National Security Legislation Amendment Bill (No. 1) 2014

Monica Biddington
Law and Bills Digest Section
Cat Barker
Foreign Affairs, Defence and Security Section

Contents

The Bills Digest at a glance .................................................. 3
Purpose of the Bill ................................................................. 4
Structure of the Bill ................................................................. 4
Background ............................................................................... 5
Protection of intelligence-related information .......................... 5
Committee consideration ......................................................... 5
Policy position of non-government parties/independents..... 6
Australian Labor Party (ALP)................................................. 6
Australian Greens................................................................. 6
Specific comments on the Bill ................................................. 6
Position of major interest groups ............................................. 7
Other comments........................................................................ 8
Financial implications ............................................................ 9
Statement of Compatibility with Human Rights ....................... 9
Key issues and provisions ....................................................... 11
Schedule 1 – ASIO employment et cetera............................... 11
Schedule 2—ASIO powers ....................................................... 12
Access to computers ............................................................... 12
Issue: breadth of the new definitions of ‘computer’ and ‘target computer’ .............................................. 13
Use of a third party computer or communication to execute a computer access warrant ............................ 13
Issue: threshold and safeguards ............................................ 14
Disruption of target and third party computers....................... 14

Date introduced: 16 July 2014
House: Senate
Portfolio: Attorney-General
Commencement: Sections 1 to 3 commence on Royal Assent; Schedules 1 to 6 commence on the 28th day after Royal Assent; Schedule 7 commences on 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 http://www.aph.gov.au/Parliamentary_Business/Bills_Legislation

When Bills have been passed and have received Royal Assent, they become Acts, which can be found at the ComLaw website at http://www.comlaw.gov.au/.
Issues: disruption of third party computers and communications ................................................. 15
Use of surveillance devices .................................................... 15
   Issue: adequacy of accountability and reporting requirements .................................................. 17
Identified person warrants .................................................. 18
   Warrants .......................................................................... 18
   Authorisations .................................................................. 19
Variations to warrants issued under Division 2 of Part III of the ASIO Act .............................................. 20
   Issue: lack of limitations on the nature of variations ....... 21
Evidentiary certificates ......................................................... 22
   Issue: computer access under a search warrant .......... 22
Authorisation to execute ASIO warrants ......................... 23
Other amendments to ASIO warrant provisions .......... 23
   Issue: use of force against persons ................................. 24
Issue: accountability for and oversight of warrant powers in Division 2 of Part III of the ASIO Act ............ 24
Schedule 3—Special intelligence operations ..................... 24
   Applications for and granting of authorities and variations to authorities .......................................... 25
   Issue: lack of appropriate limits on variations .......... 26
Effect of SIO authorities ....................................................... 27
Offences for unauthorised disclosure of information ....... 27
   Issue: scope of offences .................................................. 29
Reporting requirements ....................................................... 30
   Issue: adequacy of accountability and reporting requirements .................................................. 30
Schedule 4—ASIO co-operation and information sharing .... 31
Schedule 5—Activities and functions of Intelligence Services Act 2001 agencies ........................................ 32
Schedule 6—Protection of information .............................. 33
Schedule 7—Renaming of Defence agencies .................... 35
Concluding comments ......................................................... 36
The Bills Digest at a glance

• This Bills Digest provides an independent analysis of the background, issues and provisions of the National Security Legislation Amendment Bill (No.1) 2014 (the Bill) for the purposes of Parliamentary debate.

• One of the key issues for debate will be the lack of scrutiny the Bill itself has had at the time of debate. While the Bill has been referred to the Parliamentary Joint Committee on Intelligence and Security (PJCIS), many stakeholders were unhappy with the time allowed for submissions, and it appears that the Bill may be debated prior to the tabling of the PJCIS’s report.

• The Senate Scrutiny of Bills Committee and the Parliamentary Joint Committee on Human Rights have not yet reported on their consideration of the Bill.

• The Bill will implement the majority of Recommendations in Chapter 4 of the PJCIS’ 2013 Report of the Inquiry into Potential Reforms of Australia’s National Security Legislation.

• The Bills Digest considers each Schedule to the Bill and focuses on Schedules 2, 3 and 6.

• Schedule 2 will update and expand the Australian Security Intelligence Organisation’s (ASIO’s) powers, including by modernising and expanding powers relating to computer and data access under warrant, aligning ASIO’s surveillance device powers with those available to law enforcement and introducing ‘identified person’ warrants. The provisions are broadly consistent with the PJCIS’s recommendations, but safeguards and accountability requirements could be improved.

• Schedule 3 will introduce a ‘special intelligence operation’ (SIO) scheme under which ASIO officers and affiliates will be protected from criminal and civil liability for certain conduct engaged in for the purpose of an SIO. The safeguards and accountability requirements are less stringent than recommended by the PJCIS. Parliamentarians and media organisations have expressed concerns about the proposed offences for unauthorised disclosure of information about an SIO, particularly their potential application to journalists.

• Schedule 6 will create two new offence provisions and update existing offences relating to the unauthorised disclosure of intelligence related information. The penalty for existing offences will be increased from two years to ten years imprisonment.

• The Bill is one of three national security Bills foreshadowed by the Abbott Government in 2014. This Bill does not address matters relating to proposed changes to passport laws for foreign fighters, or mandatory data retention by telecommunications authorities for the purpose of law enforcement and national security.
Purpose of the Bill
The main purpose of the Bill is to implement recommendations made in Chapter 4 of the PJCIS’s Report of the Inquiry into Potential Reforms of Australia’s National Security Legislation (2013 PJCIS Report) by:

- amending the Australian Security Intelligence Organisation Act 1979 (ASIO Act) to:
  - align ASIO’s employment conditions with the Australian Public Service employment framework
  - modernise and streamline ASIO’s intelligence collection powers
  - establish a framework for the conduct of authorised covert intelligence operations
  - clarify ASIO’s ability to cooperate with the private sector and
  - provide for certain breaches to be referred to law enforcement agencies for investigation and
- amending the Intelligence Services Act 2001 (IS Act) to:
  - enable the Australian Secret Intelligence Service (ASIS) to collect intelligence on Australian persons involved in activities in relation to operational security
  - enable ASIS to cooperate with ASIO without ministerial authorisation when undertaking certain intelligence collection activities
  - enable ASIS to train certain individuals in the use of weapons and self-defence techniques and
  - clarify the authority of the Defence Imagery and Geospatial Organisation (DIGO) to assist government authorities with geospatial and imagery products.\(^1\)

The Bill will also:

- amend the ASIO Act and IS Act to update existing offences and increase penalties, and create two new offences in relation to the protection of intelligence-related information and
- amend the IS Act to extend immunity for actions taken in relation to overseas activities; and rename DIGO as the Australian Geospatial Intelligence Organisation and the Defence Signals Directorate (DSD) as the Australian Signals Directorate.

Structure of the Bill
The Bill is presented in seven Schedules.

Schedule 1 relates to ASIO employment conditions and will introduce a new employment framework into Part V of the ASIO Act.

Schedule 2 will make a range of amendments to ASIO’s powers, including by modernising and expanding powers relating to computer and data access under warrant, updating surveillance device powers and introducing ‘identified person’ warrants.

Schedule 3 will make amendments to provide ASIO employees and ASIO affiliates (newly defined terms) with limited protection from criminal and civil liability for the purposes of ‘special intelligence operations’.

Schedule 4 will clarify ASIO’s ability to cooperate with the private sector. It will also enable matters of prohibited disclosure of identity to be referred to law enforcement agencies for investigation.

Schedule 5 will amend the IS Act to enable cooperation between ASIS and ASIO in relation to the production of intelligence. This Schedule will make significant procedural changes to the levels of authorisation required for ASIO and ASIS employees.

Schedule 6 relates to the protection of intelligence-related information. Two new offence provisions will be created, and penalties for existing offences increased, for the unauthorised communication of intelligence information.

Schedule 7 will make amendments to rename DIGO as the Australian Geospatial Intelligence Organisation (AGO) and DSD as the Australian Signals Directorate (ASD).

**Background**

The Bill is the first tranche of the Abbott Government’s proposed reforms to national security legislation. There has been significant media attention about measures that are yet to be introduced, which will address issues relating to foreign fighters and mandatory data retention. This Bill does not address these issues. Rather, it focuses on the powers of the intelligence agencies to obtain and gather intelligence for the purpose of protecting national security.

In May 2012, the then Attorney-General, Nicola Roxon, asked the Parliamentary Joint Committee on Intelligence and Security (PJCIS) to consider a range of potential national security reforms. The Government subsequently released a discussion paper outlining reforms it wished to progress, those it was considering and those on which it expressly sought the views of the PJCIS. The potential reforms related to telecommunications interception and access to telecommunications data; telecommunications sector security; and legislation governing the Australian Intelligence Community (AIC). The PJCIS tabled its report in June 2013. The 2013 PJCIS Report included 42 recommendations including, in chapter 4, 24 in relation to legislation governing the AIC. The Bill proposes to, amongst other things, implement the majority of those recommendations. This Digest refers to particular recommendations, and assesses the Bill’s consistency with them, where relevant.

**Protection of intelligence-related information**

Edward Snowden, a former National Security Agency employee in the United States, has been accused of espionage, charged with theft of government property, unauthorised communication of national defence information and wilful communication of classified communications intelligence to an unauthorised person.

Snowden has been a whistleblower on intelligence matters and has been responsible for thousands of ‘leaks’ on matters relating to surveillance in the United States and other countries, including Australia:

Australian intelligence agencies are understood to have scoped the potential damage for future leaks from the Snowden affair and have assessed that between 15,000 and 20,000 secret Australian intelligence files could have been accessed by Snowden through his computer at NSA, although it is unknown how many of these he actually stole before seeking refuge in Russia.

The majority of the stolen reports are likely to discuss political, economic and military intelligence gleaned by Australian agencies, especially the Australian Signals Directorate (formerly DSD), in the Asia-Pacific region.

In this context, the Australian Government is introducing amendments to the offence provisions relating to the unauthorised disclosure of material that relates to intelligence information. This is not, according to the Attorney-General, a “Snowden” provision but instead is:

... designed to plug a gap in the existing legislation. Under the existing legislation, it’s a criminal offence for an officer of a national security agency to disclose intelligence material to a third party but it’s not an offence for an officer to copy or wrongfully remove that material. In other words, communication to a third party is an element of the current offence but it seems to us that it should be wrong and it should be an offence to illicitly remove intelligence material from an agency.

**Committee consideration**

On 17 July 2014, Australian Greens’ Senator Scott Ludlam moved a motion that the Bill be considered by the Senate Standing Committee on Legal and Constitutional Affairs for consideration and report by 8 November 2014. This was not agreed to by the Senate.

---

The Bill has been referred to the PJCIS for inquiry and report by 8 September 2014. Details of the inquiry are at the inquiry homepage.

It is possible that the Bill will be scheduled for debate before the report is tabled, with the Attorney-General, Senator George Brandis QC, stating at a joint press conference on 5 August 2014 that:

... [the] legislation is currently before a ... Committee and is due to report back in the first sitting fortnight of the spring sittings and we expect with the bipartisan support of the Australian Labor Party, which I acknowledge, that it will be through the Parliament in the first sitting fortnight of the spring sittings.

The Bill has not yet been considered by any other Parliamentary Committee. The lack of independent scrutiny and time for Members and Senators to consider the complexities of the Bill is concerning. It is particularly so in light of Recommendation 41 in the 2013 PJCIS Report. The PJCIS recommended that amendments implementing its recommended changes to AIC legislation be released as an Exposure Draft for public consultation as well as being subject to Parliamentary committee scrutiny and targeted consultation with the Independent National Security Legislation Monitor (INSLM) and the Inspector-General of Intelligence and Security (IGIS).

Policy position of non-government parties/independents

Australian Labor Party (ALP)
The ALP has not published a statement expressly supporting the Bill however, the Shadow Attorney-General, Mark Dreyfus QC, has given in-principle support to some proposals. More recently, there has been a suggestion that the ALP may block the proposed offences for unauthorised disclosure of information relating to special intelligence operations.

Australian Greens
On 16 July 2014, the date the Bill was introduced, the Australian Greens sought to ‘ensure the Bill is subject to rigorous committee review: we are concerned that the expanded powers may allow ASIO to implant spyware on computer networks operated by entirely innocent bystanders, and be granted immunity from the law’.

Specific comments on the Bill
The Shadow Attorney-General, Mark Dreyfus QC, and Independent Senator David Leyonhjelm have both expressed concerns about the proposed offences for unauthorised disclosure of information relating to a special intelligence operation in Schedule 3 of the Bill. Unlike the proposed offences in Schedule 6 of the Bill, which apply only to people who have worked for an intelligence agency, the offences in Schedule 3 apply to ‘any person’ and do not include any exception, for example, for a journalist reporting a matter in the public interest.

The Shadow Attorney-General has been quoted by The Guardian as follows:

“There are suggestions that the attorney general’s amendments to national security legislation could criminalise some reporting by journalists,” Dreyfus said in a statement.

“Senator Brandis has indicated that criminalising reporting of leaked national security information is not his intention. If Senator Brandis’s amendments would criminalise reporting by journalists who receive intelligence information, the government will need to make changes to remove that consequence.”

References:
Senator Leyonhjelm wrote in *The Australian* of his concerns:

I am alarmed that the government has introduced national security laws creating an offence of disclosing information about ASIO activities. This could potentially lead to the bulk of ASIO operations being classed as special intelligence operations and would make it an offence for journalists to report on information from whistleblowers.

In effect, they give ASIO immunity. If the role of ASIO is to serve the public, not the role of the public to serve ASIO, this should not be accepted.\(^{16}\)

The Palmer United Party has not released specific comments on this particular Bill.

**Position of major interest groups**

As noted above, the PJCIS is due to report on its inquiry into the Bill by 8 September 2014. Public hearings were held on 15 and 18 August 2014. Submissions were due by 6 August 2014, but until mid-August 2014, the submission from the Attorney-General’s Department (AGD) was the only one available on the inquiry webpage. The publication and timing of publication of submissions are at the discretion of Committees.

Like some Parliamentarians, media organisations have voiced concerns about the proposed offences for unauthorised disclosure of information relating to a special intelligence operation in Schedule 3 of the Bill. The Media, Entertainment & Arts Alliance wrote directly to the Attorney-General, stating:

MEAA is concerned over the Bill’s section 35P “Unauthorised disclosure of information” (appearing on page 69 of the Bill) that relates to penalties applied to a person disclosing information about a special intelligence operation. The penalties in the Bill are jail terms of between five and 10 years.

The Explanatory Memorandum makes it clear that the offences outlined in section 35P would apply to “disclosures by any person” and “persons who are recipients of unauthorised disclosure of information, should they engage in any subsequent disclosure”.

MEAA is concerned that this amendment would capture legitimate reporting of activities in the public interest. In doing so, it would criminalise journalists and journalism that performs a vital role in a healthy democracy of scrutinising government and its agencies.\(^{17}\)

*The Australian* newspaper supported the Shadow Attorney-General’s remarks in an editorial that was otherwise favourable towards the Bill:

Broadly, the new legislation deserves bipartisan support and was based largely on the advice of the Joint Parliamentary Inquiry on Intelligence and Security. But opposition legal affairs spokesman Mark Dreyfus raised a legitimate concern when he said amendments would be needed if one of the legislation’s consequences would be “criminalising journalism”. Senator Brandis insisted on Thursday that the new offences were not aimed at journalists or at placing constraints on freedom of speech. The legislation makes no such exemptions, however, which could open the way for its misuse by a government or bureaucracy intent on secrecy to avoid embarrassment.\(^{18}\)

Guardian Australia submitted that the PJCIS seek ‘a higher level of evidence and explanation to demonstrate the necessity of the powers and immunities being sought’.\(^{19}\) Further, it submitted that the PJCIS should find that the powers and immunities currently sought are disproportionately strong and the safeguards currently proposed are disproportionately weak.\(^{20}\)

---

20. Ibid.
While, the Law Council of Australia (LCA) welcomed some measures in the Bill in principle, it considered there are many aspects ‘of this Bill—such as those that seek to significantly expand the existing powers of intelligence agencies without including sufficient safeguards— that raise strong concerns’. 21

The concerns raised by the LCA in its submission have ‘led the Law Council to recommend that the NSLA Bill not be passed in its current form and the PJCIS should request the next appointed Independent National Security Legislation Monitor to consider the operation, effectiveness and implications of existing legislation with a view to addressing the issues which are raised by the Bill’. 22

The LCA stated the ‘tight timeframes for the present inquiry limits the capacity of the Law Council and other organisations to provide detailed analysis in relation to these proposals’. 23 This sentiment was echoed in several other submissions to the PJCIS’s inquiry into the Bill, including the Gilbert + Tobin Centre of Public Law (Gilbert + Tobin), Electronic Frontiers Australia and a joint submission from councils of civil liberties (CCLs). 24

Gilbert + Tobin welcomed many of the reforms, noting the Bill’s aims to ‘modernise the law to reflect developments in communications technology, to streamline the processes for intelligence agencies to apply for various types of warrants and also to provide some clarification as to the scope of the powers that these agencies possess. 25 However, Gilbert + Tobin has particular concerns about: computer access warrants (Schedule 2), establishing the special intelligence operations regime (Schedule 3), changing the rules under which ASIS may cooperate with ASIO in the performance of its functions (Schedule 5) and creating new disclosure offences for ASIO employees and contractors and increasing the maximum penalties for the existing offences (Schedule 6). 26

In relation to the proposed offences and increased penalties in Schedule 6, Gilbert + Tobin remarked that:

... the government’s claim that there are ‘significant gaps’ in the law is simply not supported. There is a wide range of existing offences that could apply to the disclosure of classified information, including severe penalties for terrorism, espionage and treason, as well as other penalties for disclosing official secrets and the disclosure of information by Commonwealth officers. And, contrary to the government’s suggestion that ‘no such offences exist’, many of these offences would also apply to the situation where a person merely possesses or retains information. Section 79 of the Crimes Act provides for a maximum penalty of seven years imprisonment where a person retains a classified document ‘when it is contrary to his or her duty to retain it’. Given this comprehensive array of existing offences, there is no demonstrable need to create a new ‘three tier structure’ for regulating the disclosure of classified information’. 27

The Inspector General of Intelligence and Security (IGIS), Dr Vivienne Thom, strongly argued in both a written submission and at a public hearing on the Bill, that more resources would be required by her office in order to effectively oversee the expanded powers proposed in the Bill. 28

**Other comments**

Professor George Williams has commented that:

The Abbott government has embarked on the biggest expansion of Australia’s anti-terrorism laws since the 2005 London bombings. Changes do need to be made. Many laws are in poor shape after being rushed through prior parliaments, while others need updating because of new technology.

---

22 Ibid., p. 5.
23 Ibid., p. 10.
26 Ibid., p. 2.
27 Ibid., pp. 13–14.
Unfortunately, the government has overreached in its reforms, which go much further than what is required. In fact, the extent to which its changes would extend the powers of government at the expense of citizens is unexpected and quite shocking.

The first bill is already in Parliament. It allows greater surveillance of computers, grants immunity from prosecution to intelligence officers engaged in special operations, and exposes journalists to jail for publishing even general information about a terrorism investigation. These changes are modest compared to what is to come.\(^{29}\)

Stakeholder concerns about specific aspects of the Bill are highlighted where relevant in the ‘Key issues and provisions’ section of this Digest.

**Financial implications**

The Explanatory Memorandum states that the Bill does not have a financial impact.\(^{30}\) However, the IGIS indicated that the Office of the IGIS would require an additional three to five staff in order to effectively oversee the new and expanded powers proposed in the Bill. The IGIS estimated that five additional staff would cost around $700,000 annually.\(^{31}\) Greg Carne of the University of New England suggested that additional funding should also be provided to the Office of the Independent National Security Legislation Monitor.\(^{32}\)

**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 Bill’s compatibility with the human rights and freedoms recognised or declared in the international instruments listed in section 3 of that Act.\(^{33}\)

The Bills engages a broad range of human rights and freedoms. The Statement of Compatibility states that the Bill will engage and limit:

- the right to protection against arbitrary and unlawful interferences with privacy and reputation in Article 17 of the *International Covenant on Civil and Political Rights (ICCPR)*—see:
  - Schedule 2; exercise of a range of powers under warrant and use of third party computers to access data in a target computer
  - Schedule 4; ASIO’s cooperation and information sharing and
  - Schedule 5; ASIS’s collection of intelligence on an Australian person and improving cooperation between ASIS and ASIO

- the right to security of the person under Article 9 of the *ICCPR* (see Schedule 2, in relation to the use of reasonable and necessary force against persons when executing warrants)

- the right to a fair hearing under Article 14 of the *ICCPR*—see:
  - Schedule 2; use of evidentiary certificates and
  - Schedule 3; special intelligence operations and related use of evidentiary certificates

- the presumption of innocence under Article 14(2) of the *ICCPR*—see:
  - Schedule 2; use of evidentiary certificates
  - Schedule 3; offences for unauthorised disclosures about special intelligence operations and use of evidentiary certificates and
  - Schedule 6; offences for unauthorised dealings with, and communication of, intelligence-related information

---

31. V Thom (IGIS), op. cit.
33. The Statement of Compatibility with Human Rights can be found in the Explanatory Memorandum to the Bill (see pages 3–34).
• the right to an effective remedy under Article 2 of the *ICCPR*—see:
  - Schedule 3; special intelligence operations and
  - Schedule 5; extending an immunity for officers of intelligence agencies for certain acts done outside Australia

• the right to freedom from arbitrary detention under Article 9 of the *ICCPR*—see:
  - Schedule 3; offences for unauthorised disclosures about special intelligence operations and
  - Schedule 6; offences for unauthorised dealings with, and communication of, intelligence-related information

• the prohibition on cruel, inhuman or degrading treatment or punishment in Article 7 of the *ICCPR* and the *Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment*—see:
  - Schedule 3; offences for unauthorised disclosures about special intelligence operations and
  - Schedule 6; offences for unauthorised dealings with, and communication of, intelligence-related information

• the right to freedom of movement under Article 12 of the *ICCPR*—see:
  - Schedule 3; offences for unauthorised disclosures about special intelligence operations and
  - Schedule 6; offences for unauthorised dealings with, and communication of, intelligence-related information

• the right to freedom of expression under Article 19 of the *ICCPR*—see:
  - Schedule 3; offences for unauthorised disclosures about special intelligence operations and
  - Schedule 6; offences for unauthorised dealings with, and communication of, intelligence-related information and

• the right to a fair trial in Article 14(1) of the *ICCPR*—see:
  - Schedule 3; special intelligence operations and
  - Schedule 6; offences for unauthorised dealings with, and communication of, intelligence-related information.

It also states that the Bill will promote:

• the right to work in Article 6 and 7 of the *International Covenant on Economic, Social and Cultural Rights (ICESCR)*—see:
  - Schedule 1; ASIO’s secondment arrangements and
  - Schedule 4; ASIO’s cooperation and information sharing

• the right to just and favourable conditions of work in Article 7 of the *ICESCR* (see Schedule 1, in relation to ASIO’s secondment arrangements) and

• the right to freedom of expression under Article 19 of the *ICCPR* (see Schedule 4, in relation to ASIO’s cooperation and information sharing).

The Statement of Compatibility outlines a detailed justification of each amendment that limits these human rights and freedoms and concludes that the Bill is compatible with human rights because ‘it promotes human rights and to the extent that it may limit human rights, those limitations are reasonable, necessary and proportionate.’ 34 However, some submitters to the PJCIS’s inquiry into the Bill have raised concerns about the human rights implications of the Bill. In particular:

---

34. Explanatory Memorandum, p. 34.
• a joint submission from several media organisations contends that the proposed offences for unauthorised disclosure of information related to special intelligence operations unacceptably ‘erode freedom of communication and freedom of the press’.

• the Pirate Party considers the proposed offences and increased penalties in Schedule 6 place undue restrictions on freedom of political communication and

• the CCLs argue that the Bill impacts disproportionately on the right to freedom of expression and the right to protection from arbitrary and unlawful interferences with privacy.

Key issues and provisions

Schedule 1 – ASIO employment et cetera.

This Schedule will make key amendments to the ASIO Act to amend the employment provisions to be harmonised with standards of the Australian Public Service. These changes are widely supported and not controversial, and implement Recommendation 26 of the 2013 PICIS Report. However, while the Explanatory Memorandum notes that these are ‘minor or technical amendments and do not have any human rights implications’, the LCA’s view is that ‘the amendments do not simply appear to be minor or technical... but increase the number of people able to perform duties and functions and exercise powers currently only permitted to be carried out by an officer or employee of ASIO.’ This is true; the new term ‘ASIO affiliates’ will expand the class of persons able to perform duties and functions previously limited to ASIO employees. This is not necessarily a concern in and of itself, so long as there are appropriate and similar safeguards and requirements for all those officers who are employed under the Act, including contractors and secondees.

New or amended definitions will be inserted into the ASIO Act, including:

• ASIO affiliate and ASIO employee (item 1)

• Deputy Director-General (item 2)

• senior position-holder (item 3) and

• authorised person (item 11).

The LCA noted at the public hearing on the Bill that:

The definition of ‘affiliate’ is quite broad... On our reading of the SIO scheme, it could authorise people beyond ASIO affiliates to be part of the scheme, so we raise some questions about providing criminal and civil immunity to people beyond that category. One thing that we have drawn attention to is that, in relation to the Crimes Act controlled operations scheme, there are some very tight controls on the conduct of people who are not law enforcement officers themselves.

Item 5 will make administrative amendments to the ASIO Act relating to delegations of power, functions or duties made under the Act. The Explanatory Memorandum confirms that any delegation of financial management will be made in accordance with the Public Governance, Performance and Accountability Act 2013.
Item 6 will amend an existing offence provision in subsection 18(2) for unauthorised communication of information or a matter that a person has obtained through being an officer or employee of ASIO or having a contractual agreement with ASIO. The amendment seeks to cover all persons associated with the organisation, including the newly defined terms of ASIO affiliate and ASIO employee. Note that the maximum penalty is amended by Item 1 of Schedule 6 from two to ten years.

Item 9 will make an amendment to existing section 23, which permits authorised persons to ask an operator of an aircraft or vessel questions relating to the aircraft or vessel, or its cargo, crew, passengers, stores or voyage. Further, the authorised persons are permitted to request an operator of an aircraft or vessel to produce documents relating to the aircraft or vessel, or its cargo, crew, passengers, stores or voyage, that are in the possession or under the control of the operator. The amendment is a consequence of expanding the class of persons who may be authorised under the ASIO Act.

Item 19 is the main amendment of interest in Schedule 1. This item will repeal existing provisions relating to the powers of the Director-General to employ officers to ASIO and substitute sections 84 to 89 with new sections to allow the Director-General to:

- engage persons as consultants or contractors (proposed new section 85)
- arrange for an ASIO employee to be seconded to a body or organisation within or outside Australia (proposed new section 86)
- arrange for a person to be seconded to ASIO (proposed new section 87).

The secondments may be subject to Ministerial Guidelines made under section 8A of the ASIO Act. That section, amongst other things, allows the Minister to, from time to time, by written notice given to the Director-General, give the Director-General guidelines to be observed about ASIO employees. The amendments relating to secondments implement Recommendation 26 of the 2013 PJCIS Report.

Proposed new section 88 will provide that, although ASIO employees are not employed under the Public Service Act 1999, the Director-General must adopt the principles of that Act in relation to ASIO employees to the extent to which the Director-General thinks they are consistent with the effective performance of the functions of ASIO.

Items 21-30 will make numerous minor amendments relating to the employment of persons under the ASIO Act as a result of the terminology amendments and new employment framework in proposed new sections 85-89.

Schedule 2—ASIO powers

Division 2 of Part III of the ASIO Act sets out the powers ASIO may access in order to fulfil its functions. Schedule 2 will make a range of amendments to Division 2, most of which address recommendations in the 2013 PCJIS Report (in particular, recommendations 20–23, 29–30, 32–33 and 35–37). Key measures include:

- modernising and expanding powers relating to computer and data access under warrant, including expanding the definition of ‘computer’ (item 4) and allowing for access via third party computers (item 23)
- aligning ASIO’s surveillance device powers with those in the Surveillance Devices Act 2004 (item 29)\(^{43}\) and
- the introduction of identified person warrants (item 41).

Access to computers

‘Computer’ is currently defined by section 22 of the ASIO Act to mean ‘a computer, a computer system or part of a computer system’. The PCJIS considered that the term ‘computer system’ may not be sufficient to take account of several computers networked together and recommended the definition be amended to include ‘multiple computers operating in a network’.\(^{44}\) It also recommended that computer access warrants issued under section 25A of the ASIO Act be able to authorise access to ‘all computers at a nominated location and all computers directly associated with a nominated person in relation to a security matter of interest’.\(^{45}\)

Item 4 of Schedule 2 will repeal and replace the definition of computer in section 22 of the ASIO Act for the purposes of Division 2 of Part III. It will provide that computer means all or part of one or more computers, one

---

44. 2013 PCJIS Report, op. cit., pp. 87–89 (recommendation 20, quote taken from p. 89).
45. Ibid.
or more computer systems, one or more computer networks, or any combination thereof. This is a significant expansion of the definition.

**Items 16 and 18** of Schedule 2 will amend subsection 25A(2) and insert **proposed subsection 25A(3)** to expand what is meant by ‘target computer’ for the purposes of a computer access warrant, by providing it may be one or more of the following:

- a particular computer
- a computer on particular premises or
- a computer associated with, used by, or likely to be used by, a person (whose identity may or may not be known).

**Issue: breadth of the new definitions of ‘computer’ and ‘target computer’**

In combination, the above amendments will significantly expand the computers to which access may be authorised under a single warrant. At its limit, a computer access warrant would be able (providing the threshold test in subsection 25A(2) is met) to authorise access to multiple computer networks across multiple locations on the basis that they are associated with a person whose identity is not known. The attempt to create a ‘catch-all’ definition of computer, together with the amendments in **items 16 and 18**, appear to have resulted in the amendments being drafted more broadly than intended by the PJCIS.

Commentators and several submitters to the PJCIS’s inquiry into the Bill have recognised the need for amendments to address technological advances, but suggested they be more precisely drafted. They have pointed out that in the absence of a definition of ‘computer network’, the definition of computer could potentially capture every computer on a university or public service network, cloud or peer-to-peer network, home computers used to access work-related networks remotely, and, ‘taken to its logical extreme … any computer that is connected to the world wide web’. Suggested improvements included a definition of ‘computer network’ that requires the individual computers in the network to be linked in a substantive way, such as having shared storage drives, or that is limited to local area networks.

Further, given the related expansion of the meaning of target computer, it is unclear why the definition of computer needs to refer to ‘one or more’ computer networks. The amendments to be made by **items 16 and 18** would appear to already cover the only circumstances in which it might be appropriate to authorise access to more than one computer network under a single warrant.

**Use of a third party computer or communication to execute a computer access warrant**

Section 25A provides for the issue of computer access warrants, with subsection 25A(4) setting out the things that may be authorised in such a warrant. **Item 23** of Schedule 2 will amend subsection 25A(4) by inserting **proposed paragraph 25A(4)(ab)** to enable ASIO to obtain access to relevant data in a target computer through the use of any other computer or communication in transit (such as an email) in certain circumstances, and if necessary for that purpose (and subject to **proposed new subsection 25A(5)**), to add, copy, delete or alter other data in that computer or communication. This amendment is intended to address the increasing difficulties ASIO is experiencing in accessing relevant data directly from a target computer due to technological developments. It responds to Recommendation 22 of the 2013 PJCIS Report, which proposed such access be allowed ‘subject to appropriate safeguards and accountability mechanisms, and consistent with existing provisions under the *Telecommunications (Interception and Access) Act 1979*’.

---


47. Gilbert + Tobin, op. cit., p. 3, D Leyonhjelm submission, op. cit., p. 3.

**Issue: threshold and safeguards**

The PJCIS considered that the same restrictions should apply to the use of third-party computers and communications as apply to access to third-party communications under a ‘B-party’ warrant issued under section 9 of the *Telecommunications (Interception and Access) Act 1979* (TIA Act). Under that section, the Attorney-General may issue a telecommunications interception warrant that allows ASIO to access a telecommunications service likely to be used by another person to communicate with a target, but only if he or she is satisfied that:

- ASIO has exhausted all other practicable methods of identifying the telecommunications services used, or likely to be used, by the target or
- interception of communications made to or from a telecommunications service used or likely to be used by the target would not otherwise be possible.

Such a warrant may only remain in force for up to three months (instead of the six month limit that otherwise applies to telecommunications interception warrants).

The amendment that will be made by item 23 falls short of replicating the restrictions that apply to B-party warrants issued under the TIA Act in two ways:

- access may be authorised ‘if, having regard to other methods (if any) of obtaining access to the relevant data which are likely to be as effective, it is reasonable in all the circumstances to do so’, instead of after all other practicable methods have been exhausted and
- the duration of a warrant authorising third party access will be no shorter than other computer access warrants (six months).

The Explanatory Memorandum provides no justification for why these restrictions have not been replicated in the proposed amendments in accordance with the PJCIS’s recommendation. Several submitters to the PJCIS inquiry have called for the threshold to be increased in line with that which applies to B-party warrants.

**Disruption of target and third party computers**

Section 25 provides for the issue of search warrants. Subsection 25(6) prohibits ASIO from doing anything that interferes with, interrupts or obstructs the lawful use of computers and other electronic equipment by persons who are not targets, or that causes those persons any loss or damage. The PJCIS recognised the difficulties posed by this absolute prohibition (which could, for instance, prevent execution of a warrant where doing so would temporarily slow a computer’s operation). Recommendation 21 of the 2013 PJCIS Report was that:

> .. the Government give further consideration to amending the warrant provisions in the *Australian Security Intelligence Organisation Act 1979* to enable the disruption of a target computer for the purposes of executing a computer access warrant but only to the extent of a demonstrated necessity. The Committee further recommends that the Government pay particular regard to the concerns raised by the Inspector-General of Intelligence and Security.

The IGIS had supported amendments, but considered it essential that any disruption allowed must be clearly justified, balance the potential consequences of interference to individuals with the threat to security and be subject to appropriate review and oversight.
Item 12 of Schedule 2 will repeal and replace subsection 25(6) to provide that ASIO is not authorised to add, delete or alter data, or do any other thing likely to:

- materially interfere with, interrupt or obstruct the lawful use by other persons of computers and other electronic equipment found on a search premises, unless it is necessary to do one or more of the things authorised under the warrant or

- cause any other material loss or damage to other persons using the equipment.

That is, immaterial interference would be permitted and material interference ‘necessary’ to execute the warrant would also be permitted. There is no indication of how necessity is to be assessed and no specific requirement for the degree of interference to be proportional to the relevant security threat. Several submitters to the PJCIS’s inquiry into the Bill have questioned the authorisation of material interference and called for greater clarity around what constitutes immaterial as opposed to material damage.56 The IGIS stated that it would assist its oversight functions if ASIO were required, in its reports to the Attorney-General under section 34 of the ASIO Act, to ‘provide advice on the extent to which there was any interference, interruption, obstruction or loss or damage to a computer or a communication in transit that occurred as a result of actions under the warrant’.57

Item 25 will repeal and replace subsection 25A(5) to make an equivalent amendment to section 25A in relation to computer access warrants.

Issues: disruption of third party computers and communications

Due to the amendment made by item 23 to enable use of a third party computer or communication to execute a computer access warrant, the amendment that will be made by item 25 has broader application than that made by item 12. It will mean that ASIO will be authorised to materially interfere with a third party’s computer or communication where necessary to do one or more of the things authorised under the warrant. This is another instance where provisions drafted to implement different recommendations of the 2013 PJCIS report appear, when taken together, to have exceeded what the PJCIS intended. Consideration should be given to whether disruption of third-party computers and communications should be subject to a higher threshold and/or restricted to that which is immaterial.

Use of surveillance devices

Sections 26–26C of the ASIO Act govern ASIO’s use of ‘listening devices’ (currently defined to include what would be more properly characterised as an optical surveillance device) and tracking devices, including the thresholds for the issue of warrants, situations in which warrants are not required and installation, maintenance and retrieval of devices.

The Government discussion paper prepared for the purposes of the PJCIS’s 2012 inquiry (Government Discussion Paper) explained that the ASIO Act provisions had not been updated to mirror those in the Surveillance Devices Act 2004 (SD Act), which governs use of electronic surveillance by law enforcement agencies. It stated:

In practice, this acts as an impediment to effective cooperation and collaboration with law enforcement partner agencies. For example, the differences in scope and terminology between the ASIO Act and the Surveillance Devices Act limit actions which can be taken by each agency in working with partner agencies. Aligning the surveillance device provisions in the ASIO Act with the more modern Surveillance Devices Act could assist in overcoming these impediments to cooperation.58

Following consideration of the matter, the 2013 PJCIS Report recommended the ASIO Act be amended to modernise the warrant provisions and align provisions relating to surveillance devices, particularly optical devices, with those in the SD Act.59 Items 5–7 and item 29 of Schedule 2 will implement this recommendation.

---

57. IGIS submission, op. cit., p. 10.
Section 22 of the ASIO Act contains definitions the purposes of Division 2 of Part III. Items 5–7 will amend section 22 to insert several definitions for the purposes of the proposed Subdivision D (use of surveillance devices) inserted by item 29. Key definitions include the following:

- **device** includes instrument, apparatus and equipment.

- **listening device** means any device capable of being used, whether alone or in conjunction with any other device, to overhear, record, monitor or listen to sounds, signals or a conversation, or words spoken to or by any person in conversation, but does not include a hearing aid or similar device used by a person with impaired hearing to overcome that impairment and permit that person to hear only sounds ordinarily audible to the human ear.

- **optical surveillance device** means any device capable of being used, whether alone or in conjunction with any other device, to record visually or observe an activity, but does not include spectacles, contact lenses or a similar device used by a person with impaired sight to overcome that impairment.

- **surveillance device** means:
  (a) a listening device, an optical surveillance device or a tracking device; or
  (b) a device that is a combination of any 2 or more of the devices referred to in paragraph (a) or (c); or
  (c) a device of a kind prescribed by regulation for the purposes of this paragraph.

- **tracking device** means a device or substance that, when installed in or on an object, enables a person to track the object or a person using or wearing the object.

Item 29 will repeal sections 26–26C of the ASIO Act and replace them with proposed Subdivision D to bring provisions governing use of surveillance devices by ASIO into closer alignment with the SD Act. The proposed provisions are largely modelled on those in the SD Act but retain some of the features of the existing provisions, in particular:

- warrants for the use of surveillance devices will continue to be issued by the Minister (see proposed subsection 26(1))
- the thresholds that currently apply for the issue of warrants under subsections 26(3) and 26B(2) in relation to persons, subsection 26(4) in relation to premises and subsection 26C(2) in relation to objects will continue to apply under proposed subsection 26(3). Broadly, the Minister must be satisfied that:
  - the person to which the warrant, premises or object relates is engaged in, or reasonably suspected of being engaged in, or of being likely to engage in, activities prejudicial to security
  - the use of a surveillance device in relation to the person, premises or object will, or is likely to, assist ASIO in carrying out its function of obtaining intelligence relevant to security
- warrants will continue to provide authorisation for the use of surveillance devices on third party premises from which a person of interest may be listened to, recorded, observed or monitored (current subsections 26(3) and (4) and proposed paragraphs 26B(1)(b) and 26B(2)(a))
- ASIO will continue to be authorised to recover surveillance devices without requiring a separate retrieval warrant (current subsections 26(6A), 26B(7), 26C(7) and 27A(3A) and proposed subsections 26B(5) and 27A(3A))
- warrants will continue to remain in force for up to six months (current subsections 26(6), 26B(5), 26C(5) and 27A(3) and proposed subsection 26A(3) and subsection 27A(3) as amended by the Bill)
- ASIO will continue to be authorised to install, use or maintain a tracking device without a warrant:
  - for the purposes of tracking a person, where the person consents to the installation, use or maintenance and
  - for the purposes of tracking an object, where the person using the object consents to the installation, use or maintenance (current paragraph 26A(2)(a) and proposed section 26E) and
• ASIO will continue not to be authorised to use ‘data surveillance devices’ (available to law enforcement agencies under the SD Act). 60

Several additional modifications have also been made, in particular:

• proposed paragraphs 26A(1)(c) and 26B(5)(j) will specify that force necessary and reasonable to do the things authorised by a warrant and authorised in the context of retrieval of a surveillance device respectively, may be used against both persons and things—this is consistent with amendments to other types of warrants made by items 13, 14, 26, 27 and 36 of Schedule 2 (see ‘Other amendments to warrant provisions’ under ‘Other provisions’ below)

• proposed paragraphs 26B(2)(c) and 3(d) will authorise entry of third party premises for the purposes of gaining entry to or exiting premises specified in a warrant—this is consistent with amendments to other types of warrants made by items 10 and 19 in accordance with Recommendation 35 of the 2013 PJCIS Report (see ‘Other amendments to warrant provisions’ below) and

• proposed paragraphs 26B(4)(c) and 5(e) will authorise replacement of an object with an equivalent object for the purpose of installation, maintenance or retrieval of the surveillance device or any associated enhancement equipment.

As with a warrant issued under section 10 of the SD Act, a surveillance device warrant issued under proposed section 26 may authorise the use of more than one surveillance device and more than one surveillance device of any kind. In addition, a single warrant may be issued in relation to one or more of the following: a particular person, particular premises and/or an object or class of object, but the separate thresholds that apply to each must still be met.

Proposed sections 26C, 26D and 26E will allow ASIO employees and ASIO affiliates to use listening devices, optical surveillance devices and tracking devices without a warrant in certain circumstances, consistent with equivalent provisions in the SD Act and existing section 26A of the ASIO Act. Proposed subsection 26F will allow the Director-General or a delegate to determine in writing that those sections do not apply to a specified ASIO affiliate or a specified class of ASIO affiliates.

Section 27A provides for the issue of foreign intelligence warrants authorising powers that mirror those available in relation to security intelligence under other provisions of Division 2 of Part III of the ASIO Act. Items 34, 35, and 38–40 will make consequential amendments to section 27A for consistency with proposed Subdivision D.

Proposed section 29A, to be inserted by item 44 of Schedule 2, will allow variations to warrants issued under Division 2 of Part III of the ASIO Act (except under section 29, which relates to emergency warrants issued by the Director-General), including surveillance devices issued under proposed section 26.

Issue: adequacy of accountability and reporting requirements

Section 34 of the ASIO Act requires that the Director-General provide a written report to the Attorney-General for each warrant issued under Division 2 of Part III on the extent to which the actions it assisted ASIO in carrying out its functions. This will continue to apply to surveillance device warrants issued under the ASIO Act. The SD Act, which the surveillance device provisions in the ASIO Act will more closely resemble as a result of the Bill, contains much more detailed reporting and record keeping requirements, including:

• under section 49, detailed reports must be made to the Minister on each warrant or authorisation

• under section 50, annual reports must be provided to the Minister with statistical information on the numbers of different warrants and authorisations applied for and granted, which the Minister must table in Parliament

• under sections 51 and 52, particular records must be kept about warrants, authorisations and applications and

• under section 53, a register of warrants and authorisations must be kept that contains particular details.

60. The definition of ‘surveillance device’ in the SD Act includes a ‘data surveillance device’ (‘any device or program capable of being used to record or monitor the input of information into, or the output of information from, a computer, but does not include an optical surveillance device’): SD Act, op. cit., section 6. The proposed definition to be inserted into the ASIO Act does not. There is, however, provision for other types of devices to be included in regulations for the purposes of proposed paragraph (c) of the definition of surveillance device.
The LCA submitted that equivalent reporting and record keeping requirements should apply to ASIO for its use of surveillance devices. The IGIS indicated that the proposed amendments in item 29 would make effective oversight of ASIO’s use of surveillance devices more challenging. It stated that reporting on use of surveillance devices without a warrant would assist with oversight, but that ‘the risk of unreasonable invasion of privacy might not justify the additional compliance cost’.

**Identified person warrants**

The Government Discussion Paper briefly outlined potential amendments to enable ASIO to apply for a single warrant to authorise the use of multiple powers against a particular target:

In approximately one third of cases, more than one ASIO Act warrant type is sought against a particular target. Under the current provisions, this requires the preparation of multiple applications, each re-casting the available intelligence case to emphasise the relevant facts and grounds to satisfy the different legislative requirements of the various warrant types, which is administratively burdensome.

The same outcome could be achieved with greater efficiency and with the same accountability by enabling ASIO to apply for a single warrant covering all ASIO Act warrant powers where the relevant legislative thresholds are satisfied.

The PJCIS and submitters to its 2012 inquiry had some reservations about the proposal. The PJCIS noted AGD’s assurance that the proposed warrants would not provide ‘blanket authority’ for ASIO powers, and was ultimately persuaded by classified evidence to give in principle support for the proposal, but believed it required further consideration. It recommended that ‘should the Government proceed’ with the proposal:

... further consideration be given to the factors that would enable ASIO to request a single warrant specifying multiple powers against a single target. The thresholds, duration, accountability mechanisms and oversight arrangements for such warrants should not be lower than other existing ASIO warrants.

**Item 41** will insert proposed Subdivision G (proposed sections 27C–27J) into Division 2 of Part III of the ASIO Act to provide for the issue of identified person warrants. Under the proposed provisions, ASIO will be able to seek a single ‘identified person warrant’ from the Minister that provides conditional approval for ASIO to exercise one or more of the powers currently available under a warrant issued under Division 2 of Part III, except for a foreign intelligence warrant (section 27A) or an emergency warrant (section 29). Authorisations may then be given by the Minister or the Director-General for the exercise of a power that has been conditionally approved. The powers conditionally approved may not actually be exercised unless and until such an authorisation is made.

**Warrants**

Under proposed subsection 27C(2), the Minister may only issue an identified person warrant in relation to a person that has been requested by the Director-General if she or he is satisfied that:

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

(b) the issuing of the warrant in relation to the person will, or is likely to, substantially assist the collection of intelligence relevant to security.

The second part of this test is somewhat lower than that which applies for the issue of search warrants under section 25 and computer access warrants under section 25A, which require the Minister to be satisfied that ‘there are reasonable grounds for believing the exercise of powers will substantially assist the collection of intelligence ... in respect of a matter... that is important in relation to security’. However, it is somewhat higher than those that apply under proposed section 26 (surveillance devices) and existing sections 27 (postal articles)

---

62. IGIS submission, p. 12.
and 27AA (delivery service articles), which require the Minister to be satisfied that the exercise of powers ‘will, or is likely to, assist’ in obtaining intelligence relevant to security.

Under proposed subsection 27C(3), the warrant must give conditional approval for ASIO to do one or more of the following:

- access records or other things in or on premises
- access data held in computers
- use one or more kinds of surveillance devices
- access postal articles that are in the course of post and
- access articles that are being delivered by a delivery service provider.

It must also be signed by the Minister and identify the person in relation to whom the warrant is issued by name if known, or otherwise by including details sufficient to identify the person.

Separate tests must be met for the subsequent making of an authorisation for ASIO to do a thing that is conditionally approved. However, authorisations may be made by the Director-General, and there are no additional tests that must be met at the warrant stage in order for conditional approval to be given for the exercise of particular powers. For instance, the Minister is not explicitly required to be satisfied that conditional approval of a particular power is appropriate in the particular circumstances.

Proposed subsection 27C(4) will provide that the warrant must specify how long it remains in force, up to a limit of six months. This is the same limit that applies to specific warrants authorising the above powers issued under sections 25A (computer access warrants), 27 (postal articles), 27AA (delivery service articles) and proposed section 26A (surveillance devices). Search warrants issued under section 25 are limited to 90 days duration. This discrepancy will be addressed by proposed subsection 27J(5), which will provide that a search authorisation given under an identified person warrant may only remain in force for up to 90 days. Proposed subsection 27C(5) will clarify that proposed subsection 27C(4) does not prevent the issue of a further warrant.

Proposed subsection 27C(6) will provide that the warrant is subject to any restrictions or conditions specified in it.

**Authorisations**

Proposed sections 27D–27H will allow the Minister or the Director-General to issue authorisations to do one or more specified things in order to exercise a power for which conditional approval has been given under an identified person warrant, if he or she is satisfied on reasonable grounds that doing that thing or those things will substantially assist the collection of intelligence relevant to the prejudicial activities of the identified person. 65

A definition of ‘prejudicial activities’ will be inserted into section 22 for the purposes of Division 2 of Part III of the **ASIO Act** by item 7 of Schedule 2, as follows:

*prejudicial activities* of a person means activities prejudicial to security that the person is engaged in, or is reasonably suspected by the Director-General of being engaged in, or of being likely to engage in.

Proposed section 27D will apply where conditional approval has been given for ASIO to access records or other things in or on premises, and will enable authorisation of things relating to searches of premises (and persons at or near the premises in certain circumstances), such as entry, search, inspection and accessing data. The things that may be authorised mirror those that may be authorised under a search warrant issued under section 25 as amended by the Bill, and will be subject to equivalent restrictions.

Proposed section 27E will apply where conditional approval has been given for ASIO to access data held in computers, and will enable authorisation of things such as entry to premises, accessing data and copying data. The things that may be authorised mirror those that may be authorised under a computer access warrant issued under section 25A as amended by the Bill, and will be subject to equivalent restrictions. Items 48 and 49 of Schedule 2 will make consequential amendments to section 108 of the **TIA Act** to clarify that the general

65. The specific tests applicable to each set of powers are set out in proposed subsections 27D(3), 27E(4), 27F(3), 27G(4) and 27H(4).
prohibition on access to stored communications does not apply if access occurred in accordance with an authorisation issued under proposed section 27E of the ASIO Act.

Proposed section 27F will apply where conditional approval has been given for ASIO to use one or more kinds of surveillance devices, and will enable authorisation of things such as installation, use and maintenance of surveillance devices of the kind specified in the conditional approval to surveil the identified person’s activities or track the person, and entry to premises to install or retrieve a device. The things that may be authorised mirror those that may be authorised in proposed section 26B under a surveillance device warrant issued under proposed section 26, and will be subject to equivalent restrictions.

Proposed section 27G will apply where conditional approval has been given for ASIO to access postal articles while in the course of post, and will enable authorisation of things such as opening the articles and inspecting and making copies of the articles or their contents. The things that may be authorised mirror those that may be authorised under a postal article inspection warrant issued under section 27 as amended by the Bill, and will be subject to equivalent restrictions.

Proposed section 27H will apply where conditional approval has been given for ASIO to access articles while they are being delivered by a delivery service provider, and will enable authorisation of things such as opening the articles and inspecting and making copies of the articles or their contents. The things that may be authorised mirror those that may be authorised under a delivery article inspection warrant issued under section 27AA and will be subject to equivalent restrictions.

The things that may be authorised under the above sections mirror in each case those that may be specified under an equivalent warrant. However, the equivalent warrant provisions for all but surveillance devices only allow such things to be specified or authorised as the Minister ‘considers appropriate in the circumstances’. No such requirement will apply to things authorised to be done under proposed sections 27D-27H.

Proposed section 27J will set out general rules that apply across the different authorisation types. These include:

- under proposed subsection 27J(1), that an authorisation request may be made to the Minister by the Director-General or to the Director-General by an ASIO employee or ASIO affiliate
- under proposed subsection 27J(2), that requests must specify the facts and grounds upon which the person making the request considers the authorisation necessary (this mirrors a requirement that applies under section 28 to warrants sought under Division 2 of Part III)
- under proposed subsection 27J(3), that an authorisation must be in writing, specify the identified person warrant under which it is given, authorise the use of necessary and reasonable force against persons and things, and if entry to premises is authorised, specify when it is authorised and specify:
  - the subject premises if made under section 27D
  - the target computer if made under section 27E
  - the thing or things authorised to be done
  - any restrictions or conditions that apply to the authorisation and
  - the period during which it is in force
- under proposed subsection 27J(5), that the period during which an authorisation is in force, which must not extend beyond when the relevant warrant is in force (and if given in relation to search powers under section 27D, must not be more than 90 days) and
- under proposed subsection 27J(6), that an authorisation ceases to be in force at the earliest of:
  - when the identified person warrant under which it was issued ceases to be in force
  - when it is revoked by the Minister or the Director-General or
  - the time specified in the authorisation.

Variations to warrants issued under Division 2 of Part III of the ASIO Act

Several types of warrants may be issued by the Minister under Division 2 of Part III of the ASIO Act as amended by the Bill, namely:

- search warrants (section 25)
- computer access warrants (section 25A)
• surveillance device warrants (proposed new section 26, replacing listening and tracking device warrants under current sections 26, 26B and 26C)
• warrants to inspect postal articles (section 27)
• warrants to inspect delivery service articles (section 27AA)
• foreign intelligence warrants (section 27A) and
• identified person warrants (proposed section 27C).

There is not currently any provision for warrants to be varied in the event of a change of circumstances. Instead, a new warrant must be sought. AGD gave an example of where a variation power may be appropriate in evidence to the 2013 PJCIS inquiry:

For example, if ASIO had a computer access warrant relating to a particular computer and also entry to the premises in which that computer is located. If the person moved house unexpectedly, before entry to the premises to access the computer occurred, the ability to request a variation to amend the address could be appropriate, as the core grounds (to access data on the target computer) would not have changed.66

AGD also noted the LCA’s suggestion that a new warrant should be required where there is a significant change in circumstances, stating it was ‘envisaged that in instances where there is a significant or material change in circumstances, ASIO would apply for a new warrant, rather than seek a variation’.67

Recommendation 23 of the 2013 PJCIS Report was that the ASIO Act be amended to allow the Attorney-General to vary ASIO warrants.68 Item 44 will implement that recommendation by inserting proposed section 29A, which will allow the Attorney-General, on request, to vary a warrant of a type listed above. A variation must be in writing, and if it extends a warrant, must not extend the total period for which the warrant is in force beyond the normal limits that apply (90 days for search warrants and six months for others). A warrant may be varied more than once.

Under proposed subsection 29A(4), requests for variations will be required to specify the facts or other grounds on which the variation is sought and ‘where appropriate’, the grounds on which the Director-General suspects a person of being engaged in, or likely to engage in, activities prejudicial to security. The Explanatory Memorandum states that the only circumstance in which the latter requirement is necessary is where a request is made to vary a surveillance device warrant initially issued in relation to premises or an object so that it applies to a person.69

**Issue: lack of limitations on the nature of variations**

The Explanatory Memorandum states ‘[w]here there have been significant changes to the circumstances which applied when the original warrant was issued, a new warrant will be sought.’70 However, proposed section 29A contains nothing to ensure that this will always be the case. Further, while the Director-General is required to specify the grounds on which a variation is considered necessary, the Attorney-General is not specifically required to be satisfied of any matters before making a variation.

In contrast, the provisions enabling variations to controlled operations authorities under Part IAB of the Crimes Act specify that:

• a variation must not be made unless the authorising officer is satisfied on reasonable grounds that the variation will not authorise a significant alteration of the nature of the controlled operation (subsection 15GO(5))
• a variation may be granted in accordance with the application or subject to conditions (subsection 15GQ(1)) and

---

67. Ibid.
69. Explanatory Memorandum, p. 92.
70. Ibid.
• a variation may only be made if the authorising officer is satisfied of reasonable grounds of some of the same matters that must be met for the issue of an initial authorisation, as well as that the nature and extent of the suspected criminal activity are such as to justify the variation sought (subsection 15GQ(2)).

Adoption of the last of the above features would possibly detract from the utility of a variation as opposed to a new application. However, the inclusion of provisions replicating at least the first two features in proposed section 29A would place reasonable limits on the power to make variations without diminishing their usefulness. In his submission to the PJCIS’s inquiry into the Bill, Greg Carne suggested that an indicative list of minor variations should be written into this provision to guide assessments of minor as opposed to significant variations. This could complement an equivalent to the first of the Crimes Act features outlined above.

Evidentiary certificates

The Government Discussion Paper proposed that the ASIO Act be amended to include an evidentiary certificate regime to protect the identity of officers and sensitive capabilities involved in the execution of warrant powers; currently, protecting information that reveals sensitivities about the identity of ASIO officers and capabilities used in the course of exercising special warrant powers relies on successful public interest immunity claims or, where available, orders obtained under the National Security Information (Criminal and Civil Proceedings) Act 2004. Unlike the Telecommunications (Interception and Access Act) 1979 (TIA Act) and the Surveillance Devices Act 2004 (SD Act), there is no consistent regime to protect ASIO information, capabilities and officer identities under the ASIO Act.

The 2013 PJCIS Report endorsed the proposal in Recommendation 37, which also recommended that the Government ‘give consideration to making uniform across Commonwealth legislation provisions for the protection of certain sensitive operational capabilities from disclosure in open court.’ Item 47 will insert proposed section 34AA into the ASIO Act to implement the first part of that recommendation.

Proposed section 34AA will allow the Director-General or Deputy Director-General to issue an evidentiary certificate setting out matters relating to acts or things done by or on behalf of ASIO in relation to:
• computer access warrants and surveillance device warrants
• foreign intelligence warrants and emergency warrants, but only to the extent that the acts or things relate to computer access or surveillance device powers and
• authorisations relating to computer access and surveillance devices, including under a foreign intelligence warrant or identified person warrant.

Proposed subsection 34AA(3) will provide a non-exhaustive list of matters that may be specified in a certificate, including details of premises entered under a warrant, details of a computer used to obtain access to data and details of who exercised a particular power.

Proposed subsection 34AA(4) will provide that in a proceeding (defined in proposed subsection 34AA(5)) a certificate is to be taken as prima facie (as opposed to conclusive) evidence of the matters stated therein. This is consistent with the PJCIS recommendation and existing provisions in the TIA and SD Acts, and provides scope for the court or a defendant to challenge the matters set out in the certificate.

Issue: computer access under a search warrant

Proposed section 34AA has been drafted, and appropriately so, to confine the matters that may be specified in a certificate to technical (and specifically, technological) matters. The way this has been achieved is by limiting the matters that may be specified to powers under computer access and surveillance device provisions. However,

73. Evidentiary certificates are a means for third parties to proceedings to provide evidence to a court, generally on a formal or technical matter. Certificates are generally to be taken as prima facie evidence of the relevant matter, but in some instances are used to provide conclusive evidence. See AGD, A guide to framing Commonwealth offences, infringement notices and enforcement powers, Australian Government, Canberra, updated September 2011, pp. 54–55 (accessed 21 August 2014).
76. TIA Act, op. cit., section 18; SD Act, op. cit., section 62.
under subsection 25(5), a search warrant may also authorise use of computers and electronic equipment to access, inspect and copy data. The omission of things done under subsection 25(5) from the evidentiary certificate provisions in proposed section 34AA presents an inconsistency that is not addressed in the Explanatory Memorandum. It is not clear if this was deliberate or perhaps a drafting oversight.

Authorisation to execute ASIO warrants

Section 24 of the ASIO Act currently provides for the Director-General or approved senior position holders to approve certain people to exercise powers under provisions relating to the recovery of devices, and warrants issued under Divisions 2 and 3 of Part III of the ASIO Act. Item 8 of Schedule 2 will repeal and replace the provision so that classes of persons may be approved to exercise those powers. This amendment implements Recommendation 32 of the 2013 PJCIS Report.77

Other amendments to ASIO warrant provisions

Subsection 25(4) of the ASIO Act sets out matters the Minister may specify in a search warrant if considered relevant in the circumstances. Item 10 of Schedule 2 will insert proposed paragraph 25(4)(aa) to enable the Minister to specify entry onto ‘any premises for the purposes of gaining entry to or exiting’ the premises to which the warrant relates. The amendment relates only to entry and does not provide for the exercise of search powers in third party premises. This item, and item 19, which will make an equivalent amendment to subsection 25A(4) in relation to computer access warrants, implement Recommendation 35 of the 2013 PJCIS Report.78

In making its recommendation, the PJCIS stated it was of the view that ‘whatever amendments are made to facilitate this power should acknowledge the exceptional nature and very limited circumstances in which the power should be exercised’.79 There is no recognition in the proposed amendments or in the Explanatory Memorandum of this part of the Recommendation. For example, there is no requirement for ASIO to attempt to obtain consent from the owner of the third party premises before relying on its powers under warrant. The LCA recommended that if these amendments proceed, they should be limited to instances where:

- there is no other way to gain access to the subject premises; or

- there is a substantial risk that that [sic] without access to third-party premises the authorised officer would be detected.80

The IGIS stated that it would assist its oversight functions if ASIO were required to include, in its reports to the Attorney-General under section 34 of the ASIO Act, whether the execution of each warrant involved entry onto third-party premises, the reasons for entry, and the result.81

Paragraph 25(7)(a) requires a search warrant to authorise the use of any force necessary and reasonable for the execution of the warrant. Items 13 and 14 of Schedule 2 will replace the subheading that precedes subsection 25(7) and amend paragraph 25(7)(a) to:

- clarify that force may be used at any time during the execution of the warrant, not just on entry (as is implied by the current subheading) and

- provide that force may be used against both persons and things.

Items 26 and 27 will make equivalent amendments to section 25A (computer access warrants), and item 36 will make an equivalent amendment to section 27A (foreign intelligence warrants).

These items respond to Recommendation 36 of the 2013 PJCIS Report. The recommendation was for amendments to clarify that reasonable force may be used at any time during the execution of a warrant ‘and

---

79. Ibid., p. 128.
81. IGIS submission, op. cit., p. 11.
may only be used against property, and not persons. The amendments therefore go against the recommendation by authorising the use of force against persons.

**Issue: use of force against persons**

AGD’s submission to the PJCIS’s inquiry into the Bill justifies departing from the PJCIS’s recommendation by stating that force may need to be used against persons in some circumstances, such as where a person attempts to physically obstruct the execution of a warrant. Further, it states that any force that was not reasonable and necessary in the circumstances may attract criminal or civil liability. However, the LCA and the Muslim Legal Network remain opposed to the amendments as drafted and have suggested modifications.

The IGIS and the LCA suggested that if the use of force against persons is to be permitted in the execution of ASIO warrants, it could be explicitly restricted to police officers assisting, who already receive appropriate training, and not extended to ASIO employees and affiliates. The Director-General of ASIO indicated that while police usually assist in the execution of warrants, he considered it important for ASIO officers to be able to use force against persons on the rare occasions in which it might be necessary. The Muslim Legal Network suggested the inclusion of specific limitations on the power equivalent to those that apply under subsections 34V(2) and (3) of the ASIO Act with respect to use of force against a person taken into custody by police.

**Issue: accountability for and oversight of warrant powers in Division 2 of Part III of the ASIO Act**

Section 94 of the ASIO Act requires the Director-General to provide annual reports to the Minister as soon as practicable after 30 June each year. The reports are tabled in Parliament after any necessary exclusions have been made. Subsection 94(1) sets out matters relating to warrants issued under Division 3 of Part III of the ASIO Act that must be included in annual reports. Proposed subsection 94(2A), to be inserted by item 4 of Schedule 3 will set out (very limited) matters relating to special intelligence operations that must be included.

There is not currently a requirement to report any details in relation to warrants issued under Division 2 of Part III of the ASIO Act, nor are any such provisions proposed in the Bill. Given the various expansions to ASIO’s warrant powers proposed in the Bill, consideration should be given to requiring the provision of some non-identified information such as the number of the different warrants sought, granted and refused, in ASIO’s annual reports.

As noted in the relevant sections above, the IGIS has also suggested that ASIO be required to include several specific matters in the reports it makes to the Attorney-General under section 34 of the ASIO Act.

**Schedule 3—Special intelligence operations**

Schedule 3 will insert proposed Division 4 into Part III of the ASIO Act to provide for a ‘special intelligence operation’ (SIO) scheme under which ASIO officers and affiliates will be protected from criminal and civil liability for certain conduct engaged in for the purpose of a SIO. The enactment of such a scheme was recommended in the 2013 PJCIS Report and by the Independent National Security Legislation Monitor (INSLM) in its 2014 annual report. The Attorney-General explained the need for an SIO scheme in a recent interview as follows:

> Let us say that there is an agent who, under deep cover, penetrated a terrorist cell and was involved in conversations concerning the planning of a terrorist attack for example. Technically, that person might be guilty of the crime of criminal conspiracy or guilty of the preparation of a terrorist event. That person would be undercover and the purpose of their conduct would be to conduct an undercover operation but at least technically, the conduct

---

82. Ibid., pp. 128–30 (quote taken from p. 130).
83. AGD, Submission to Parliamentary Joint Committee on Intelligence and Security, Inquiry into the National Security Legislation Amendment Bill (No. 1) 2014 (Submission to PJCIS), July 2014, p. 17, accessed 11 August 2014.
84. LCA, op. cit., pp. 28–29; Muslim Legal Network, op. cit.
87. Muslim Legal Network, op. cit.
88. A definition of ‘ASIO affiliate’ will be inserted into the ASIO Act by item 1 of Schedule 1 of the Bill.
in which they were engaged in carrying out that operation might place them in breach of certain criminal laws. Now, we want to protect intelligence officers from exposure to liability in circumstances like that.  

The 2013 PJCIS Report specifically recommended that the scheme be subject to similar safeguards and accountability arrangements as apply to the controlled operations scheme outlined under Part IAB of the Crimes Act 1914, which applies to law enforcement agencies. The SIO scheme in the Bill is similar to the controlled operations scheme but, as outlined below, the safeguards and accountability requirements it contains are less stringent. Further, the LCA, Gilbert + Tobin, the CCLs, the Muslim Legal Network and Blueprint have questioned the need for the scheme in the first place, suggesting it would be more appropriate to continue to rely on the Commonwealth Director of Public Prosecutions’ (CDPP’s) discretion not to prosecute. When this was put to the Director-General of ASIO, he argued ‘there is, I think, a level of obligation that we owe people—people who go to very, very great risks on our behalf—that they are not going to then get beaten over the head for some minor misdemeanour or whatever conducted in the course of their business’.  

Section 4 of the ASIO Act contains definitions used throughout the Act. Item 1 of Schedule 3 will amend that section to insert several definitions for the purposes of the proposed SIO scheme, including ‘authorising officer’ and ‘special intelligence operation’, which will be defined as follows:

authorising officer means:
(a) the Director-General; or
(b) a Deputy Director-General.

special intelligence operation is an operation:
(a) in relation to which a special intelligence operation authority has been granted; and
(b) that is carried out for a purpose relevant to the performance of one or more special intelligence functions; and
(c) that may involve an ASIO employee or an ASIO affiliate in special intelligence conduct.

‘Special intelligence function’ will be defined as a function of ASIO set out in paragraphs 17(1)(a), (b), (e) or (f) of the ASIO Act. Those paragraphs relate to ASIO’s functions of obtaining, correlating and evaluating intelligence relevant to security, communicating such intelligence for purposes relevant to security, obtaining foreign intelligence in Australia and communicating it in accordance with the ASIO Act, and cooperating with and assisting intelligence, law enforcement and other government agencies with their functions.

Item 3 of Schedule 3 will insert proposed Division 4 into Part III of the ASIO Act.

Applications for and granting of authorities and variations to authorities

Proposed section 35B will allow an ASIO employee to apply to an authorising officer for an authority to conduct an SIO. Applications are to be in writing and signed by the applicant, unless he or she reasonably believes the delay associated with a written application may be prejudicial to security. Proposed subsection 35B(4) will provide that if an application is made by other means, the applicant must make a written record and give a copy of it to the relevant authorising officer as soon as practicable.

Proposed section 35C will set out the means and conditions for granting of SIO authorities. The authorising officer to whom an application is made may grant an authority to conduct an SIO either unconditionally or subject to conditions if satisfied on reasonable grounds that:

- the SIO will assist ASIO in the performance of one or more special intelligence functions
- the circumstances justify the conduct of an SIO
- any unlawful conduct involved will be limited to the maximum extent consistent with conducting an effective SIO

91. LCA, op. cit., pp. 29–31; Gilbert + Tobin, op. cit., pp. 6–7; CCLs, op. cit., pp. 8–10; Muslim Legal Network, op. cit.; Blueprint for Free Speech, op. cit., p. 4.
92. D Irvine (Director-General of ASIO), op. cit., p. 22.
• the SIO will not be conducted in such a way as to induce a person who otherwise would not have done so, to commit a crime
• the conduct involved in the SIO will not cause the death of, of serious injury to, any person; involve the commission of a sexual offence against any person; or result in significant loss of, or serious damage to, property.

These parameters are similar to those in the equivalent *Crimes Act* provision (section 15GI), though necessarily less specific. However, that section also requires the authorising officer to be satisfied that the conduct involved in a controlled operation will not seriously endanger the health or safety of any person (paragraph 15GI(2)(g)(i)). The Explanatory Memorandum does not explain why this requirement has not been replicated.

Unlike the equivalent *Crimes Act* provision (section 15GH), **proposed section 35B** does not require certain information to be provided in the application. However, the matters of which the authorising officer must be satisfied under **proposed section 35C** would set the parameters for what must be provided in an application.

Under **proposed subsection 35C(4)**, an SIO authority will need to be in writing and signed by the authorising officer, unless he or she reasonably believes the delay associated with a written authority may be prejudicial to security. **Proposed subsection 35C(5)** will provide that if an authority is granted by other means, the authorising officer must issue a written record that complies with **proposed section 35D** within seven days.

Under **proposed section 35D**, SIO authorities will be required to contain particular information, including the persons authorised to engage in ‘special intelligence conduct’ (conduct for which the person would be subject to civil or criminal liability but for **proposed section 35K**), a general description of the nature of such conduct and the period of effect of the SIO authority. **Proposed paragraph 35D(1)(d)** will provide that the period of effect of an SIO authority must not exceed 12 months. Neither the PJCIS nor the INSLM recommended a particular time limit for SIOs. However, the 2013 PJCIS Report noted the 12 month period suggested in the Government Discussion Paper without adverse comment.93 The initial period of effect of controlled operations authorities granted by authorising officers under the *Crimes Act* must not exceed three months, after which extensions may be granted by certain members of the Administrative Appeals Tribunal (extensions of up to three months at a time may be granted up to a total duration of 24 months).94 The LCA, Gilbert + Tobin, the CCLs and Blueprint have submitted that the initial duration of SIOs should be reduced to three or six months.95 Similarly, the same organisations suggest that authorities should be granted, or at least varied (see **proposed section 35F** below) by an independent, external body.96

Under **proposed section 35E**, an SIO will come into force at the time it is granted and will have effect for the period specified under paragraph 35D(1)(d) unless it is cancelled (under **proposed section 35G**) or the period of effect extended (under **proposed section 35F**).

**Proposed section 35F** will allow an authorising officer to vary an SIO authority at his or her own initiative or on application by an ASIO employee. As with applications for and grants of authorities, applications and variations must be in writing unless there is a reasonable belief that the associated delay may be prejudicial to security, in which case written records must be made soon afterwards (**proposed subsections 35F(2), (3), (6) and (7)**). **Proposed subsection 35F(8)** will provide that an authority may be varied more than once.

**Issue: lack of appropriate limits on variations**

**Proposed subsection 35F(4)** provides that an authorising officer must not vary an SIO authorisation unless he or she is satisfied on reasonable grounds that the SIO as varied will assist ASIO in the performance of one or more special intelligence functions, and considers it appropriate to make the variation. **Proposed subsection 35F(5)** provides that any variation must not extend the authority beyond a total period of effect of 12 months.

The equivalent *Crimes Act* provision (section 15GO) specifies what a variation may do (including authorising additional persons to engage in controlled conduct, authorising existing participants to engage in additional or alternative conduct and providing that specified persons are no longer authorised to engage in controlled conduct).

---

94. *Crimes Act*, op. cit., paragraph 15GK(1)(h), subsection 15GQ(4) and Subdivision C, Division 2 of Part IAB.
95. LCA, op. cit., p. 36; Gilbert + Tobin, op. cit., p. 7; CCLs, op. cit., p. 10; Blueprint for Free Speech, op. cit., p. 6.
96. LCA, op. cit., p. 39; Gilbert + Tobin, op. cit., pp. 7–8; CCLs, op. cit., p. 10; Blueprint for Free Speech, op. cit., p. 6.
conduct) (subsection 15GO(2)). It also prohibits an authorising officer from granting a variation unless he or she is satisfied on reasonable grounds that to do so will not authorise a significant alteration of the nature of the particular operation (subsection 15GO(5)). These restrictions, particularly the latter, are important safeguards against variations being used to authorise entirely new operations where fresh authorities should instead be sought, and should be replicated in the proposed SIO scheme.

**Effect of SIO authorities**

**Proposed subsection 35H(1)** will explicitly set out that an SIO authority ‘authorises each person who is identified in the special intelligence operation authority to engage in the special intelligence conduct specified in the special intelligence operation authority in respect of that person’. **Proposed subsection 35H(2)** notes the limitations that may be imposed on the time for which the authorisation is in effect in relation to a particular person.

**Proposed section 35K** will set the parameters for the protection from civil and criminal liability that applies to participants in authorised SIOs. **Proposed subsection 35K(1)** will provide that a participant in an SIO is not subject to any civil or criminal liability for, or in relation to, conduct if:

- he or she engages in the conduct in the course of, and for the purposes of, the SIO
- he or she engages in the conduct in accordance with the SIO authority
- he or she is identified in the SIO as a person authorised to engage in special intelligence conduct for the purposes of the SIO
- the conduct does not involve intentionally inducing another person to commit an offence against Australian law that they would not otherwise have intended to commit
- the conduct does not involve the participant engaging in conduct that causes the death of, or serious injury to, any person; involves the commission of a sexual offence against any person; or causes significant loss of, or serious damage to, property and
- any requirements specified in a Ministerial determination made under **proposed subsection 35K(2)** have been met.

The protection from liability does not apply if a participant acts outside the parameters of an SIO granted under section 35C.

Part of the protection provided is somewhat broader than that provided under the controlled operations scheme. In particular, under paragraphs 15HA(2)(d) and 15HB(2)(d) of the Crimes Act protection is not provided if a participant’s conduct is likely to cause the death of, or serious injury to, any person or involve the commission of a sexual offence against any person. Under **proposed paragraph 35K(1)(e)**, protection is only excluded if the participant’s conduct actually causes death or serious injury, or the commission of a sexual offence. The reason for this discrepancy is unclear.

**Proposed section 35N** will provide protection from criminal responsibility for certain ancillary conduct related to special intelligence conduct engaged in by a participant in an SIO, equivalent to that provided for in relation to controlled operations under section 15HE of the Crimes Act.

**Proposed section 35L** will clarify that the proposed Division does not permit ASIO to engage in a particular act or obtain particular information outside the normal warrant or approval process that applies. In particular, where ASIO requires a warrant under the ASIO Act or Part 2-2 of the TIA Act (interception warrants), or is required to comply with Division 3 of Part 4-1 of the TIA Act (permitted access to telecommunications data), an SIO authority cannot displace such a requirement.

**Offences for unauthorised disclosure of information**

**Proposed section 35P** contains two offences for unauthorised disclosure of information relating to an SIO.

Under **proposed subsection 35P(1)** a person will commit an offence if he or she:

- discloses information and
• the information relates to an SIO.\(^97\)

The maximum penalty for the offence will be imprisonment for five years. The Explanatory Memorandum states that the Government considers this penalty appropriate on the basis of:
• parity with offences for disclosing information about a questioning warrant or questioning and detention warrant in section 34ZS of the ASIO Act and\(^98\)
• comparison to the three year penalty for the proposed offences of unauthorised dealing with ASIO records and unauthorised recording of ASIO information to be inserted by item 4 of Schedule 6 of the Bill (proposed sections 18A and 18B).\(^99\)

The maximum penalty for the corresponding offence in the Crimes Act (subsection 15HK(1)) is imprisonment for two years. This discrepancy is not addressed in the Explanatory Memorandum, but the consequences of unauthorised disclosures about SIOs are potentially more significant than such disclosures about controlled operations, particularly in relation to disclosures about ASIO’s capabilities.

Under proposed subsection 35P(2) a person will commit an offence if he or she:
• discloses information and
• the information relates to an SIO and\(^100\)
• either:
  – the person intends to endanger the health or safety of any person or prejudice the effective conduct of an SIO or
  – the person is reckless as to whether the disclosure of the information will endanger the health or safety of any person or prejudice the effective conduct of an SIO.

The maximum penalty for the offence will be imprisonment for ten years. This penalty is the same that applies to the corresponding offence in the Crimes Act (subsection 15HL(1)) and that which will apply to the offence of unauthorised communication of ASIO information in subsection 18(2) of the ASIO Act, as amended by item 1 of Schedule 6 of the Bill (which will amend the penalty from two to ten years).

Proposed subsection 35P(3) provides for a defence to the above offences that apply if the disclosure was:
• in connection with the administration or execution of Division 4 of Part III of the ASIO Act
• for the purposes of legal proceedings arising out of or otherwise related to that Division, or any report of such proceedings
• in accordance with a requirement imposed by law or
• in connection with the performance of functions or duties, or the exercise of powers, of ASIO.

A defendant bears an evidential burden in relation to such a defence, in accordance with subsection 13.3(3) of the Criminal Code.

Defendants will also have access to the general defences set out in Part 2.3 of the Criminal Code.\(^101\)

Proposed subsection 35P(4) applies the broadest level of extended geographical jurisdiction (category D) to the offences in the section, such that the offences apply whether or not the relevant conduct or a result of that conduct occurs in Australia.\(^102\)

---

97. Automatic fault elements will apply in accordance with section 5.6 of the Criminal Code Act 1995 (Criminal Code, accessed 11 August 2014). This will require the prosecution to prove that the person intentionally disclosed the information and was reckless as to whether the information related to an SIO.

98. The INSLM recommended in 2012 that the penalties for the offences in section 34ZS be reduced from five to two years: Declassified annual report 2011–12, INSLM, Canberra, 20 December 2012, pp. 80–83 (recommendations IV/4 and IV/5), accessed 29 July 2014.

99. Explanatory Memorandum, p. 113. See pages 34–35 of this Digest for an overview of the proposed sections 18A and 18B.

100. Automatic fault elements will apply to the matters in these first two dot points in accordance with section 5.6 of the Criminal Code. This will require the prosecution to prove that the person intentionally disclosed the information and was reckless as to whether the information related to an SIO.

101. There are a number of defences outlined in the Criminal Code that apply generally across Commonwealth law, including mistake or ignorance of fact under section 9.1.
**Issue: scope of offences**

The offences have been the most controversial aspect of the proposed SIO scheme. Two main concerns have been raised—that the offences do not contain exceptions for public interest disclosures or whistleblowing by ASIO employees, and that they apply to any person and would therefore capture disclosures by, for example, journalists.  

A *Sydney Morning Herald* article and the LCA’s submission to the PJCIS’s inquiry into the Bill point out that the corresponding *Crimes Act* offences include exceptions for disclosures of misconduct to the Commonwealth Ombudsman or the Law Enforcement Integrity Commissioner for which the proposed offences contain no equivalent. However, the *Crimes Act* provisions were enacted prior to the *Public Interest Disclosure Act 2013* (*PID Act*), which introduced a statutory scheme to support reporting of wrongdoing by public officials in the Commonwealth public sector. Under the *PID Act*, an ASIO officer would be protected from civil, criminal and administrative liability for making a ‘public interest disclosure’ in relation to an SIO either internally or to the IGIS (though not to anyone else). Types of ‘disclosable conduct’ include, for example, conduct that contravenes an Australian law, involves corruption or abuse of public office, is an abuse of trust, or constitutes maladministration.

While the *PID Act* goes some way to addressing concerns about whistleblowing, neither it nor the provisions in the Bill would provide any exception to the proposed offences for journalists. Some of the concerns raised on this aspect fail to take account of the application of fault elements to the offences under section 5.6 of the Criminal Code. For example, the Joint media organisations submission states that journalists could be convicted for disclosing information that they had ‘no idea’ or were ‘not aware of’ being related to an SIO. This is not the case. For both offences, the prosecution will need to prove that:

- the person intentionally disclosed information and
- the person was reckless as to whether that information related to an SIO.

In order to make out recklessness with respect to the circumstance that information related to an SIO, the prosecution will need to establish that:

- the person was aware of a substantial risk that the information related to an SIO and
- having regard to the circumstances known to him or her, it is unjustifiable to take the risk that it was.

However, there may be instances where a person knows or is aware of a substantial risk that information relates to an SIO, but where he or she considers that there is considerable public interest in making the disclosure—for example, in reporting on misconduct or abuse of powers. The CDPP has the discretion not to prosecute an offence if it considers it is not in the public interest to do so. However, an exception or defence to the proposed offences—at least to the basic offence, which does not require any intended harm—would provide

---

104. D Wroe, op. cit.; LCA, op. cit., pp. 42–43; *Crimes Act*, op. cit., subsections 15H(3) and 15HL(3).  
106. Ibid., sections 10 and 26. ASIO employees may make disclosures to other agencies, bodies and individuals in certain circumstances, but only if the disclosure does not contain ‘intelligence information’ as defined by section 41 of the *PID Act*. Under subparagraph 41(1)(b)(iii), intelligence information includes information that is about, or might reveal ‘operations that have been, are being, or are proposed to be, undertaken by an intelligence agency’. For a good explanation of the very restricted application of the *PID Act* to intelligence agencies in general and in the context of the proposed offences, see AJ Brown, *Submission to Parliamentary Joint Committee on Intelligence and Security, Inquiry into the National Security Legislation Amendment Bill (No. 1) 2014*, 6 August 2014, accessed 22 August 2014.  
107. Ibid., section 29.  
108. Joint media organisations, op. cit., p. 3.  
much clearer protection for public interest disclosures. The Shadow Attorney-General, Mark Dreyfus, has been quoted as stating that if criminalising journalism was the effect of the provisions, ‘the government will need to make changes to remove that consequence’. 111

Other concerns raised in relation to the breadth of the offences are the lack of defences for information already publicly available (as is proposed for offences that will be amended or inserted by Schedule 6 of the Bill) and for seeking legal advice on a potential disclosure (as per the equivalent Crimes Act offences). 112

**Reporting requirements**

Proposed subsection 35Q will require the Director-General of ASIO to report in writing to the Minister and the IGIS on each SIO for each six-month period for which an authority has effect. The report must include information on the extent to which the SIO has assisted ASIO in the performance of one or more of its special intelligence functions during the period to which the report relates.

Item 4 of Schedule 3 will amend the ASIO Act by inserting proposed subsection 94(2A) to require the Director-General to include, in the annual reports provided to the Minister and tabled in Parliament:

- the total number of applications for SIO authorities made during the year and
- the total number of SIO authorities granted during the year.

**Issue: adequacy of accountability and reporting requirements**

As noted above, the PJCIS specifically recommended that the SIO scheme be subject to similar safeguards and accountability arrangements as apply to the controlled operations scheme in the Crimes Act. In addition to matters already detailed, the Bill falls short of this recommendation in several respects, in particular:

- it does not require a particular officer to be identified as having operational responsibility for an SIO
- far less detail is required in annual reporting
- there are no specific provisions addressing the keeping of adequate records and
- there is no specific obligation on the IGIS to inspect and report on records relating to SIOs.

Under section 15GK of the Crimes Act, a controlled operation authority must identify the ‘principal law enforcement officer’ responsible for the conduct of the operation. 113 Proposed section 35D contains no equivalent requirement.

Section 15HN of the Crimes Act requires annual reports to be made to the Minister and the Ombudsman detailing not just the numbers of applications made and granted, but also a range of other information, including:

- the number of applications for authorities that were refused
- the number of applications for variations that were granted
- the number of applications for variations that were refused
- for each authority in force at any time in the relevant period:
  - the date on which the operation commenced
  - if the operation ceased during that period, the date of cessation and the outcomes of the operation, otherwise the date it is due to cease
- for authorities for which applications for variations were made, the dates on which they were sought and either refused or granted
- the nature of criminal activities against which the operations were directed
- the identity of each person targeted under the operations
- the nature of conduct engaged in for the purposes of the operations

111. M Dreyfus, quoted in D Wroe, op. cit.
112. D Leyonhjelm submission, op. cit., p. 3; LCA, op. cit., p. 43.
113. Crimes Act, op. cit., sections 15GK and 15GC.
• details of any loss or serious damage to property that occurred in the course of, or as a direct result of, the operations
• details of any personal injuries that occurred in the course of, or as a direct result of, the operations and
• the number of authorities that were cancelled or expired.\(^\text{114}\)

The numbers of urgent as opposed to formal applications, authorities and variations must also be identified separately where relevant in relation to the matters above.

There are also provisions to ensure that:
• a person may be identified in a report by an assumed name or number instead of their actual name in certain circumstances
• the report does not disclose information that identifies any person involved in an operation, or would be likely to lead to such a person being identified and
• information that could reasonably be expected to endanger a person’s safety, prejudice an investigation or prosecution or compromise an agency’s operational activities or methodologies is excluded from the report before it is tabled.\(^\text{115}\)

While some of the requirements set out above may need to be modified or omitted to suit the different context of SIOs, there is no apparent reason why others, such as total numbers relating to applications for authorities and variations and associated grants and refusals, could not be exactly replicated in relation to SIOs.

The Crimes Act also contains specific obligations relating to records that must be kept and details to be maintained on a general register. It is not clear why these have not been replicated in Schedule 3 of the Bill. At a public hearing into the Bill the Office of the IGIS indicated that effective oversight of the scheme would be reliant on ASIO’s record keeping:

... what we are looking at with oversight ... is not whether it assisted ASIO; it is more whether the conduct under that operation has been appropriate, proportionate and reasonable and what actually has gone on. So the current reporting requirement would not be the information we would need; we would need a lot more. If there is no express reporting requirement, we would rely heavily on ASIO’s ability to keep appropriate records.\(^\text{116}\)

Finally, the Crimes Act specifically requires the Ombudsman to inspect records relating to controlled operations at least once every 12 months and to report annually on the results of such inspections.\(^\text{117}\) The IGIS has general powers under the Inspector-General of Intelligence and Security Act 1986 to oversee ASIO’s compliance with laws and inspect its records, and is required to comment on any inspections in its annual reports.\(^\text{118}\) However, there are no existing provisions and none in the Bill that would require regular inspections of records relating to SIOs.

**Schedule 4—ASIO co-operation and information sharing**

Schedule 4 of the Bill comprises the Government’s response to recommendations 33 and 34 of the 2013 PJCIS Report.

Section 92 of the ASIO Act contains two offences relating to the unauthorised publication of the identity of a current or former ASIO officer, employee or agent. The maximum penalty for the offences is imprisonment for one year.

Section 18 of the ASIO Act sets parameters around when ASIO intelligence or information may be communicated outside the agency. Under subsection 18(3), information that relates, or appears to relate, to commission of a ‘serious crime’ may be passed on to law enforcement authorities if other requirements are met. As ‘serious

---

114. **Crimes Act**, op. cit., sections 15HM and 15HN.
115. Ibid., subsections 15HM(2C), and 15HN(2)–(4).
116. J Blight (Assistant IGIS, Office of the IGIS), *Evidence to Parliamentary Joint Committee on Intelligence and Security, Inquiry into the National Security Legislation Amendment Bill (No. 1) 2014*, 15 August 2014, p. 6, accessed 22 August 2014. See also the IGIS’s submission to the PJCIS’s inquiry into the Bill.
117. **Crimes Act**, op. cit., sections 15HO and 15HS.
crime’ is defined in section 4 of the ASIO Act as an offence punishable by imprisonment exceeding 12 months, ASIO has been precluded from sharing information in relation to an offence or possible offence against section 92. Recommendation 34 of the 2013 PJCIS Report was for legislative amendments to enable ASIO to refer breaches of section 92 to a law enforcement agency. **Items 1 to 3 of Schedule 4** will amend subsection 18(3) accordingly.

Section 19 of the **ASIO Act** provides authority for ASIO to cooperate with Commonwealth, state and territory and approved foreign authorities as far as necessary for, or conducive to, its functions, subject to any arrangements made or directions given by the Minister. The Government Discussion Paper explained that it was unclear whether section 19 might be read to imply that ASIO should not cooperate with organisations outside government. The PJCIS considered that ASIO’s cooperation with the private sector was ‘clearly necessary’ and in the public interest in light of the sector’s ownership and control of a significant portion of Australia’s critical infrastructure. Accordingly, Recommendation 33 of the 2013 PJCIS Report was for a legislative amendment to formalise ASIO’s capacity to cooperate with the private sector.

**Item 5 of Schedule 4** will insert **proposed paragraph 19(1)(d)** to expand the list of entities with which ASIO may cooperate in performing its functions to include ‘any other person or body whether within or outside Australia’. This is a very broadly cast provision. AGD’s submission to the PJCIS’s inquiry into the Bill explains that ASIO may need to cooperate with organisations incorporated outside Australia but that have a significant presence here. The submission and the Explanatory Memorandum also point out that ASIO’s cooperation under the proposed paragraph may be subject to arrangements made or directions given by the Minister in accordance with subsection 19(1) and any written guidelines issued by the Minister under section 8A of the **ASIO Act**. However, the provisions do not require the Minister to make such arrangements, or issue directions or guidelines. Nor do they require that persons or bodies be approved by the Minister as being capable of assisting ASIO to perform its functions, as is currently the case under paragraph 19(1)(c) for authorities of foreign countries. The IGIS stated that this ‘could circumvent current authorisation and oversight arrangements that are in place to ensure compliance with human rights obligations’. Consideration should be given to how cooperation under the proposed provision might be more narrowly circumscribed without unduly limiting necessary cooperation, by requiring some form of Ministerial approval, direction or guidelines.

**Schedule 5 – Activities and functions of Intelligence Services Act 2001 agencies**

The amendments made under this Schedule will outline a new function of ASIS of cooperation with ASIO in relation to the production of intelligence on Australian persons in limited circumstances outside Australia.

**Item 1** will insert a new definition into existing section 3 of the **IS Act**: 

**Operational security of ASIS** means the protection of the integrity of operations undertaken by ASIS from:

(a) interference by a foreign person or entity; or

(b) reliance on inaccurate or false information.

The functions of ASIS are outlined in section 6(1) of the **IS Act**. **Proposed subparagraph 6(1)(db)** will explicitly note the function to undertake activities in accordance with **proposed section 13B** (which will be inserted by **item 11**).

**Item 11** will insert **proposed section 13B**, implementing Recommendation 39 of the PJCIS Report, which was that during cooperative intelligence operations, common standards should apply for the authorisation of intrusive activities involving the collection of intelligence on an Australian person.

The amendment will be made to the **IS Act**, inserting:

---

121. Ibid., p. 123.
122. AGD, Submission to PJCIS, op. cit., p. 16.
123. Ibid., pp. 15–16; Explanatory Memorandum, p. 118.
124. IGIS submission, op. cit., p. 16.
13B Activities undertaken in relation to ASIO

When an activity may be undertaken in relation to ASIO

(1) Subject to 13D, ASIS may undertake an activity, or a series of activities, if:

(a) the activity or series of activities will be undertaken for the specific purpose, or for purposes which include the specific purpose, of producing intelligence on an Australian person or a class of Australian persons; and

(b) the activity or series of activities will be undertaken outside Australia; and

(c) the activity or series of activities will be undertaken to support ASIO in the performance of its functions; and

(d) either:

(i) the Director-General of Security; or
(ii) a person who is authorised under section 13C for the purposes of this subparagraph;

has, in writing, notified ASIS that ASIO requires the production of intelligence on the Australian person or class of Australian persons.

The effect of this provision will be that a Ministerial authorisation is not required, enabling ASIS and ASIO to move quickly and cooperatively in the performance of its functions. In other circumstances, ASIS will still be required to obtain Ministerial authorisations before undertaking a particularly intrusive activity overseas. Without Executive scrutiny of authorisations, it is possible that a higher number of cooperative authorisations can be issued in an efficient way, to capture accurate and useful intelligence.

Gilbert + Tobin is concerned that proposed section 13B of the IS Act would circumvent the requirement of ministerial authorisation in some circumstances, further stating it believes that ‘the current legislative arrangements strike an appropriate balance between the distinct characteristics of ASIS as a foreign intelligence agency and the need in some circumstance for it to assist ASIO to collect intelligence about Australians overseas’. 127

However, a safeguard provision will also be inserted by proposed section 13E, requiring the Director-General to be satisfied that:

(a) there are satisfactory arrangements in place to ensure that activities will be undertaken in accordance with section 13B only for the specific purpose of supporting ASIO in the performance of its functions; and

(b) there are satisfactory arrangements in place to ensure that the nature and consequences of acts done in accordance with section 13B will be reasonable, having regard to the purposes for which they are carried out.

Schedule 6 – Protection of information

Item 1 will amend the existing penalty in section 18 of the ASIO Act for the offence of unauthorised communication of information. It is an offence for a person to communicate to another person any information that has come to that person by reason of past or current ASIO employment. Communications are permissible between specified categories of ASIO employment and unauthorised communication currently has a maximum penalty of two years imprisonment. This item will amend that maximum penalty to 10 years imprisonment.

The Explanatory Memorandum states that the ‘necessity for increasing the penalty has become apparent through recent domestic and international incidents involving the unauthorised disclosure of security intelligence-related information.’ 128

Further:

127 Gilbert + Tobin, op. cit., p. 11.
128 Explanatory Memorandum, p. 30.
The amendments will also extend the application of these offences to additional agencies in the Australian Intelligence Community, being DIO and ONA to address a legislative gap in the framework for the protection of information handled and produced within the entirety of the Australian Intelligence Community.\textsuperscript{129}

The LCA notes that the ‘proposed offences or increases in penalties have not been subject to proper consultation despite having the potential for significant limitations on freedom of speech.’\textsuperscript{130}

Gilbert + Tobin submits:

... the proposed 10 year penalties for disclosing national security information would far exceed the penalties found in other legislation. Section 79 of the Crimes Act provides for a maximum of seven years imprisonment where a person discloses official secrets ‘with the intention of prejudicing the security or defence of the Commonwealth.’ This offence applies to intelligence officers and other individuals who are entrusted with classified information. It is not clear why the offences in the ASIO Act and IS Act should carry a greater maximum penalty where there is no such intention to prejudice security or defence.\textsuperscript{131}

The Explanatory Memorandum justifies this penalty increase to be proportionate to the gravity of the wrongdoing targeted by the offence. The penalty has not been revised since the ASIO Act commenced in 1979. The Government proposes that increasing the penalty to 10 years imprisonment will improve the effectiveness of the offence as a deterrent. Further, the Explanatory Memorandum states:

Given the potentially devastating consequence of the unauthorised disclosure of security intelligence-related information, it is appropriate that the maximum penalty applying to subsection 18(2) is of a sufficient magnitude to communicate clearly the gravity of the wrongdoing involved and Parliament’s strong expectation that persons to whom intelligence and national security-related information is entrusted will handle that information lawfully at all times.\textsuperscript{132}

The Explanatory Memorandum provides a lengthy justification for the increase in penalty, noting also that the proposed new penalty reflects ‘an appropriate gradation with that applying to the espionage offences in Division 91 of the Criminal Code 1995, which is 25 years’ imprisonment’.\textsuperscript{133}

An exception to the offence will be inserted by item 2, providing in proposed subsection 18(2A) that the offence does not apply to information that has already been communicated or made available to the public with the authority of the Commonwealth. The exception will not apply to disclosure in the nature of a ‘leak’.\textsuperscript{134} In this regard, Chapter 2 (subsection 13.3(3)) of the Criminal Code applies, requiring the defendant to show that the information was already otherwise available prior to his or her conduct.

AGD sought to clarify the application of the offence in Schedule 6, to address public concern that the offences were targeted at journalists:

...the offences do not target journalists; they apply broadly and there are elements of them being designed so that they will not apply to legitimate reporting of national security matters – schedule 6 in particular...[The offences] are limited to persons who are in a specified form of relationship with the intelligence agency.\textsuperscript{135}

Item 4 will insert proposed sections 18A and 18B in Part III of the ASIO Act. These will be two new offence provisions.

Proposed subsection 18A(1) will create an offence for an entrusted person’s unauthorised dealing with records. There is a lengthy explanation of the operation of the offence in the Explanatory Memorandum, at pages 134-142. The key elements of this offence to note are:

\textsuperscript{129} Ibid.
\textsuperscript{130} LCA, op. cit., p. 5.
\textsuperscript{131} Gilbert + Tobin, op. cit., p. 12.
\textsuperscript{132} Explanatory Memorandum, p. 131.
\textsuperscript{133} Ibid.
\textsuperscript{134} Ibid., p. 133.
\textsuperscript{135} J Lowe (Acting First Assistant Secretary, National Security Law and Policy Division, AGD), Evidence to Parliamentary Joint Committee on Intelligence and Security, Inquiry into the National Security Legislation Amendment (No. 1) Bill 2014, 15 August 2014, p. 10, accessed 22 August 2014.
The offence will apply to a person who is, or who has been an ‘entrusted person’ (ASIO employee, ASIO affiliate or other similarly contracted person to ASIO). The person must have been an entrusted person at the time at which he or she obtained the record.

The relevant record is a record of ASIO, or pertains to ASIO’s performance of its functions.

The unauthorised dealing in relation to a record can include (proposed subparagraphs 18A(1)(d)(i)-(v)) copying the record, transcribing the record, retaining the record, removing the record or dealing with the record in any other manner, in an unauthorised manner (proposed paragraph 18A(1)(e)).

The exception to making out the offence is that the record is lawfully available (proposed subsection 18A(2)).

The maximum penalty will be three years’ imprisonment.

Proposed section 18B also creates a new offence for an entrusted person who makes a record of information or a matter, outside of the person’s employment or agreement with ASIO. The penalty for this offence is three years’ imprisonment. An exception to the offence can be found under proposed subsection 18B(2) where the offence does not apply if the information or matter has already been made available to the public with the authority of the Commonwealth. Proposed section 18B is also noted as an alternative verdict for charges made under proposed subsection 18A(1).

Extended geographical jurisdiction – category D – will apply to these offences. The Explanatory Memorandum justifies this extension by noting the unacceptable risk of significant harm to Australia’s national interests should any entrusted person engage in unauthorised conduct:

Category D extended geographical jurisdiction is necessary to ensure the effective operation of the offences in subsection 18(2) and sections 18A and 18B. Entrusted persons into whose possession records have come, or into whose knowledge information has come, may potentially include non-Australian persons (such as foreign officials) who are based outside Australia, or who may leave Australia after a temporary stay. Given the risks to national security interests presented by any unauthorised dealing with security intelligence information, it is appropriate that flexibility is retained to bring such persons to justice, should they deal with records or information acquired or prepared by the Organisation in connection with its functions, or which relates to the performance by the Organisation of its functions, in a manner that contravenes the terms on which access was provided. The geographical location or citizenship of such persons does not undermine the risk of significant harm that their actions may cause to Australia’s national security interests.136

Corresponding amendments are made to the IS Act, which includes inserting definitions of record and signals into the Definitions in section 3. Items 9-22 amend or insert new secrecy offences in Part 6 of the IS Act to prohibit: the unauthorised communication of certain information, the unauthorised dealing with records, and the unauthorised recording of information or matters.

Regarding these amendments the IGIS has submitted that there needs to be some clarity regarding entrusted persons who make complaints to the IGIS:

... complainants to the IGIS, particularly those who have worked in the intelligence community or have entered into some contract, agreement or arrangement with an intelligence agency, require clear advice about whether secrecy laws or undertakings prevent them giving information to the IGIS when making complaints or proactively disclosing matters to the office....

There should be clear statutory authority for individuals to provide information to the IGIS for the purpose of complaints and inspections under the IGIS Act, notwithstanding other laws, agreements or undertakings.137

Schedule 7 – Renaming of Defence agencies

The amendments in this Schedule will facilitate the renaming of DIGO to the Australian Geospatial-Intelligence Organisation (AGO) and DSD to the Australian Signals Directorate (ASD). According to the Explanatory Memorandum, p. 146.

136. IGIS, op. cit., p. 20.
Memorandum, this will ‘better reflect the national roles that those organisations play in support of Australia’s security’.

All references to DIGO and DSD in the IS Act will be replaced by AGO and ASD respectively. Further, items 58–63 and 65–143 will amend the following Acts to take account of the renaming of DIGO and DSD to AGO and ASD:

(a) Anti-Money-Laundering and Counter-Terrorism Financing Act 2006
(b) Archives Act 1983
(c) Australian Human Rights Commission Act 1986
(d) Australian Security Intelligence Organisation Act 1979
(e) Crimes Act 1914
(f) Crimes (Overseas) Act 1964
(g) Criminal Code Act 1995
(h) Freedom of Information Act 1982
(i) Independent National Security Legislation Monitor Act 2010
(j) Inspector-General of Intelligence and Security Act 1986
(k) Privacy Act 1988
(l) Public Interest Disclosure Act 2013.

Concluding comments

The Bill proposes some significant changes to the operations of intelligence agencies, enabling them to update their powers to better respond to current and emerging threats to Australia’s national security. The Bill implements the Government’s response to recommendations in Chapter 4 of 2013 PJCIS Report as well as new measures to update offences relating to unauthorised communications under the ASIO Act and IS Act. The provisions responding to the 2013 PJCIS Report are broadly consistent with the recommendations it contained. However, some of the safeguards and accountability requirements could be improved, particularly those that clearly fall short of what was recommended by the PJCIS. The Bill has attracted significant criticism from stakeholders in this regard. Further, the Bill seems to represent a situation where the whole is greater than the sum of its parts. In drafting provisions to respond to particular recommendations of the PJCIS, not enough attention has been given to the cumulative impact of those amendments in practice, and the additional safeguards that may be appropriate to offset that impact.

It is possible that the Bill may be debated without time for due consideration and scrutiny by the Parliament. Recommendation 41 of the 2013 PJCIS Report was that amendments implementing its recommended changes to AIC legislation be released as an Exposure Draft for public consultation as well as being subject to Parliamentary committee scrutiny and targeted consultation with the INSLM and the IGIS. The Government chose not to release an Exposure Draft and the office of INSLM has been vacant since April 2014, but the Government did refer the Bill to the PJCIS for inquiry and report. If the Bill is debated prior to the PJCIS reporting back to Parliament, that would represent a clear rejection of the PJCIS’s earlier recommendation.
