticism of recklessness as the fault element in the “basic offence” in subsection 35P(2)**

The Media, Entertainment and Arts Alliance (MEAA) has stated that, while the INSLM’s recommendations are ‘welcome’, they have ‘not changed the fundamental intent of section 35P which is to intimidate whistleblowers and journalists’.

One of its concerns is the absence of a requirement that an “outsider” must have actual knowledge that the information he or she discloses ‘relates to’ an SIO. The MEAA argues that this means journalists will continue to face uncertainty in determining whether a potential publication may contravene section 35P. Supporters of this view may prefer that the fault element of recklessness in proposed paragraph 35P(2)(b) is replaced with that of knowledge.

A similar argument might also be made in relation to the requirement in proposed paragraph 35P(2)(c) that a person must be reckless as to whether the disclosure will cause harm. (That is, it might be said that this provision fails to provide clear guidance to a person about their potential exposure to criminal liability, in advance of making a disclosure.) If it is considered that “outsiders” should only be exposed to criminal liability if they know

---

384. That is, the use of the heading ‘disclosures by entrusted persons’ is used to denote two offences which apply exclusively to defined class of persons. This may lead to a necessary implication that a heading which denotes offences that apply to ‘other disclosures’ means disclosures by persons who are not in the class to which the first category of offences applies. (It is not certain that the statement at page 184 of the Explanatory Memorandum could be relied upon as an aid to interpretation under section 15AB of the Acts Interpretation Act 1901. Extrinsic materials cannot be used to displace the ordinary meaning of a provision that is unambiguous on its face, unless the ordinary meaning would lead to a manifest absurd result).

385. For an example of alternative verdict provisions in the ASIO Act, see subsections 18A(3)-(4) and 18B(3)-(4). The use of an alternative verdict provision would mean that, if an ‘entrusted person’ is prosecuted for an offence against subsection 35P(1B) and the trier of fact is not satisfied that the person is guilty of that offence—but the trier of fact is satisfied that the person is guilty of an alternative offence against subsection 35P(2) or subsection 35P(2A)—then the trier of fact may convict the person of the alternative offence. This is provided, however, that the person has been accorded procedural fairness in relation to the alternative offence. A provision of this kind may be of utility in cases in which there is evidence suggesting that the ‘entrusted person’ knew or intended that the disclosure would cause harm, but there may be reasonable doubt as to the person’s status as an ‘entrusted person’. This would ensure that fresh charges would not need to be laid.


387. Ibid.
that disclosure will be harmful, or intend to cause harm, this would require the removal of proposed subsection 35P(2) from the 2016 Bill, with the only offence applying to outsiders being the “aggravated offence” in proposed subsection 35P(2A).

On the other hand, it might be argued that limiting the fault elements to knowledge or intention could have unintended, adverse consequences. It may allow conduct to go unpunished, which should arguably be regarded as culpable. It might reasonably be argued that a person who is aware of a substantial risk that the information they are considering disclosing relates to an SIO, and a substantial risk that their disclosure may have a harmful effect, should be held criminally responsible if they unjustifiably take that risk.

**New prior publication defence — proposed subsection 35P(3A) (item 6)**

Proposed subsection 35P(3A) contains the defence of prior publication which applies only to the ‘outsider’ offences in proposed subsections 35P(2) and 35P(2A).

Consistent with the general principles of criminal responsibility in subsection 13.3(3) of the *Criminal Code*, the defendant bears the evidentiary burden in relation to this defence. This means that he or she must adduce or point to evidence suggesting a reasonable possibility the relevant matters exist. If the defendant does so, the prosecution must then discharge its legal burden to negate that possibility beyond reasonable doubt.

The defence contains four elements, the third of which was not explicitly recommended by the INSLM:

- **paragraph 35P(3A)(a)** — the information disclosed must ‘already been communicated, or made available, to the public (‘prior publication’)
- **paragraph 35P(3A)(b)** — the person was not directly or indirectly involved in the prior publication
- **paragraph 35P(3A)(c)** — at the time of disclosure, the person believes that the disclosure will not endanger the health or safety of any person, and will not prejudice the effective conduct of an SIO
- **paragraph 35P(3A)(d)** — having regard to the nature, extent and place of the prior publication, the person has reasonable grounds for that belief.

The Explanatory Memorandum states that the exception, framed in this way, is needed to accommodate circumstances in which a subsequent disclosure of information already in the public domain may cause additional harm. The Explanatory Memorandum refers to the example of information being brought into the public domain inadvertently, such as where a classified document is released in error. While prompt action might be taken to reverse the publication, a subsequent disclosure on a large scale “is likely to bring that information to the attention of a much greater number of people and could result in considerable new or additional harm.”

**Comment on the “prior publication” defence**

**Interaction with the fault elements applying to proposed paragraphs 35P(2)(c) and 35P(2A)(c)**

It is difficult to see how proposed subsection 35P(3A) will, in practical terms, add significant additional protection to the requirements of proof in relation to the harm elements in proposed paragraphs 35P(2)(c) and 35P(2A)(c).

That is, the effect of proposed subsection 35P(3A) is that the offences in proposed subsections 35P(2) and 35P(2A) do not apply to a person who believes, on reasonable grounds, that a disclosure of previously published information will not cause the harm or damage of the kind specified in proposed subparagraph 35P(3A)(c)(i) or subparagraph 35P(3A)(c)(ii).

Yet the offences in proposed paragraphs 35P(2)(c) and 35P(2A)(c) apply to persons who (respectively) are reckless that the disclosure will cause harm of the same kind as that specified in proposed subparagraph 35P(3A)(c)(i) or subparagraph 35P(3A)(c)(ii); or who know or intend that their disclosure will cause harm of that kind.

---

389. Ibid., pp. 185–186.
390. As per proposed paragraph 35P(3A)(c).
391. As per proposed paragraph 35P(3A)(d).
In other words, if a person discloses information, which he or she believes on reasonable grounds will not endanger health or safety, or will not prejudice the effective conduct of an SIO, then it is difficult to envisage how he or she might credibly be at risk of prosecution in the first place and therefore have need to rely on the proposed prior publication defence.

The INSLM’s report endorsed a recommendation of the Review of Commonwealth Criminal Law: Final Report, Chaired by former Chief Justice of the High Court of Australia, Sir Harry Gibbs (‘Gibbs Review’). The Gibbs Review recommended a prior publication defence, but also made the following statement:

31.33 The Review Committee sees considerable merit in the suggestion in effect put forward by the Communications Law Centre of the University of New South Wales that there should be no assumption that a second or subsequent disclosure would be harmful or more harmful than the original disclosure and that the test should be the actual harm done by the re-publication of the information having regard to any prior publication of the information. Indeed, assuming that is the effect of the law, then, in relation to the categories of information, disclosure of which would, under these proposals attract criminal sanctions only on proof of harm, there would appear to be little requirement for a specific defence of prior publication. [Emphasis added.]

31.34 However, the limited categories of information as to which this Report proposes no requirement for proof of harm must be taken into consideration. Circumstances are readily available where information in these categories disclosed without authority is so widely published that a further publication will cause no additional damage. Indeed, that is what happened in the UK in the case of the Spycatcher publication. In such circumstances, it would be nonsensical to punish the subsequent publisher, provided that person had not been involved in the prior publication. 392

Stakeholder consultation

The Government stated, in its response to the INSLM’s report, that it would consult with stakeholders in developing a prior publication defence. It is not known whether such consultation has taken place (or will take place). In the event that such consultations have been undertaken, it is not evident how the views of relevant stakeholders have been taken into consideration, particularly the views of media organisations and others who may have occasion to rely on the proposed defence.

In this regard, it is worth noting that the MEAA was critical of the INSLM’s recommendation for a prior publication defence, describing it as creating ‘a game of chicken for journalists’ in that ‘any journalist seeking to be the first to publish a legitimate news story would face prosecution while any subsequent story written after that point would be defensible’ (provided that the conditions of the defence were satisfied). 393

Application of existing exceptions in subsection 35P(3) to the new offences (item 5)

Item 5 amends subsection 35P(3), which contains exceptions to the disclosure offences. It adds a reference to all four new offences so that the exemptions in subsection 35P(3) will apply to them.

Extended geographical jurisdiction—subsection 35P(4) (item 7)

Item 7 amends subsection 35P(4) to apply the existing extended geographical jurisdiction provision to all of the new offences.

Subsection 35P(4) provides that the offences in section 35P are subject to what is known as ‘Category D’ extended geographical jurisdiction under section 15.4 of the Criminal Code. This means that a prosecution can be brought in relation to conduct occurring wholly outside Australia. (However section 16.1 of the Criminal Code provides that the Attorney-General’s consent is required to a prosecution brought under Category D jurisdiction, if the defendant is not an Australian citizen or a body corporate incorporated under an Australian law.)

The Explanatory Memorandum to the NSLA Bill states that applying Category D jurisdiction to section 35P was considered ‘necessary to ensure that the offences apply to SIO participants or persons who have knowledge of an SIO who are not Australian citizens and who engage in unauthorised disclosures outside Australia’. 394 This was

393. MEAA, Journalists still face jail under ASIO Act changes, op. cit.
justified on the basis that the risk of harm to Australia’s national security and intelligence-gathering capabilities as a result of unauthorised disclosures did not depend on the physical location of the discloser.\footnote{395}

Importantly, the continued application of Category D jurisdiction means that the new “outsiders offences” will, if enacted, continue to apply to foreign journalists or other non-Australian persons who are ‘whistleblowers’ who may obtain and choose to disclose information relating to an SIO.

Other issues—omissions from the 2016 Bill

Statutory prosecutorial consent requirement

The 2016 Bill does not propose the enactment of a statutory requirement that prosecutions of offences against section 35P may only be commenced with the consent of the Attorney-General. The absence of such a provision stands in contrast to other offences in the \textit{ASIO Act}, which are subject to a statutory requirement of this kind.\footnote{396}

It is suggested that there would be benefit in enacting a statutory consent requirement in preference to continued reliance on the Attorney-General’s direction to the CDPP regarding the potential prosecution of journalists. This would also strengthen the value of a consent requirement as a safeguard, since legislation—unlike Ministerial directions—cannot be revoked or amended unilaterally by the Executive Government of the day. In addition, in a joint submission to the INSLM in January 2015, the Attorney-General’s Department and ASIO stated:

Given that prosecutorial consent requirements are generally incorporated in the relevant offence provisions rather than by way of an executive direction, we consider there would be benefit in inserting a general prosecutorial consent requirement in section 35P.

Having the requirement for prosecutorial consent apply in respect of the provision as a whole rather than just in relation to the prosecution of journalists could also alleviate the difficulty identified by the PJCIS in identifying a person as a journalist for the purpose of the prosecutorial consent requirement, and could remove any potential (actual or perceived) for arbitrariness in this regard.\footnote{397}

Alternatively, if there is no intention to replace the existing direction to the CDPP with a statutory consent requirement, expanding its application to all prosecutions (not just journalists) may remove the potential for, or perception of, arbitrariness or preferential treatment of classes of prospective defendants.

Further, according to the National Tertiary Education Union (NTEU), on 30 March 2015, the Chief of Staff to the Attorney-General informed the NTEU that the Government would give ‘careful consideration’ to the NTEU’s suggestion to expand the direction to academics and researchers. The outcome of any such consideration does not appear to have been announced publicly.\footnote{398}

Further consideration of alternative or complementary measures

Although the INSLM considered that a public interest defence would not be necessary if other amendments to section 35P were made, this appears to be a policy issue in respect of which reasonable minds may differ. Accordingly, Members of the Parliament may wish to continue consideration of possible alternative or complementary measures to those proposed in Schedule 18, in the course of debating the 2016 Bill.

Several stakeholders continue to support alternative approaches. For example, the MEAA stated that the amendments would not change the ‘fundamental intent of section 35P’, which was said to be ‘to intimidate whistleblowers and journalists’ and to ‘stifle and punish legitimate public interest journalism’.\footnote{399}

Legal academic Dr Kieran Hardy also supports a public interest defence in addition to implementing the INSLM’s recommendations. He described the INSLM’s recommendations as making it ‘more difficult to prosecute

\footnotesize{395. }Ibid.
\footnotesize{396. }ASIO \textit{Act}, subsection 18C(4) and subsection 92(3).
\footnotesize{397. }Attorney-General’s Department and ASIO, \textit{Submission to the INSLM inquiry into the impact on journalists of section 35P of the ASIO Act}, January 2015, p. 29.
\footnotesize{398. }Kwok (NTEU), ‘Attorney-General to consider further protections for academics from s 35P offences’, op. cit. (The NTEU uploaded a \textit{copy of the letter}, which states, at p. 4, ‘the Government will give careful consideration to your organisation’s suggestion that the consent requirement is extended to academics and researchers who make disclosures in that professional capacity.’)
\footnotesize{399. }MEAA, \textit{Journalists still face jail under ASIO Act changes}, op. cit.
journals compared to the offence as it stands’ but argued that the absence of a public interest defence fails to address ‘the major issue with the offence—that section 35P does not provide any scope for journalists to disclose information in the public interest’. On this basis, Dr Hardy disagreed with the INSLM’s conclusion that a public interest defence would be unnecessary if the ‘outsiders offences’ were enacted as recommended.

**Other provisions**

**Exemptions to terrorism organisation offences: funds for legal representation (Schedule 1)**

Sections 102.6 and 102.8 of the *Criminal Code* criminalise getting funds to, from or for a terrorist organisation and associating with terrorist organisations respectively. The COAG Review recommended an exemption to the offence in section 102.6 for receipt of funds from a terrorist organisation for legal advice or representation in connection with a range of proceedings. Schedule 1 of the Bill will partially implement that recommendation by exempting receipt of funds solely for the purpose of ‘legal advice or legal representation in connection with the question of whether the organisation is a terrorist organisation’. It will also include an equivalent exemption to the offence in section 102.8 (which the COAG Review recommended, by majority, be repealed).

This Schedule is unchanged from the 2015 Bill. The PJCIS did not recommend any changes.

**Security assessments by ASIO (Schedule 12)**

ASIO’s security assessment function is set out in Part IV of the *ASIO Act*. Security assessments are written statements provided by ASIO in relation to:

- the question of whether it would be consistent with the requirements of security for ‘prescribed administrative action’ to be taken in respect of a person or
- the question of whether the requirements of security make it necessary or desirable for prescribed administrative action to be taken in respect of a person.

‘Prescribed administrative action’ is defined in section 35 of the *ASIO Act*. The sorts of actions it refers to include, for example, decisions relating to visas, passports and citizenship, and action that relates to or affects a person’s access to information or places to which access is restricted on security grounds.

The definition of ‘security assessment’ in section 35 of the *ASIO Act*, and section 40 of the Act, currently limit the circumstances in which security assessments may be provided to states and state authorities, and how they may be provided. Currently, a security assessment may be provided to a state or state authority:

- via a Commonwealth agency, where any prescribed administrative action in relation to a person by the state or state authority would affect security in connection with matters within the functions and responsibilities of that Commonwealth agency or
- directly, if the prescribed administrative action would affect security in connection with an event designated in writing by the Minister as a special event, and would affect security in connection with matters within the functions and responsibilities of a Commonwealth agency.

Schedule 12 will amend Part IV of the *ASIO Act* so that ASIO would be permitted to provide security assessments directly to states and state authorities, but retain the option of providing them via a Commonwealth agency where appropriate.

It will also remove the limitation whereby a security assessment may only be provided to a state or state authority where the prescribed action ‘would affect security in connection with matters within the functions and responsibilities of a Commonwealth agency’.

---

400. Hardy, ‘Despite changes, terror law will still curb freedom’, op. cit.
401. Ibid.
404. Item 1 of Schedule 1.
406. ASIO Act, section 35; ‘Security’ is defined in section 4 of the Act.
407. ASIO Act, section 40.
408. Item 4 of Schedule 12, proposed replacement subsection 40(1).
ASIO will be prohibited from providing information or advice (whether directly or via a Commonwealth agency) that it knows is intended to be used, or likely to be used, by a state or state authority in considering prescribed administrative action in relation to a person, except in the form of a security assessment.\(^{410}\)

The amendments will not affect the rights of a person to apply to the AAT for review of an adverse or qualified security assessment under Division 4 of Part IV of the ASIO Act. This is because such a review is of the security assessment itself, not any decision the assessment informed.

Section 61 of the ASIO Act requires Commonwealth agencies involved in decisions to which the assessment is relevant to treat any AAT finding that does not confirm the assessment as superseding it. Item 7 of Schedule 12 in the 2016 Bill will amend section 61 to impose the same requirement on states and state authorities, implementing recommendation 19 of the PJCIS’s report on the 2015 Bill.\(^{411}\)

**Classification of publications et cetera (Schedule 13)**

Schedule 13 of the Bill will amend the Classification Act to extend the threshold test for the requirement to refuse classification to a publication, film or computer game that advocates the doing of a terrorist act by extending the definition of ‘advocates’.\(^{412}\)

At present, paragraph 9A(2)(a) of the Classification Act requires classification to be refused where the publication, film or computer game ‘directly or indirectly counsels or urges the doing of a terrorist act’. Item 1 will amend this to also refuse classification where the publication, film or computer game ‘promotes’ or ‘encourages’ the doing of a terrorist act.

This extension of the definition of advocating a terrorist act is identical to the change to that definition in paragraph 102.1(1A)(a) of the Criminal Code. The definition in the Criminal Code was amended by the Counter-Terrorism Legislation Amendment (Foreign Fighters) Act 2014 in December 2014.\(^{413}\)

In explaining the addition of these terms to the definition, the Explanatory Memorandum states:

> While there may be some overlap with the terms ‘counsels’ or ‘urges’ the doing of a terrorist act, which may include conduct such as inducement, persuasion or insistence, or to give advice about the doing of a terrorist act, the inclusion of the additional terms is designed to ensure coverage of a broader range of conduct that may be considered as advocating the doing of a terrorist act, beyond the existing conduct of ‘counsels’ or ‘urges’.\(^{414}\)

As noted in the ‘Position of major interest groups’ section of this Digest, some stakeholders were concerned this measure could limit freedom of expression by also restricting legitimate discussion. AGD’s supplementary submission to the PJCIS stated:

> Schedule 13 is not intended to, and is unlikely to affect, artistic freedom. A publication, film or computer game will not advocate the doing of a terrorist act merely because it depicts, describes or discusses terrorist acts. Under the proposed changes to the definition of advocates, the content must directly or indirectly ‘counsel, urge, promote or encourage’ the doing of a terrorist act.\(^{415}\)

This Schedule is unchanged from the 2015 Bill. The PJCIS did not recommend any changes.

---

409. Ibid.
410. ASIO Act, subsection 40(2), as amended by item 5 of Schedule 12.
413. Counter-Terrorism Legislation Amendment (Foreign Fighters) Act 2014.
415. AGD, Supplementary submission to NJCIS, op. cit., p. 32.
Delayed notification search warrants (Schedule 14)

A scheme allowing delayed notification search warrants (DNSWs) was enacted in 2014, implementing a recommendation of the former INSLM.416 DNSWs are only available in relation to suspected terrorism offences punishable on conviction by imprisonment for seven years or more.417

Schedule 14 will amend various provisions in Part IAAA of the Crimes Act to clarify that rather than being required to themselves hold certain suspicions and beliefs, the AFP Commissioner (who must consent to an application being made) and an issuing officer must be satisfied the officer applying for the warrant holds those suspicions and beliefs on reasonable grounds.418 The thresholds that must be met for an officer to seek a warrant will remain unchanged.419 The amendments will bring the provisions for the issue of warrants into closer alignment with the general offence-related search warrant scheme in Part IAA of the Crimes Act.420

This Schedule is unchanged from the 2015 Bill. The PICIS did not recommend any changes.

Dealing with national security information in proceedings (Schedule 16)

Schedule 16 will amend the NSI Act to provide that orders made by a court under that Act in relevant circumstances will override any disclosure requirements provided by the regulations.421

The relevant existing provisions in the NSI Act require court orders made under existing subsections 19(1A) and (3A), relating to dealing with national security information in criminal and civil proceedings, to be consistent with both the Act and the regulations. The proposed amendments provide that these orders must be consistent with both the NSI Act and its regulations except where the orders are made on an application by the Attorney-General or a representative. In these situations, the orders would not need to be consistent with the regulations.

This proposal is similar to existing provisions providing for the regulations not to apply to information that is subject to orders under subsections 22(2) or 38B(2), both of which relate to the disclosure of national security information. The principle difference is that the existing provisions relate to situations where the Attorney-General, prosecutor and defendant or their representative have agreed to arrangements about the disclosure of the information.

While the proposed amendments extend the nature of orders able to be inconsistent with the regulations beyond arrangements agreed to by all parties, to also include applications made by the Attorney-General, some safeguard is provided by the requirement that the orders must still be made by the court, and the court must consider the orders to be appropriate in the interest of national security ( subsections 19(1A) and (3A)).

Proposed subsections 23(2) and 38C(2) also maintain the existing ability for orders made under existing sections 22 and 38B respectively to override any disclosure requirements provided by the regulations, but clarify that the regulations continue to apply to aspects of the information not dealt with by the order.

This Schedule is unchanged from the 2015 Bill. The PICIS did not recommend any changes to the provisions. However, it did recommend amendments to the Explanatory Memorandum to correctly reflect the proposed amendments (recommendation 7); this has been addressed in the Explanatory Memorandum to the 2016 Bill.

Disclosures by taxation officers (Schedule 17)

The amendments in Schedule 17 of the Bill will broaden the range of circumstances in which protected taxation information may be disclosed to Australian government agencies to allow disclosure for security related purposes. This is consistent with other disclosures permitted by the Taxation Administration Act 1953.423

417. Crimes Act, subsection 3ZZAA(4).
418. ‘Eligible issuing officer’ is defined in section 3ZZAD of the Crimes Act. Only certain judges and members of the Administrative Appeals Tribunal fall within the definition.
419. Existing and proposed section 3ZZBA of the Crimes Act.
420. Crimes Act, section 3E(1). The issuing officer is required to be satisfied that there are reasonable grounds for the relevant suspicion, not to hold that suspicion him or herself.
422. PICIS, Advisory report on the Counter-Terrorism Legislation Amendment Bill (No.1) 2015, op. cit., pp. 82–86.
423. Taxation Administration Act 1953.
Section 355-70 of Schedule 1 to the *Taxation Administration Act 1953* already provides for disclosure to law enforcement and related agencies in listed circumstances. However, the Government considers there is a need for such information to be available to other agencies that may be involved in national security functions, and points specifically to the example of the AFP-led National Disruption Group (NDG). The NDG was formed to prevent, disrupt and prosecute Australian involvement in foreign fighter activities, and along with several law enforcement agencies, includes the Departments of Human Services and Social Services.

Disclosure of protected taxation information is an offence under section 355–25 of Schedule 1 to the *Taxation Administration Act 1953*. Section 355–65 contains tables listing exceptions to the offences under section 355–25 to allow taxation officers to disclose protected information when performing certain duties. Subsection 355–65(2) provides Table 1, which lists exceptions allowing the disclosure of information ‘relating to social welfare, health or safety’.

**Item 1 of Schedule 17** will insert proposed new item 10 to the table in subsection 355-65(2) to provide an additional exception allowing the disclosure of information to an Australian government agency where the disclosure is for the purposes of ‘preventing, detecting, disrupting or investigating conduct that relates to a matter of security as defined in section 4 of the *Australian Security Intelligence Organisation Act 1979*’.

This amendment will broaden the range of circumstances in which protected taxation information may be disclosed to Australian government agencies. However, the proposed item may be considered to be in keeping with the intent of the many existing exceptions for law enforcement purposes in section 355-70.

**Item 2 of Schedule 17** will insert proposed section 355-182 to provide a further exception to ensure that information obtained under the exception above can be shared with the Commonwealth Ombudsman for the purposes of a function or duty of the Ombudsman. This will implement recommendation 20 of the PJCIS’s report on the 2015 Bill.

**Concluding comments**

**Measures previously included in the 2015 Bill**

Recent reforms to Australia’s already strong legislative framework for protecting national security and countering terrorism have included new and expanded offences, additional and broader powers for law enforcement and intelligence agencies, and new grounds on which dual nationals may lose their Australian citizenship. Those reforms included two sets of amendments to the control order regime passed in 2014 that expanded both the grounds on which orders may be sought and the purposes for which they may be granted.

Most of the key amendments in the Bill also concern the control order regime, either directly, via the proposed reduction of the minimum age for control orders, or indirectly, through proposed changes to control order proceedings and the proposed monitoring powers regime. The latter of these would make coercive powers normally used for investigations or monitoring compliance with regulatory schemes available for broader preventative and protective purposes.

Implementation in the 2016 Bill of the PJCIS’s recommendations on the 2015 Bill will increase safeguards and improve accountability associated with those measures. However, with the exceptions of replacing the court-appointed advocates scheme for young people with a special advocates scheme and amendments to narrow the scope of the offence of advocating genocide, implementation of those recommendations leave the scope of many of the actual measures largely unchanged.

**New measures**

As a general proposition, a regime of special advocates has the potential to improve procedural fairness in relation to control order applications where sensitive information is withheld from the subject of an order (or his or her lawyer). However, it is suggested that the particular scheme proposed in the 2016 Bill has not been subject to sufficient scrutiny to provide the Parliament with a meaningful assurance that its provisions will be workable and effective in practice. Further review, of a participatory and transparent kind, is arguably needed.

The referral of Part 2 of Schedule 15 to a Parliamentary committee for inquiry and report would seem to be a

---

425. AFP, ‘National efforts’, AFP webpage.
sensible and prudent step, so that the Parliament may hear directly from key stakeholders who would operate under the proposed scheme.

The proposed amendments to section 35P of the ASIO Act in Schedule 18 implement the Government’s response to the recommendations of the INSLM’s report of October 2015. Overall, the proposed measures are reasonably consistent with those recommendations. However, a number of ambiguities and uncertainties are also apparent in the framing and drafting of the proposed provisions. The relationship between the proposed “insiders” offence and the existing offence in subsection 18(2) of the ASIO Act may be problematic.

Members of the Parliament may wish to consider the merits of complementary or alternative measures to the Government’s proposed amendments. In particular, several interest groups, including members of the legal profession and the media, continue to support a public interest defence. They have disputed the conclusions and reasoning of the INSLM on this issue of policy, and their basis for doing so does not seem unreasonable.