Australian Government

Attorney-General's Department

Parliamentary Joint Committee on Intelligence and Security

Inquiry into the National Security Legislation Amendment Bill (No. 1) 2014

Attorney-General's Department Submission

July 2014

Introduction

1. The Attorney-General's Department welcomes the opportunity to provide the Parliamentary Joint Committee on Intelligence and Security with this submission as part of the Committee's examination of the National Security Legislation Amendment Bill (No. 1) 2014.

2. The Bill was introduced into the Senate on 16 July 2014 by the Attorney-General, Senator the Hon George Brandis QC, and referred to the Committee on that date for reporting by 8 September 2014.

Background

3. In May 2012, the then Attorney-General, the Hon Nicola Roxon MP, requested the Committee to inquire into a number of potential reforms to Australia's national security legislation. In July 2012, the Department provided a Discussion Paper, *Equipping Australia Against Emerging and Evolving Threats*, to assist the Committee examine these issues. The Committee formally adopted the proposed terms of reference on 6 July 2012 and made a series of recommendations in its *Report on Inquiry into Potential Reforms to National Security Legislation* of May 2013 which was tabled on 24 June 2013.

The purpose of the Committee inquiry

4. The purpose of the Committee's inquiry is to scrutinise whether the Bill appropriately implements the recommendations agreed by the Committee in 2013 and to assess the balance of national security and safeguards proposed in the legislation.

5. Many of the safeguards which apply to these measures have been set out in the explanatory material to the Bill, including the Statement of Compatibility.

6. The Department also notes that the Attorney-General's media release of 16 July 2014 indicated that the Government has decided to retain the position of the Independent National Security Legislation Monitor.

The National Security Legislation Amendment Bill (No. 1) 2014

7. The Bill is, in large part, the Government's response to the recommendations in Chapter 4 of the Committee's report relating to proposed reforms of legislation governing the Australian Intelligence Community (Recommendations 20-41). It implements 18 of the 22 recommendations in whole and 3 in part. The Bill primarily amends the *Australian Security Intelligence Organisation Act 1979* and the *Intelligence Services Act 2001*.

8. The Bill enhances the capability of the Australian Intelligence Community in seven key areas:

- Modernising the Australian Security Intelligence Organisation's (ASIO) statutory employment framework (Schedule 1)
- Modernising and streamlining ASIO's warrant-based intelligence collection powers (Schedule 2)
- Strengthening ASIO's capability to conduct covert intelligence operations subject to appropriate safeguards and oversight (Schedule 3)
- Clarifying and improving the statutory framework for ASIO's co-operative and information-sharing activities (Schedule 4)
- Enhancing the capabilities of agencies under the Intelligence Services Act (Schedule 5)

- Improving protection of intelligence-related information (Schedule 6), and
- Renaming of Defence agencies to better reflect their roles (Schedule 7).

9. A table attached to this submission sets out the way in which the recommendations have been implemented.

10. In addition to the measures proposed by the Committee, the Bill also contains five additional measures:

- additional amendments to employment provisions relating to ASIO, including to provide for voluntary moves to the Australian Public Service (Item 19 in Schedule 1– new section 89) and consolidating the various terminology used in the ASIO Act and across the Commonwealth statute book to describe persons employed by ASIO or performing functions or services for ASIO in accordance with a contract, agreement or other arrangement (Item 4 of Schedule 1)
- the extension of immunity for actions preparatory or ancillary to an overseas activity of an agency under the Intelligence Services Act (Item 12 of Schedule 5 amending subsection 14(2) of the Intelligence Services Act)
- clarifying that an ASIS staff member or agent can use a weapon or self-defence technique in a controlled environment, like a gun club, a firing range or a martial arts club, where it would be lawful for any other Commonwealth officer and/or member of the public to engage in that activity and where the use would otherwise be consistent with proper performance of an ASIS function
- amendments to the secrecy offences in relation to staff, employees or persons under a contract, agreement or arrangement with ASIO or an agency under the Intelligence Services Act or persons having been an employee or agent of a person who has entered into a contract, agreement or arrangement with ASIO or an agency under the Intelligence Services Act (Schedule 6) in three ways:
  - increasing penalties for the existing unauthorised communication offences in the ASIO Act and the Intelligence Services Act from two years' imprisonment to 10 years' imprisonment
  - extending the existing Intelligence Services Act disclosure offences to cover the Defence Intelligence Organisation and the Office of National Assessments and to ensure that all offences cover information received by the agency as well as prepared by it, and
  - creating new offences in relation to unauthorised dealings with records and unauthorised recording of information (with a maximum penalty of three years' imprisonment)
- renaming the Defence Imagery and Geospatial Organisation as the Australian Geospatial-Intelligence Organisation (AGO) and the Defence Signals Directorate as the Australian Signals Directorate (ASD) (Schedule 7) and providing a specific function for the IGIS to report on the extent to which the AGO complies with rules made under section 15 of the Intelligence Services Act (Item 134 of Schedule 7).

11. Further details about these measures are also included in the table.

Conclusion

12. The Department trusts that this information is of assistance to the Committee. The Department is willing to provide any other assistance to the Committee in undertaking this inquiry.

Table of Recommendations 20-41 of the Parliamentary Joint Committee on Intelligence and Security's *Report on Inquiry into Potential Reforms to National Security Legislation* on Australian Intelligence Community Legislation Reforms (Chapter 4) and how they have been implemented in the National Security Legislation Amendment Bill (No. 1) 2014

Recommendation		Position adopted in Bill and relevant provisions
20	The Committee recommends that the definition of computer in the *Australian Security Intelligence Organisation Act 1979* be amended by adding to the existing definition the words 'and includes multiple computers operating in a network'. The Committee further recommends that the warrant provisions of the ASIO Act be amended by stipulating that a warrant authorising access to a computer may extend to all computers at a nominated location and all computers directly associated with a nominated person in relation to a security matter of interest.	**Supported** **Schedule 2: Powers of ASIO** ***Item 4 (definition of computer)*** 'Computer' means all or part of: • one or more computers • one or more computer systems • one or more computer networks • any combination of the above. Since the definition of 'computer' was originally inserted into the ASIO Act the use of multiple computing devices and networked computers systems has become increasingly prevalent. The definition has been broadened to specifically include reference to 'one or more computer networks', removing any ambiguity as to whether computer networks are included. It also includes 'one or more computers' to address the practical issue that data relevant to the security matter may be stored on a number of computers. The reference to a 'computer system' has been retained from the existing definition. ***Item 18 (subsection 25A(3) – target computer)*** Target computer may be any one or more of: • a particular computer • a computer on particular premises • a computer associated with, used by, or likely to be used by a person (whose identity may or may not be known). A computer access warrant currently requires the specification of a 'particular computer' as a target computer. Such an approach is out of date with the way computer technology is currently used. Together with the new definition of 'computer', this amendment will enable ASIO to apply for computer access warrants to authorise it to use computers, computer systems and computer

Recommendation		Position adopted in Bill and relevant provisions
		networks located at particular premises or associated with a nominated person in order to obtain access to data relevant to a matter that is important in relation to security and held in the relevant computers, computer systems or computer networks.
21	The Committee recommends 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.	**Supported** **Schedule 2: Powers of ASIO** The current limitations in subsection 25(6) and 25A(5) that prevent any interference, interruption or obstruction or any loss or damage, can prevent ASIO from effectively executing a search warrant or a computer access warrant as they prevent a warrant from authorising even minor interferences or disruptions. They also create uncertainty if it is not possible to determine whether an act may cause a disruption. These subsections are replaced by new subsections establishing a limitation that prevents a warrant from authorising activities that are likely to materially interfere, interrupt, obstruct, or cause other material loss or damage. ***Item 12 (subsection 25(6) – search warrants)*** ***Certain acts not authorised*** Subsection 25(5) does not authorise the addition, deletion or alteration of data or the doing of any thing likely to: (a) materially interfere with, interrupt or obstruct the lawful use by other persons of a computer or other electronic equipment, or a data storage device, found on the subject premises unless the addition, deletion or alteration, or the doing of the thing, is necessary to do one or more of the things specified under subsection 25(5), or (b) cause any other material loss or damage to other persons lawfully using the computer, equipment or device. Under subsection 25(5), the Minister may authorise in a search warrant, that where there is reasonable cause to believe that data relevant to the security matter may be accessible by using a computer or other electronic equipment, or a data storage device, use of the computer, equipment or device for the purpose of accessing that data, and if necessary to achieve that purpose, other data can be added, deleted or altered. ***Item 25 (subsection 25A(5) – computer access warrants)*** ***Certain acts not authorised*** Subsection 25A(4) does not authorise the addition, deletion or alteration of data or the doing of any thing likely to: (a) materially interfere with, interrupt or obstruct a communication in transit or the lawful use by other persons of a computer unless the addition, deletion or alteration, or the doing of the thing, is necessary

Recommendation		Position adopted in Bill and relevant provisions
		to do one or more of the things specified in the warrant, or (b) cause any other material loss or damage to other persons lawfully using a computer. Under subsection 25A(4), the Minister may authorise in a computer access warrant use of a computer for the purpose of obtaining access to data relevant to the security matter held in a target computer, and if necessary to achieve that purpose, adding, deleting or altering other data in the target computer may be done. Advancements in technology have made it increasingly difficult for ASIO to execute computer access warrants. Persons being investigated are increasingly security conscious and technically proficient, requiring innovative methods of achieving access to the target computer without detection, including methods that may cause a temporary interruption to the target computer. The modified limitations in Items 12 and 25 will allow ASIO to undertake: • acts authorised by a search warrant that are likely to cause immaterial interference, interruption or obstruction of the lawful use of a computer or other electronic equipment, or a data storage device, found on the subject premises, or likely to cause any other immaterial loss or damage to other persons lawfully using the computer, equipment or device, and • acts authorised by a computer access warrant that are likely to cause an immaterial interference, interruption or obstruction to a communication in transit or the lawful use of a computer, or likely to cause any other immaterial loss or damage to other persons lawfully using a computer. ASIO will be able to undertake acts under a search or computer access warrant that are likely to cause a material interference, interruption or obstruction only where necessary to execute the warrant. An immaterial interference would include using a minor amount of storage space or bandwidth, for example.
	The Committee further recommends that the Government pay particular regard to the concerns raised by the Inspector-General of Intelligence and Security (IGIS) (these were to minimise the impact on parties unrelated to the security matter and that there should be appropriate review and oversight mechanisms).	The ASIO Act provides appropriate review and oversight mechanisms. In particular, the IGIS will have oversight over the use of these proposed provisions under the *Inspector-General of Intelligence and Security Act 1986*. The test for the Attorney-General in issuing either a search warrant or a computer access warrant will not change. In the case of a search warrant, the Attorney-General must be satisfied that there are reasonable grounds for believing that access by ASIO to records or other things on particular premises will substantially assist the collection of intelligence in accordance with the ASIO Act in respect of a matter that is important in relation to security. For a computer access warrant, the

Recommendation		Position adopted in Bill and relevant provisions
		Attorney-General must be satisfied that there are reasonable grounds for believing that access by ASIO to data held in the target computer will substantially assist the collection of intelligence in accordance with the ASIO Act in respect of a matter that is important in relation to security. The Attorney-General can also include appropriate additional conditions and restrictions in both warrant types. In undertaking its function of obtaining intelligence relevant to security, ASIO is required to comply with the *Attorney-General's Guidelines in relation to the performance by the Australian Security Intelligence Organisation of its function of obtaining, correlating, evaluating and communicating intelligence relevant to security (including politically motivated violence)* made under section 8A of the ASIO Act. These Guidelines require ASIO to use as little intrusion into individual privacy as possible, consistent with the performance of its functions, and wherever possible, to use the least intrusive method of obtaining intelligence before using more intrusive methods. In the event that the Director-General of Security is satisfied that ASIO has obtained data under warrant that is not required for the purposes of the performance of ASIO's functions or the exercise of its powers, then it must be destroyed in accordance with section 31 of the ASIO Act. Further, ASIO Policies and Procedures provide practical guidance to staff and ensure legal obligations are understood and complied with.
22	The Committee recommends that the Government amend the warrant provisions of the *Australian Security Intelligence Organisation Act 1979* to allow ASIO to access third party computers and communications in transit to access a target computer under a computer access warrant, subject to appropriate safeguards and accountability mechanisms, and consistent with existing provisions under the *Telecommunications (Interception and Access) Act 1979* (the Committee specifically referred to B-Party warrants).	**Supported** **Schedule 2: Powers of ASIO** ***Item 23 (paragraph 25A(4)(ab))*** 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—using any other computer or a communication in transit to access the relevant data and, if necessary to achieve that purpose, adding, copying, deleting or altering other data in the computer or the communication in transit. This proposed provision would enable ASIO to be authorised under a computer access warrant to use a third party computer or communication in transit for the limited and specific purpose of obtaining access to data relevant to the security matter being investigated and held in the target computer. This addresses technological developments which have made it increasingly difficult for ASIO to execute its computer access warrants. Under the amendment, a computer access warrant may specifically authorise ASIO to add, copy, delete or alter data on a third party computer or communication in transit where necessary to facilitate access to the data relevant to the security matter held in the target computer. However, the warrant would not authorise ASIO to use the third party computer or communication in transit for

Recommendation		Position adopted in Bill and relevant provisions
		other purposes. There are a range of appropriate safeguards and accountability mechanisms. While the proposal to use third party computers or communications in transit to gain access to the target computer could indirectly affect the privacy of third parties, such activity is subject to significant safeguards. ASIO will only be authorised to use a third party computer or a communication in transit where it is reasonable in all the circumstances to do so. In making this assessment, ASIO must consider other methods of gaining access to the relevant data which are likely to be as effective. The IGIS will have oversight of the use of these proposed provisions. The Attorney-General's Guidelines (referred to above), which require ASIO to use as little intrusion into individual privacy as is possible, consistent with the performance of its functions, and use the least intrusive method of obtaining intelligence before using more intrusive techniques, also apply. Proposed new section 33 in Item 46 of Schedule 2 specifically provides that ASIO will not be authorised to intercept communications passing over a telecommunications system under a computer access warrant and any such interception will need to be authorised under an appropriate telecommunications interception warrant. ***Item 46 (Relationship with other laws (subsection 33(1))*** *Computer access—relationship with the Telecommunications (Interception and Access) Act 1979* Nothing in section 25A, 27A or 27E, or in a warrant or authorisation under those sections, authorises, for the purposes of the *Telecommunications (Interception and Access) Act 1979*, the interception of a communication passing over a telecommunications system operated by a carrier or a carriage service provider. The other safeguards and accountability mechanisms are modelled on, but not identical to, those in the *Telecommunications (Interception and Access) Act 1979* relating to B-Party warrants as recommended by the Committee. For example, subsection 9(3) of the Telecommunications (Interception and Access) Act requires satisfaction that all other practicable methods of identifying the relevant services have been exhausted or that the interception of the relevant communication would not otherwise be possible. An approach requiring exhaustion of all other methods was considered in this context but was considered too limiting – instead ASIO will only be authorised to access a third party computer or communication in transit where it is reasonable in all the circumstances to do so. In making this assessment, ASIO must consider other methods of gaining access to the relevant data which are likely to be as effective. The existence and relative

Recommendation		Position adopted in Bill and relevant provisions
		effectiveness of other methods of intelligence collection is, therefore, a relevant and persuasive, but non-determinative, consideration. There are also some necessary differences between the safeguards and accountability mechanisms for B-Party warrants and ASIO computer access warrants, which ensure that ASIO warrants are appropriate and adapted to achieving the security purposes to which they are directed. For example, a B-Party warrant has a maximum duration of three months but also authorises access to the content of communications. Unlike B-Party warrants, access to third party computers and communications under ASIO computer access warrants ((which have a maximum duration of six months) will only be for the specific purpose of obtaining access to data relevant to the security matter being investigated and held in the target computer . Retaining the existing maximum duration of six months is necessary to maintain ASIO's capabilities. Further, it would result in an arbitrary distinction if ASIO was able to obtain a six-month warrant to directly access a target computer but only had three months in which to gain access to that same computer via a third party computer or a communication in transit. Such a distinction would compound the operational inefficiencies to which the computer access reforms in the Bill are directed.
23	The Committee recommends the Government amend the warrant provisions of the *Australian Security Intelligence Organisation Act 1979* to promote consistency by allowing the Attorney-General to vary all types of ASIO Act warrants.	**Supported** **Schedule 2: Powers of ASIO** ***Item 44 (new section 29A – variation power)*** (1) The Minister may, on request by the Director General, vary a warrant issued under this Division (other than under section 29). (2) The variation must be in writing. (3) If the variation extends, or further extends, the period during which the warrant is in force, the total period during which the warrant is in force must not exceed: (a) for a warrant issued under section 25—90 days, or (b) for a warrant issued under section 25A, 26, 27, 27AA or 27C—6 months. (4) The request by the Director General must specify: (a) the facts and other grounds on which the Director General considers it necessary that the warrant should be varied, and (b) where appropriate—the grounds on which the Director General suspects a person of being engaged in or reasonably suspected by the Director General of being engaged in, or of being likely to engage in, activities prejudicial to security. (5) A warrant may be varied more than once under this section.

Recommendation		Position adopted in Bill and relevant provisions
		Currently, there is no express ability to vary the terms of a warrant, meaning that minor changes in circumstances during the life of a warrant, such as where the premises to be searched change because a person changes their address or the description of a target computer changes because a person acquires a new computer, would generally require a new warrant. Other reasons for which a variation could be sought include where alterations are required to the specific things that a warrant authorises, such as the times of the day or night authorised for entry onto premises. It would be more efficient to enable the Attorney-General to vary warrants on application by the Director-General. However, these efficiencies would not reduce accountability. The Attorney-General will still have responsibility for issuing and varying warrants and the IGIS will also continue to have oversight of all warrant documentation. A request for variation of a warrant will identify the changes being sought to a warrant and must specify the facts and grounds on which such a change is considered necessary. The Attorney-General would retain the decision-making power on whether to grant a variation. Importantly, the variation power will not enable the Attorney-General to extend a warrant's duration beyond the maximum period allowed in the provisions for that type of warrant.
24	Subject to the recommendation on renewal of warrants, the Committee recommends that the maximum duration of *Australian Security Intelligence Organisation Act 1979* search warrants not be increased.	**Supported** No change proposed in the Bill.
25	The Committee recommends that the *Australian Security Intelligence Organisation Act 1979* be amended to allow the Attorney-General to renew warrants.	**Not supported** On further consideration, this proposal is not considered necessary because the same criteria and level of accountability should apply to both renewal and issuing and in this case a renewal provision would unnecessarily duplicate the issuing provisions.
26	The Committee recommends that the *Australian Security Intelligence Organisation Act 1979* be amended to modernise the Act's provisions regarding secondment arrangements.	**Supported** **Schedule 1: ASIO employment, etc** ***Item 19 (new sections 86 and 87)*** **86 Secondment of ASIO employees** *Secondment* (1) The Director-General may, in writing, arrange for an ASIO employee to be seconded for a specified period to a body or organisation whether within or outside Australia. *Termination of secondment*

Recommendation		Position adopted in Bill and relevant provisions
		(2) The Director-General may at any time, by notice given to the body or organisation to which an ASIO employee is seconded under subsection (1), terminate the secondment. **87 Secondment of persons to the Organisation** (1) The Director-General may, by written agreement with a body or organisation (whether within or outside Australia), arrange for a person who is an officer, employee or other member of staff of the body or organisation to be made available to the Organisation to perform services in connection with the performance or the exercise of any of the Organisation's functions or powers. (2) The terms and conditions (including remuneration and allowances) applicable to a person performing services under an agreement are those specified in the agreement. To enhance ASIO's ability to develop its workforce and access specialised skills and experience, ASIO may wish to second staff to and from other bodies or organisations, whether within or outside of Australia, for a period of time. Due to the specified scope of the functions and powers of ASIO and other agencies, legal complexities can arise as to the status of a person's work and which type of work may be undertaken during the placement or secondment. Currently, a secondment arrangement to or from ASIO may be done by way of ad hoc arrangements and may be facilitated by the person taking leave from their home agency and being temporarily employed by the seconding agency. Including specific provisions in the ASIO Act dealing with secondments would enable such secondments to occur with greater efficiency and provide greater clarity as to which agency the person works for during the secondment period and the associated legislative and other obligations with which they must comply. The secondment provisions operate independently of the existing 'co-operation' provisions, and do not circumvent any current limitations on a person exercising an agency's functions in legislation.
27	The Committee recommends that the *Intelligence Services Act 2001* be amended to clarify the authority of the Defence Imagery and Geospatial Organisation to undertake its geospatial and imagery functions.	**Supported** **Schedule 5: Activities and Functions of Intelligence Services Act agencies** ***Items 4 and 5 (paragraph 6B(e)(ii) and new paragraph 6B(e)(iia))*** These provisions will enable DIGO to provide assistance to Commonwealth and State authorities and bodies approved by the Minister in relation to the provision of: • technical assistance in the production and use of all imagery and geospatial products (including technical assistance in relation to products which use intelligence information – removing a current exclusion of these products due to a technical drafting issue), and • assistance in relation to technologies as well as products (which may not be covered by the existing

Recommendation		Position adopted in Bill and relevant provisions
		term products).
28	The Committee recommends that the *Australian Security Intelligence Organisation Act 1979* be amended to create an authorised intelligence operations scheme, subject to similar safeguards and accountability arrangements as apply to the Australian Federal Police controlled operations regime under the *Crimes Act 1914*.	**Supported** **Schedule 3 – protection for special intelligence operations** The Bill would insert a new Division 4 of Part III establishing the scheme of special intelligence operations (new sections 35A-35R). The provisions have the following operation: • 35A provides that the Division is not intended to limit a court's discretion to admit or exclude evidence or stay criminal proceedings in the interests of justice • 35B sets out how applications can be made for authorities to conduct special intelligence operations • 35C provides for the granting of authorities and the matters that an authorising officer must consider, including how a special intelligence operation will assist ASIO in the performance of one or more special intelligence functions (defined to refer to paragraphs 17(1)(a), (b), (e) or (f) of the ASIO Act). A special intelligence operation cannot authorise serious offences against the person (including causing death or serious injury or the commission of a sexual offence) or against property (actions resulting in the serious loss of, or serious damage to, property are also prohibited) • 35D sets out the content of authorities – including the conditions applicable to a special intelligence operation and the fact that it cannot exceed 12 months • 35E sets out the commencement and duration of authorities • 35F provides for the variation of authorities • 35G provides for the cancellation of authorities • 35H sets out the effect of an authority • 35J details what occurs when there is a defect in the authority • 35K provides for a limited form immunity for special intelligence conduct during a special intelligence operation • 35L provides that the requirements to otherwise obtain a warrant under either the *Australian Security Intelligence Organisation Act 1979* or the *Telecommunications (Interception and Access) Act 1979*, are not affected • 35M sets out the effect of a person being unaware of variation or cancellation of an authority • 35N provides protection from criminal responsibility for certain ancillary conduct • 35P creates new offences for the unauthorised disclosure of information and the unauthorised disclosure of information endangering safety (detailed below) • 35Q requires the Director-General to report to the Minister and the IGIS on special intelligence

Recommendation		Position adopted in Bill and relevant provisions
		operations, and • 35R sets up an evidentiary certificate regime relating to the granting of a special intelligence operation. New subsection 94(2A) of the ASIO Act will also require ASIO to report in its annual report on the number of applications made and the number of authorities granted during the year. ASIO is required to conduct its activities in a lawful manner. However, in some instances, collecting intelligence may require engaging in conduct that could expose a person to civil or criminal liability. As a consequence, some significant investigations either do not commence or are ceased due to the risk that a person could be exposed to criminal or civil liability. For example, in some cases, collecting intelligence on a terrorist group may be best achieved by ASIO associating with known terrorists or terrorist groups. Without a special intelligence operations scheme, this would expose participants to criminal liability, for example, in relation to offences concerning membership of, receiving training from or providing support to a terrorist organisation. Currently, there is no immunity, limited or otherwise, for ASIO to engage in such conduct. In comparison, there is immunity for Australia's foreign intelligence agencies under the Intelligence Services Act and for law enforcement agencies under the Crimes Act. The controlled operations scheme in the *Crimes Act 1914* contains offences for the disclosure of information relating to controlled operations (sections 15HK and 15HL of the Crimes Act). Comparable offences have been included in new section 35P of the ASIO Act. These offences are necessary and appropriate given the significant, adverse consequences that disclosure of information about covert intelligence operations will have on national security interests – both in prejudicing or frustrating the conduct of operations and in jeopardising the lives and safety of participants and persons connected to them. These offences do not contain an express defence for the disclosure of information to an independent oversight body because provision is made for such disclosures under the *Public Interest Disclosure Act 2013* which provides that secrecy offences do not apply to disclosures made in accordance with the public interest disclosure regime, including disclosure of intelligence information or matters relating to the conduct of an intelligence agency to an agency head or the IGIS. In addition, secrecy offences do not apply to disclosures to the IGIS in accordance with notices issued under the *Inspector-General of Intelligence and Security Act 1986*, by reason of subsection 18(9) of that Act. There are two offences in proposed section 35P. The primary offence has a maximum penalty of five years' imprisonment which applies to persons who intentionally disclose information and either know or are reckless as to whether that information relates to a special intelligence operation. The aggravated

Recommendation		Position adopted in Bill and relevant provisions
		offence has a maximum penalty of ten years' imprisonment. This offence requires proof, in addition to elements of the primary offence, that either the person intended to endanger the health or safety of any person or prejudice the effective conduct of an operation or that the disclosure of information will endanger the health or safety of a person or prejudice the effective conduct of a special intelligence operation. There are some differences in the penalties applying to offences for the unauthorised disclosure of information relating to controlled operations in the Crimes Act and the proposed offences relating to special intelligence operations. The penalty for the primary offence in the Crimes Act of disclosing information relating to a controlled operation is two years' imprisonment, while the penalty is five years' imprisonment under the corresponding proposed ASIO Act offence. The higher proposed penalty in the ASIO Act is designed to align with existing penalties for secrecy offences in relation to intelligence operations (such as the penalty applying to disclosing information in relation to a questioning or questioning and detention warrant in section 34ZS). The safeguards and accountability arrangements in relation to the special intelligence operations scheme have been modelled as closely as possible on those that apply to the law enforcement controlled operations regime under the Crimes Act. However, the controlled operations scheme in Part 1AB of the Crimes Act was developed for a different purpose to the proposed special intelligence operations scheme. Controlled operations are covert law enforcement activities, focusing on the collection of evidence for use in prosecutions of serious offences whereas the proposed special intelligence operations scheme is about the gathering of intelligence relevant to national security issues. Certain conduct can never be authorised (see above). Further, the protection from liability also excludes conduct that intentionally induces another person to commit an offence that they would not otherwise have intended to commit (see proposed section 35C). The protection from liability will also only apply to conduct engaged in by an authorised participant in the course of an operation where it is in accordance with the authority – if a person was found to act outside the authorisation, they would not be protected from the liability incurred outside of the authorisation. Special intelligence operations will only be approved if the Director-General or a Deputy Director-General is satisfied that the nature of the intelligence or the threat justifies the conduct of a special intelligence operation and they may cancel the authorisation at any time and for any reason. Importantly, an authority cannot authorise activities that would require a warrant under the ASIO Act or a warrant or an authorisation under the Telecommunications (Interceptions and Access) Act. ASIO must report on the conduct of all special intelligence operations authorised under the proposed

Recommendation		Position adopted in Bill and relevant provisions
		scheme on a six monthly basis to the Attorney-General and the IGIS. In addition, ASIO's annual reports must include the number of applications and authorisations made under the proposed scheme. The IGIS would have oversight of these proposed provisions and individuals can complain to the IGIS under the Inspector-General of Intelligence and Security Act. The IGIS can recommend that the Government pay compensation to a person who is adversely affected by authorised conduct in the course of a special intelligence operation.
29	The Committee recommends that should the Government proceed with amending the ASIO Act to establish a named person warrant, further consideration be given to the factors that would enable ASIO to request a single warrant specifying multiple powers against a single target.	**Supported** **Schedule 2: Powers of ASIO** ***Item 41 (new subdivision G (identified person warrants) – new sections 27C-27J)*** In approximately one third of cases, more than one warrant type is sought in relation to a particular person. Under the current provisions, this requires the preparation of multiple warrant requests by the Director-General and the issuing of multiple warrants by the Attorney-General. It is more operationally effective to enable the Attorney-General to consider a single warrant request from the Director-General and to authorise the types of special powers that he or she considers would be appropriate for ASIO to use in relation to a particular person. In addition to administrative efficiencies, the proposed identified person warrant would enable ASIO to respond more quickly to changing circumstances in the operational environment. The proposed identified person warrant would enable the Attorney-General, if he or she is satisfied that the legislative threshold is met, to provide conditional approval for ASIO to exercise those particular types of powers for the duration of the warrant (including searches of premises, computer access, surveillance or inspection of postal or delivery service articles). The Director-General or the Attorney-General can then give an authorisation to engage in particular powers for which conditional approval is granted. The Attorney-General may include conditions and restrictions in the warrant, which may include that it only provides authority to use certain special powers in certain circumstances. The threshold for issuing the warrant will have two limbs: • an identified person is engaged in or is reasonably suspected by the Director-General of being engaged in or likely to engage in activities prejudicial to security, and • the issuing of an identified person warrant in relation to the person will or is likely to substantially assist the collection of intelligence relevant to security. The Director-General or Attorney-General must consider and separately grant authority for the use

Recommendation		Position adopted in Bill and relevant provisions
		of each power, if satisfied that the use of that power in a particular circumstance will substantially assist ASIO to collect intelligence in relation to the activities prejudicial to security. Although the proposed warrant would provide this new decision-making power to the Director-General, as well as the Attorney-General, there is no effective reduction in the applicable accountability measures as the Attorney-General must provide conditional approval for ASIO to use particular types of powers, the Attorney-General retains the discretion to impose conditions or restrictions as he or she considers appropriate and the Director-General would continue to be required to discontinue action under the warrant if the grounds on which the warrant was issued by the Attorney-General cease to exist. The duration of warrants will not be extended under the new identified person warrants. There are a range of accountability mechanisms to ensure that these powers are appropriately used including appropriate internal controls and IGIS oversight of the use of these powers.
30	The Committee recommends that the *Australian Security Intelligence Organisation Act 1979* be amended to modernise the warrant provisions to align the surveillance device provisions with the *Surveillance Devices Act 2004*, in particular by optical devices.	**Supported** **Schedule 2: Powers of ASIO** ***Items 5, 6 and 7 (amendments to definitions including 'optical surveillance device' and 'surveillance device')*** ***Item 29 (new Subdivision D – use of surveillance devices – new sections 26-26F)*** The ASIO Act surveillance device provisions have been more closely aligned in the Bill with the Surveillance Devices Act as the Surveillance Devices Act is a more modern piece of legislation and better reflects technological developments. The Surveillance Devices Act also provides greater legal certainty regarding the scope of activities permitted to be undertaken under a warrant. Alignment of the existing warrantless surveillance provisions in subsection 26(1) of the ASIO Act with those in the Surveillance Devices Act are reflected in proposed sections 26C and 26D. ASIO's existing power to install, use or maintain surveillance devices on third party premises for the purpose of observing/listening to the target in the primary premises, which does not appear in the Surveillance Devices Act, will also be retained. The Surveillance Devices Act was developed for law enforcement agencies and consequently, there are certain aspects that are not as well suited to ASIO's security intelligence functions. For example, the legislative test for the issuing of a warrant under the Surveillance Devices Act relates to relevant offences whereas ASIO only investigates security matters. On this basis, the existing tests for obtaining a warrant have been retained as has the Attorney-General's role as an issuing authority. The provisions of the Surveillance Devices Act relating to internal authorisation in section 39 were not considered necessary and have not been adopted on that basis. Further, ASIO's

Recommendation		Position adopted in Bill and relevant provisions
		existing capabilities to recover devices without warrant in subsections 26(6A), 26B(7), 26C(7) and 27A(3A) have been retained and tailored to ASIO's operational context in proposed subsection 26B(5). The existing duration of surveillance devices warrants which can be up to six months has also been retained. The provisions around entry to third party premises have also been modified, based on the provisions of the Surveillance Devices Act, and Recommendation 35. ASIO's surveillance devices framework has also been amended to facilitate ASIO's operational effectiveness in certain respects. For example, ASIO will be permitted to replace an object with an equivalent object for the purposes of installing, using or maintaining a surveillance device. ASIO's surveillance devices framework does not include a power to use data surveillance devices. ASIO's use of warranted powers remains the subject of extensive accountability and oversight mechanisms, which are different to those of law enforcement agencies with external and independent scrutiny being provided by the IGIS, and not the Ombudsman. In addition to internal controls, there are also requirements to report to the Attorney-General on the effectiveness of each warrant and to comply with the Attorney-General's Guidelines, which includes requirements of proportionality and using as little intrusion into privacy as possible.
31	The Committee recommends that the *Australian Security Intelligence Organisation Act 1979* not be amended to enable person searches to be undertaken independently of a premises search.	**Supported** No change proposed in the Bill.
32	The Committee recommends that the *Australian Security Intelligence Organisation Act 1979* be amended to establish classes of persons able to execute warrants.	**Supported** **Schedule 2: Powers of ASIO** ***Item 8 (new section 24 – exercise of authority under warrant)*** *Who may exercise authority under warrant etc.* (1) The authority conferred by a relevant warrant or relevant device recovery provision may be exercised on behalf of the Organisation only by: (a)the Director-General, or (b)a person approved under subsection (2), or (c)a person included in a class of persons approved under subsection (2). *Approval of persons authorised to exercise authority under warrant etc.* (2) The Director-General or a person appointed under subsection (3) may, in writing, approve a person, or a class of persons, as people authorised to exercise, on behalf of the Organisation, the authority conferred by relevant warrants or relevant device recovery provisions.

Recommendation		Position adopted in Bill and relevant provisions
		(3) The Director-General may, in writing, appoint a senior position-holder, or a class of senior position-holders, for the purposes of subsection (2). *Definitions* (4) In this section: ***relevant device recovery provision*** means subsection 26B(5) or (6), 27A(3A) or (3B) or 27F(5). ***relevant warrant*** means a warrant issued under this Division or under Division 3. Currently, section 24 of the ASIO Act provides that the Director-General (or senior officer authorised in writing by the Director-General for the purposes of section 24) may approve certain people to exercise authority conferred by warrants. In effect, this requires ASIO to maintain a list of every individual who may be involved in executing a warrant, which can create operational inefficiencies for ASIO. At times, the execution of a warrant takes place in unpredictable and volatile environments and ASIO needs to be able to change the people who will exercise the authority of a warrant at short notice, or with no notice. To ensure compliance with the legislation and provide sufficient operational flexibility, ASIO may be required to list a large number of persons for this purpose – even though they will not all be required to exercise authority. The ability to specify relevant ASIO staff by level and/or reference to their role and work area is a more effective way of listing appropriate persons able to execute the warrant. Both the existing provision and the proposed amendment rely on ASIO maintaining effective records in relation to the actual execution of the warrant for accountability and oversight purposes. This is an area that the IGIS will continue to inspect and monitor.
33	The Committee recommends that the *Australian Security Intelligence Organisation Act 1979* be amended to formalise ASIO's capacity to co-operate with private sector entities.	**Supported** **Schedule 4: ASIO co-operation and information-sharing** ***Item 5 (new paragraph 19(1)(d))*** any other person or body whether within or outside Australia Section 19 of the ASIO Act provides that ASIO may co-operate with other authorities in connection with the performance of its functions. Paragraphs 19(1)(a) and (b) provide that ASIO may co-operate with authorities of the Commonwealth, as well as Departments, police forces and authorities of the States, where it is necessary for, or conducive to, the performance of ASIO's functions in section 17 of the ASIO Act. This new provision will confirm ASIO's ability to co-operate with the private sector, including any other person or body, whether within or outside of Australia, in connection with the performance of its functions. Where ASIO seeks to co-operate with a private sector organisation outside Australia, this may be subject to arrangements made or

Recommendation		Position adopted in Bill and relevant provisions
		directions given by the Minister as provided for under subsection 19(1) of the ASIO Act. ASIO's functions relating to security are not geographically limited and it may be necessary for ASIO to co-operate with persons or bodies not in Australia to protect Australia's national security. For example, ASIO may need to co-operate with a company that is incorporated outside Australia but has a significant presence within Australia, where it may own or operate critical infrastructure. The IGIS has oversight functions to ensure that ASIO acts legally and with propriety and complies with ministerial directions and guidelines.
34	The Committee recommends that the *Australian Security Intelligence Organisation Act 1979* be amended so that ASIO may refer breaches of section 92 to law enforcement for investigation.	**Supported** **Schedule 4: ASIO co-operation and information-sharing** **Items 1-3 (new subparagraph 18(3)(b)(ia))** Section 92 of the ASIO Act makes it an offence for a person to publish or otherwise make public, the identity of an ASIO employee or affiliate or a former ASIO employee or affiliate. This offence is punishable by one years' imprisonment. Section 18 of the ASIO Act limits the circumstances in which a person can communicate information or intelligence acquired through their relationship with ASIO. Information may be passed to law enforcement agencies in relation to a 'serious crime' or where the Director General, or a person authorised by the Director-General, is satisfied that it is in the national interest to communicate the information. A 'serious crime' is defined in section 4 of the ASIO Act as an offence punishable by imprisonment exceeding 12 months. Because the penalty in section 18 does not satisfy the threshold to be a serious crime and it may not necessarily always be in the national interest to communicate a breach of section 92, ASIO is currently unable to pass information to law enforcement agencies about the possible commission of an offence under section 92 where it does not otherwise relate to security. The existing exemptions in subsections 92(1B) and 92(2) will be retained in situations where a person either identifies themselves or consents to the action being taken or in relation to the broadcasting, datacasting or reporting of proceedings in the Parliament.
35	The Committee recommends that the *Australian Security Intelligence Organisation Act 1979* be amended to clarify that the incidental power in the search and computer access warrant provisions includes entry to a third party's premises for the purposes of executing those warrants. However, the Committee is of the view that whatever	**Supported** **Schedule 2: Powers of ASIO** **Item 10 (new paragraph 25(4)(aa) (search warrants))** **Item 19 (new paragraph 25A(4)(aaa) (computer access))** These provisions would allow the Attorney-General to issue a warrant authorising ASIO to enter any premises for the purposes of gaining entry to or exiting the premises specified in the warrant,

Recommendation		Position adopted in Bill and relevant provisions
	amendments are made to facilitate this power should acknowledge the exceptional nature and very limited circumstances in which the power should be exercised.	being the 'subject premises' in relation to a search warrant and the 'specified premises' in relation to a computer access warrant. Third party premises would only be accessed if that is the most operationally viable means of entry, such as through common areas in an apartment complex, or if other methods of entry pose too great a risk to the safety of officers or risk of an operation being exposed. Another situation in which they could be used is where, due to unforseen circumstances, a person returns home while a search warrant is being executed. The Attorney-General's Guidelines require all activities to be done with as little intrusion into privacy as possible. Therefore, third party premises would only be accessed where such an intrusion was justified due to the operational circumstances of the case. Further, these provisions do not provide any powers to search or otherwise collect intelligence on a third party premises – it is limited to entry to the premises. Wherever possible and appropriate in the operational circumstances, ASIO will obtain consent of the third party. Persons who are concerned about activity or interference by ASIO are able to raise concerns with the IGIS, who can inquire into those matters.
36	The Committee recommends that the *Australian Security Intelligence Organisation Act 1979* be amended to clarify that reasonable force can be used at any time for the purposes of executing the warrant, not just on entry, and may only be used against property and not persons.	**Supported in part** The clarification that reasonable force can be used at any time is supported. However, the exclusion of the use of reasonable force against a person is not supported. There may be circumstances in which reasonable force against a person is necessary to execute a warrant, for example where a person attempts to physically obstruct the execution of a warrant. On this basis, the provisions will make it clear that force can also be used against persons. ASIO would generally be assisted by law enforcement officers for this purpose and those law enforcement officers would rely on the power conferred by the ASIO Act warrant to use reasonable force. Lethal force or force which causes grievous bodily harm is not authorised and if the use of force was not reasonable and necessary in the circumstances, it may attract criminal and or civil liability. **Schedule 2: Powers of ASIO** ***Items 13-14 (search warrants)*** ***Items 27-28 (computer access warrants)*** These provisions amend the headings to the provision (authorisation of entry measures) to remove limitation to entry and insert an express reference to use of force against persons and things to ensure that the use of reasonable force against persons is covered. ***Item 30 (surveillance devices warrants)***

Recommendation		Position adopted in Bill and relevant provisions
		Item 36 (foreign intelligence warrants) ***Item 41 (identified person warrants: new section 27J(3)(d))*** These provisions insert an express reference to use of force against persons and things to ensure that the use of reasonable force against persons is also covered.
37	The Committee recommends that the *Australian Security Intelligence Organisation Act 1979* be amended to introduce an evidentiary certificate regime to protect the identity of officers and sources. The Committee also recommends that similar protections be extended to ASIO in order to protect from disclosure in open court its sensitive operational capabilities, analogous to the provisions of the *Telecommunications (Interception and Access) Act 1979* and the protections contained in the counter terrorism provisions in the Commonwealth *Criminal Code*.	**Supported** **Schedule 2: Powers of ASIO** ***Item 47 (new section 34AA – evidentiary certificates)*** (1) Subject to subsection (2), the Director-General or a Deputy Director-General may issue a written certificate setting out such facts as he or she considers relevant with respect to acts or things done by, on behalf of, or in relation to, the Organisation: (a) in connection with a relevant warrant; or (b) in accordance with a relevant authorising provision. (2) A certificate may be issued with respect to acts or things done in connection with: (a) a warrant issued under section 27A or 29, but only if the warrant authorises the doing of acts or things referred to in section 25A or 26B, and only with respect to those acts or things; or (b) a warrant issued under section 27C, but only if acts or things are authorised under section 27E or 27F under the warrant, and only with respect to those acts or things. (3) Without limiting subsection (1), the certificate may set out one or more of the following: (a) if premises were entered under the relevant warrant or relevant authorising provision: (i) details of the premises; or (ii) the time of day or night the premises were entered; (b) if data was accessed under the relevant warrant or relevant authorising provision—details of the computer, telecommunications facility, electronic equipment, data storage device or communication in transit used for the purpose of obtaining such access; (c) if the warrant is a surveillance device warrant—the matters required to be specified under section 26A for the warrant; (d) if one or more surveillance devices were installed, used or maintained under the relevant warrant or relevant authorising provision: (i) details of the installation, use or maintenance of the surveillance device or devices; or (ii) details of the installation, use or maintenance of any enhancement equipment in relation to the surveillance device; or (iii) details of the processes and procedures employed to use the surveillance device or devices, or any

Recommendation		Position adopted in Bill and relevant provisions
		enhancement equipment; or (iv) details of acts or things done for the purposes of recovering the surveillance device or devices, or any enhancement equipment; (e) details of things done under the relevant warrant or relevant authorising provision that were reasonably necessary to conceal the fact that things were done under the relevant warrant or relevant authorising provision; (f) details of persons who exercised the authority given by the relevant warrant or relevant authorising provision; (g) details of things done under the relevant warrant or relevant authorising provision that were reasonably incidental to any of the acts or things done by, on behalf of, or in relation to, the Organisation in connection with the relevant warrant or relevant authorising provision. (4) In a proceeding, a certificate under subsection (1) is prima facie evidence of the matters stated in the certificate. (5) In this section: ***proceeding*** means: (a) a proceeding or proposed proceeding in a federal court, or in a court of a State or Territory; or (b) a proceeding or proposed proceeding (including a hearing or examination, or proposed hearing or examination) by or before: (i) a tribunal in Australia; or (ii) any other body, authority or person in Australia having power to hear or examine evidence. ***relevant authorising provision*** means subsection 26B(5) or (6), section 26C, 26D or 26E or subsection 27A(3A) or (3B) or 27F(5). ***relevant warrant*** means a warrant issued under section 25A, 26, 27A, 27C or 29. An additional evidentiary certificate provision is also included in Schedule 3 in relation to the issuing of authorities to conduct special intelligence operations.
	The Committee further recommends that the Attorney-General give consideration to making uniform across Commonwealth legislation provisions for the protection of certain sensitive operational capabilities from disclosure in open court.	There are a range of mechanisms to protect sensitive information in court proceedings. These include the *National Security Information (Criminal and Civil Proceedings) Act 2004* which applies to all civil and federal criminal proceedings and provides a framework for protection of sensitive operational capabilities from disclosure in open court. The Department will consider whether reforms are required.

Recommendation		Position adopted in Bill and relevant provisions
38	The Committee recommends that the *Intelligence Services Act 2001* be amended to add a new ministerial authorisation ground where the Minister is satisfied that a person is, or is likely to be, involved in intelligence or counter-intelligence activities in circumstances where such an investigation would not currently be within the operational authority of the agency concerned.	**Supported** 'Intelligence or counter-intelligence activities' relates to the operational security of ASIS. **Schedule 5: Activities and functions of Intelligence Services Act agencies** ***Item 1 (section 3 – definition of operational security)*** ***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 ***Item 6(new subparagraph 9(1A)(a)(iiia) – operational security)*** activities that pose a risk, or are likely to pose a risk, to the operational security of ASIS The current ministerial authorisation grounds in subparagraph 9(1A)(a) of the Intelligence Services Act do not specifically cover the situation where an Australian person is, or is likely to be, involved in activities that pose a risk, or are likely to pose a risk, to the operational security of ASIS. The new provisions will better protect the integrity of ASIS operations and its staff members and agents from the risk of being interfered with or undermined by foreign persons or entities (for example, non-State adversaries such as terrorist organisations) or where ASIS is at risk of relying on inaccurate or false information. There are several existing safeguards under the Intelligence Services Act that currently apply to Ministerial Authorisation grounds that would equally apply to these measures. The IGIS has oversight of these authorisations, ensuring the authorisation is proper and lawful. The IGIS also oversights the legality and propriety of any activity undertaken by ASIS under the authorisation.
39	The Committee recommends that where ASIO and an *Intelligence Services Act 2001* agency are engaged in a co-operative intelligence operation a common standard based on the standards prescribed in the ASIO Act should apply for the authorisation of intrusive activities involving the collection of intelligence on an Australian person.	**Supported in part** The Government has supported this recommendation in part by enhancing ASIS's ability to co-operate with ASIO overseas by adopting the standard relating to less intrusive activities in the ASIO Act. Under these amendments, ASIS can only produce intelligence overseas on Australian persons to assist ASIO without the requirement to obtain a Ministerial Authorisation, if ASIO would not require a warrant to undertake the same activities in Australia. The differences in the legislative regimes that apply to ASIO when it produces intelligence on Australian persons who are overseas have led to situations that limit the extent of co-operation between the two agencies. These amendments (set out below) provide consistent protections for Australian persons that will apply to this co-operation as well as providing a means of addressing

Recommendation		Position adopted in Bill and relevant provisions
		the risk of delay in ASIS being able to act in an emergency situation. There are a range of safeguards and oversight mechanisms that apply to this activity, some of which are explicitly set out in the new provisions. For example, action will only be able to be undertaken when the Director-General or an authorised person in ASIO requests assistance in writing (except in emergency situations – see 13B). ASIS will still be required to obtain a Ministerial authorisation under section 9 of the Intelligence Services Act before undertaking particularly intrusive activities overseas (for example, the use of tracking devices, listening devices and the interception of telecommunications) or if its activities are unrelated to ASIO's requirements. The two agencies will continue to have distinct functions and comply with the limits set out in their governing legislation. The IGIS has oversight functions to ensure that the agencies act legally and with propriety and comply with ministerial directions and guidelines. The Foreign Minister and the Attorney-General will be able to jointly issue written guidelines in relation to undertaking activities. Any intelligence produced will only be retained and communicated in accordance with the rules to protect the privacy of Australians made by the Minister for Foreign Affairs under section 15 of the Intelligence Services Act. The IGIS will have to be notified where an activity is undertaken in an emergency and requests for assistance must be retained and made available to the IGIS on request. The provisions also require annual reporting to the Foreign Minister. **Schedule 5: Activities and functions of Intelligence Services Act agencies** ***Item 11 (new Division 3 of Part 2 – activities undertaken in relation to ASIO (new sections 13B-13G))*** **Division 3—Activities undertaken in relation to ASIO** **13B Activities undertaken in relation to ASIO** *When an activity may be undertaken in relation to ASIO* (1) Subject to section 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:

Recommendation		Position adopted in Bill and relevant provisions
		(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. (2) The undertaking of an activity or series of activities under subsection (1) is subject to any conditions specified in the notice under paragraph (1)(d). *When notice from ASIO not required—particular activity* (3) Paragraph (1)(d) does not apply in relation to the undertaking of a particular activity in relation to a particular Australian person if a staff member of ASIS who: (a) is authorised under subsection (7); and (b) will be undertaking the activity reasonably believes that it is not practicable in the circumstances for ASIO to notify ASIS in accordance with that paragraph before undertaking the activity. (4) If ASIS undertakes an activity in accordance with subsection (3), ASIS must, as soon as practicable, notify ASIO and the Inspector-General of Intelligence and Security, in writing, of the activity. *Effect of this section* (5) ASIS may undertake an activity or series of activities under subsection (1) without an authorisation under section 9 for the activity or series of activities. *Incidental production of intelligence* (6) An activity, or a series of activities, does not cease to be undertaken: (a) in accordance with this section; or (b) for the specific purpose of supporting ASIO in the performance of its functions; only because, in undertaking the activity or series of activities, ASIS also incidentally produces intelligence that relates to the involvement, or likely involvement, of an Australian person in one or more of the activities set out in paragraph 9(1A)(a). *Authorised staff members* (7) The Director-General may authorise, in writing, a staff member of ASIS, or a class of such staff members, for the purposes of paragraph (3)(a). *Instruments not legislative instruments* (8)The following are not legislative instruments: (a) a notice under paragraph (1)(d); (b) a notice under subsection (4);

Recommendation		Position adopted in Bill and relevant provisions
		(c) an authorisation made under subsection (7). **13C Authorised persons for activities undertaken in relation to ASIO** *Authorised persons* (1) The Director-General of Security may authorise, in writing, a senior position-holder, or a class of senior position-holders, for the purposes of subparagraph 13B(1)(d)(ii). *Authorisation is not a legislative instrument* (2) An authorisation made under subsection (1) is not a legislative instrument. *Definitions* (3) For the purposes of this section, ***senior position-holder*** has the same meaning as in the *Australian Security Intelligence Organisation Act 1979*. **13D Certain acts not permitted** If ASIO could not undertake a particular act in at least one State or Territory without it being authorised by warrant under Division 2 of Part III of the *Australian Security Intelligence Organisation Act 1979* or under Part 2-2 of the *Telecommunications (Interception and Access) Act 1979*, this Division does not allow ASIS to undertake the act. **13E Director-General to be satisfied of certain matters** The Director-General must 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. **13F Other matters relating to activities undertaken in relation to ASIO** *ASIO to be consulted before communicating intelligence* (1) If, in undertaking an activity or series of activities in accordance with section 13B, ASIS produces intelligence, ASIS must not communicate the intelligence outside ASIS (other than in accordance with subsection (2)) unless ASIO has been consulted. *Intelligence to be communicated to ASIO* (2) If, in undertaking an activity or series of activities in accordance with section 13B, ASIS produces intelligence, ASIS must cause the intelligence to be communicated to ASIO as soon as practicable after the production. *Notices to be made available to the Inspector-General of Intelligence and Security*

Recommendation		Position adopted in Bill and relevant provisions
		(3) If a notice is given to ASIS under paragraph 13B(1)(d), the Director-General must ensure that a copy of the notice is kept by ASIS and is available for inspection on request by the Inspector-General of Intelligence and Security. *Reports about activities to be given to the responsible Minister* (4) As soon as practicable after each year ending on 30 June, the Director-General must give to the responsible Minister in relation to ASIS a written report in respect of activities undertaken by ASIS in accordance with section 13B during the year. **13G Guidelines relating to activities undertaken in relation to ASIO** (1) The responsible Minister in relation to ASIO and the responsible Minister in relation to ASIS may jointly make written guidelines relating to the undertaking of activities in accordance with section 13B. (2) Guidelines made under subsection (1) are not a legislative instrument.
40	The Committee recommends that the *Intelligence Services Act 2001* be amended to enable ASIS to provide training in self-defence and the use of weapons to a person co-operating with ASIS.	**Supported** **Schedule 5: Activities and functions of Intelligence Services Act agencies** ***Items 14-15 and 17-20 – Schedule 2 – limits on provision of weapons, training etc*** Currently, ASIS is only permitted to provide training in the use of weapons and self-defensive techniques for defensive purposes to ASIS staff members and agents. This is inconsistent with ASIS's ability to protect others who are co-operating with ASIS in the performance of its functions under section 13 of the Intelligence Services Act. This is because it restricts joint training activities with those persons as ASIS cannot run training that includes individuals who are not ASIS staff members or agents. This amendment will only allow ASIS to train officers from the small number of Australian agencies that have a lawful right under Australian law to carry weapons (for example, the Australian Defence Force) as well as training staff from a limited number of trusted foreign authorities that are approved by the Foreign Minister after consulting with the Prime Minister and the Attorney-General. In practice this will be the United States of America, United Kingdom, Canadian and New Zealand agencies. All training in the use of weapons and self-defence techniques and the issuing of weapons for this training must be approved by the Minister. The approval by the Minister must specify the purpose for which the training or weapon is provided, any conditions that must be complied with and the kind of weapon involved and copies of all approvals by the Minister must be provided to the IGIS. The IGIS will oversight the operation of this new provision for legality and propriety.

Recommendation		Position adopted in Bill and relevant provisions
41	The Committee recommends that the draft amendments to the *Australian Security Intelligence Organisation Act 1979* and the *Intelligence Services Act 2001*, necessary to give effect to the Committee's recommendations, should be released as an exposure draft for public consultation. The Government should expressly seek the views of key stakeholders, including the Independent National Security Legislation Monitor and Inspector-General of Intelligence and Security. In addition, the Committee recommends the Government ensure that the draft legislation be subject to Parliamentary committee scrutiny.	**Supported in part (the intent of public and stakeholder consultation and consideration by a Parliamentary Committee)** The Government has given effect to this recommendation by different means: • Referral of Bill to the Committee for public consultation – including a report following public submissions and hearings, and • Consultation with IGIS on the policy and draft Bill. There has not been any consultation with the Independent National Security Legislation Monitor due to a vacancy in the office. The Monitor's statutory remit in section 6 of the *Independent National Security Legislation Monitor Act 2010* relates to Australia's counter-terrorism and national security legislation and other relevant laws of the Commonwealth, not proposed laws.

Five additional measures implemented in the National Security Legislation Amendment Bill (No. 1) 2014

Schedule and Reference in Bill	Measures
Schedule 1: ASIO employment, etc: **Other provisions relating to the modernising of employment provisions in the ASIO Act**	There are a number of new employment provisions (see, for example, Item 19 which includes new sections 84 (employees) and 85 (consultants and contractors) and section 88 (which facilitates the application of the principles of the Public Service Act to the extent that the Director-General considers that they are consistent with the effective performance of ASIO's functions)). Two of these changes are discussed below.
Item 19 (new section 89 (voluntary moves to APS))	**Facilitating the transfer of an ASIO employee to the APS** This provision will apply the transfer provision in section 26 of the *Australian Public Service Act 1999* to ASIO employees as if they were APS employees and ASIO were an APS agency. It is consistent with similar provisions enacted for ASIS employees in the *Foreign Affairs Portfolio Miscellaneous Measures Act 2013* (in section 36A of the Intelligence Services Act).
Item 4 (new definitions of 'ASIO affiliate' and 'ASIO employee'	**New definitions of 'ASIO affiliate' and 'ASIO employee'** ***ASIO affiliate*** means a person performing functions or services for the Organisation in accordance with a contract, agreement or other arrangement, and includes a person engaged under section 85 and a person performing services under an agreement under section 87, but does not include the Director-General or an ASIO employee. ***ASIO employee*** means a person employed under section 84 or 90. The inclusion of two new definitions will consolidate various terminology used in the ASIO Act and across the Commonwealth statute book. An ASIO employee will be defined by reference to those persons employed under the new employment provisions, including new section 84 which sets out new employment provisions. Under the ASIO Act, non-employees, referred to as 'ASIO affiliates', may exercise ASIO functions and perform services for ASIO under a contract, agreement or other arrangement. ASIO affiliates may be able to exercise certain ASIO powers, if and when appropriately authorised to do so. The use of this term enables the imposition of appropriate limitations on the scope of ASIO affiliates' authority by excluding them from being able to exercise powers or where the Director-General has the ability to exclude certain ASIO affiliates, including classes of affiliates, from being able to engage in particular activities.

Schedule and Reference in Bill	Measures
Schedule 5: activities and functions of Intelligence Service Act agencies: Item 12 (amends subsection 14(2) of the Intelligence Services Act)	**Extends the immunity for actions preparatory or ancillary to an overseas activity of an Intelligence Services Act agency** Amendments are being made to the limited protection from liability to remove an anomaly in the application of the limited protection from liability from Australian laws under subsection 14(2) of the Intelligence Services Act. Currently, a person who assists an Intelligence Services Act agency inside Australia where that act is preparatory to, in support of, or otherwise directly connected with the proper performance of the Intelligence Services Act agencies' functions receives the protection. However, they would not receive that protection if they happened to provide that same assistance outside Australia. This is clearly anomalous and is not how the protection was intended to operate. This amendment will ensure that persons who assist the Intelligence Services Act agencies outside Australia are also provided with the same limited protection from Australian law where that act is preparatory to, in support of, or otherwise directly connected with the proper performance of the Intelligence Services Act agencies' functions. The people most likely to assist ASIS are officers from other Commonwealth agencies. The IGIS will continue to oversight the operation of section 14, and in any proceedings involving its operation, may certify any facts relevant to the question of whether an act was done in the proper performance of a function of an Intelligence Services Act agency.
Schedule 5: use of weapons in a controlled environment Item 16	**Clarifies that an ASIS staff member or agent can use a weapon or self-defence technique in a controlled environment in limited circumstances** ASIS staff members and agents are currently restricted from using weapons in a controlled environment, like a gun club, a firing range or a martial arts club, where it would be lawful for any other Commonwealth officer and/or member of the public to engage in that activity and where the use would otherwise be consistent with proper performance of an ASIS function. For example, there are circumstances where it would be common for members of the public and other Commonwealth officers to engage in these activities overseas. If an ASIS staff member is unable to participate, it creates a potential distinction between them and others, which risks drawing undue attention to them and their activities. There are a number of safeguards to limit the scope of authority and to facilitate effective independent oversight. The Guidelines issued by the Director-General of ASIS that are given to

Schedule and Reference in Bill	Measures
	the IGIS will set out the limited circumstances in which this amendment will operate – including that only ASIS staff members who have received appropriate familiarisation training would be able to engage in such activities. The IGIS will also continue to oversight ASIS's compliance with the Guidelines.
Schedule 6: protection of information	**Amends secrecy offences in relation to staff, employees or a person who has entered into any contract, agreement or arrangement with ASIO or an agency under the Intelligence Services Act or persons having been an employee or agent of a person who has entered into a contract, agreement or arrangement with ASIO or an agency under the Intelligence Services Act**, in three ways: o increases the penalties for the existing unauthorised communication offences in the ASIO Act and the Intelligence Services Act from two years' imprisonment to 10 years' imprisonment o extends the existing Intelligence Services Act disclosure offences to cover the Defence Intelligence Organisation and the Office of National Assessments and ensures that the offence covers any information or matter that was acquired, or prepared by, or on behalf of, ASIO or an agency under the Intelligence Services Act in connection with its functions or relating to the performance of its functions, and o creates new offences in relation to the intentional unauthorised dealings with records and the intentional unauthorised recording of information (with a maximum penalty of three years' imprisonment) (ie where the recording or dealing was not in the ordinary course of the person's duties of employment or terms of a contract or agreement or was not specifically directed by an authorised person within the agency). The reforms to the intelligence-specific secrecy offences in the ASIO Act and the Intelligence Services Act are necessary to address gaps identified in the coverage of existing offences. In particular, the reforms will strengthen Australia's capability to manage the risk of unauthorised disclosures by so-called 'trusted insiders'. These are persons who have access to intelligence-related information in the course of their official duties and who disclose or otherwise compromise it without authority. Members of intelligence agencies are in a unique position of trust, and receive information, often highly classified, for the purpose of performing official duties. They are made aware of the procedures for handling such information and their obligations to act in strict accordance with their authority at all times. Given this, there is a strong and legitimate expectation that these persons will handle that information lawfully at all times.

Schedule and Reference in Bill	Measures
	The offences are subject to a number of safeguards to ensure that their application is limited to serious instances of wrongdoing. For example, there is a requirement that the Attorney-General must consent to all prosecutions. There are also exemptions for persons who communicate information that is already in the public domain with the authority of the Commonwealth. Further, the prosecution must prove beyond reasonable doubt that the person intentionally undertook the relevant conduct (such as copying, removing or retaining a record) and the relevant conduct was not within their duties or was without authorisation. Importantly, the offences do not preclude a person from making a public interest disclosure in accordance with the *Public Interest Disclosure Act 2013* as it applies to intelligence agencies. This includes, for example, the ability to make a complaint to the IGIS. The offences similarly do not prevent a person from complying with a statutory notice to produce documents or provide information to the IGIS.
Schedule 7: renaming of Defence agencies **Enabling IGIS to report on AGO's compliance** Item 134 (amending subsection 35(2B) of the *Inspector-General of Intelligence and Security Act 1986*	**Renaming the Defence Imagery and Geospatial Organisation as the Australian Geospatial-Intelligence Organisation (AGO) and the Defence Signals Directorate as the Australian Signals Directorate** These amendments will rename the Defence Imagery and Geospatial Organisation as the Australian Geospatial-Intelligence Organisation (AGO) and the Defence Signals Directorate as the Australian Signals Directorate (ASD). While these agencies have been known by their updated names for some time, these amendments will place this on a statutory footing and will better reflect the national roles that those organisations play in support of Australia's security. **Enabling IGIS' reporting** This amendment will provide the IGIS with a specific function for the IGIS to report on the extent to which the AGO complies with rules made under section 15 of the Intelligence Services Act which is consistent with current practice.