2013-2014

THE PARLIAMENT OF THE COMMONWEALTH OF AUSTRALIA

SENATE

NATIONAL SECURITY LEGISLATION AMENDMENT BILL (NO. 1) 2014

EXPLANATORY MEMORANDUM

(Circulated by authority of the

Attorney-General, Senator the Honourable George Brandis QC)

NATIONAL SECURITY LEGISLATION AMENDMENT BILL (NO. 1) 2014

GENERAL OUTLINE

1. The Bill will modernise and improve the legislative framework that governs the activities of the Australian Intelligence Community (AIC), primarily the *Australian Security Intelligence Organisation Act 1979* (ASIO Act), and the *Intelligence Services Act 2001* (IS Act).

2. On 24 June 2013, the Parliamentary Joint Committee on Intelligence and Security's (PJCIS) *Report on Potential Reforms of Australia's National Security Legislation* was tabled. Chapter 4 of this Report identified a number of practical limitations in this legislation. The Bill implements the Government's response to the Committee's 22 recommendations on intelligence legislation reforms. It will modernise and strengthen the legislative framework for the AIC.

3. The Bill enhances the capability of our intelligence agencies in seven key areas:

- Modernising ASIO's 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, with 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 IS Act agencies (Schedule 5)
- Improving protection of intelligence-related information (Schedule 6), and
- Renaming of Defence agencies to better reflect their roles (Schedule 7).

FINANCIAL IMPACT STATEMENT

4. This Bill does not have a financial impact.

STATEMENT OF COMPATIBILITY WITH HUMAN RIGHTS

Prepared in accordance with Part 3 of the Human Rights (Parliamentary Scrutiny) Act 2011

National Security Legislation Amendment Bill (No. 1) 2014

This Bill is compatible with the human rights and freedoms recognised or declared in the international instruments listed in section 3 of the *Human Rights (Parliamentary Scrutiny) Act 2011*.

Overview of the Bill

1. The National Security Legislation Amendment (No. 1) Bill 2014 amends the *Australian Security Intelligence Organisation Act 1979* (the ASIO Act) and the *Intelligence Services Act 2001* (the IS Act) to implement the Government's response to recommendations in Chapter 4 of the Parliamentary Joint Committee on Intelligence and Security's (PJCIS) *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation* (tabled in June 2013) relating to reforms of the legislation governing the Australian Intelligence Community.

2. The Bill also contains some additional measures to update and strengthen the secrecy offences in the ASIO Act and the IS Act in relation to the intentional unauthorised communication, handling or treatment of intelligence-related information.

3. Improving these laws will better enable these agencies to respond to current and emerging threats to Australia's national security. It will also better protect the integrity of these agencies and the personal safety of their personnel and promote greater co-operation between these agencies.

4. Overview of Schedules:

- Schedule 1 modernises ASIO Act employment provisions to more closely align them with Australian Public Service (APS) standards, streamlines and simplifies terminology used to describe employment and other relationships and makes consequential amendments to a range of other Acts
- Schedule 2 modernises and streamlines ASIO's warrant based intelligence collection powers, including in relation to computer access warrants, surveillance devices and warrants against an identified person of security concern
- Schedule 3 provides ASIO employees and ASIO affiliates with limited protection from criminal and civil liability in authorised covert intelligence operations (referred to as 'special intelligence operations')
- Schedule 4 clarifies the ability of ASIO to co-operate with the private sector and enables breaches of section 92 of the ASIO Act, related to non-disclosure of identity obligations, to be referred to law enforcement agencies for investigation
- Schedule 5 amends the IS Act to enable Australian Secret Intelligence Service (ASIS) to undertake a new function of co-operating with ASIO in relation to the production of intelligence on Australian persons in limited circumstances, will create a new ground of Ministerial authorisation enabling ASIS to protect its operational security and will allow ASIS to train certain individuals in use of

weapons and self-defence techniques. It will also extend immunity for IS Act agencies for actions taken in relation to an overseas activity of the agency, provide a limited exception for use of a weapon or self-defence technique in a controlled environment and clarify the authority of the Defence Imagery and Geospatial Organisation (DIGO) to provide assistance

- Schedule 6 relates to the protection of intelligence-related information by creating two new offence provisions and updating existing offence provisions, including by increasing penalties in the IS Act and ASIO Act, and
- Schedule 7 provides for the renaming of DIGO as the Australian Geospatial Intelligence Organisation (AGO) and the Defence Signals Directorate (DSD) as the Australian Signals Directorate (ASD).

5. Overview of specific measures:

The Bill will improve and clarify aspects of the ASIO Act and IS Act through:

- updating ASIO Act employment provisions to more closely align them with the APS standards, providing for the secondment of staff to and from ASIO and facilitating the transfer of ASIO employees to APS agencies while protecting their identity
- improving ASIO's intelligence-collection powers by:
  - enabling it to obtain intelligence from a number of computers (including a computer network) under a single computer access warrant, including computers at a specified location or those which are associated with a specified person
  - amending the current limitation on disruption of a target computer
  - allowing ASIO to use third party computers and communications in transit to gain access to a target computer under a computer access warrant
  - modernising provisions related to surveillance devices to better align them with the *Surveillance Devices Act 2004* and improving their functionality and operation
  - establishing an identified person warrant for ASIO to utilise multiple warrant powers against an identified person of security concern
  - enabling warrants to be varied by the Attorney-General where minor changes in circumstances or administrative errors are identified
  - facilitating the Director-General of Security (Director-General) to authorise a class of persons able to execute warrants rather than listing individuals
  - clarifying that the search warrant, computer access, surveillance devices and identified person warrant provisions authorise access to third party premises to execute a warrant, and
  - clarifying that force which is necessary and reasonable to do things specified in the warrant may be used at any time during the execution of a warrant, not just on entry
- introducing an evidentiary certificate regime in relation to special intelligence operations and specific classes of warrants issued under Division 2 of Part III of

the ASIO Act to protect the identity of employees, sources and sensitive operational capabilities

- providing limited protection from criminal and civil liability for ASIO employees and affiliates, in relation to authorised special intelligence operations, subject to appropriate safeguards and accountability arrangements
- confirming ASIO's ability to co-operate with the private sector
- enabling breaches of section 92 of the ASIO Act (publishing the identity of an ASIO employee or affiliate) to be referred to law enforcement for investigation when it is not otherwise relevant to security
- enabling the Minister responsible for ASIS to authorise the production of intelligence on an Australian person who is, or is likely to be, involved in activities that pose a risk to, or are likely to pose a risk to, the operational security of ASIS
- enhancing the ability of ASIS, without a Ministerial authorisation, to co-operate with ASIO when undertaking less intrusive activities to collect intelligence relevant to ASIO's functions on an Australian person or persons overseas in accordance with ASIO's requirements
- enhancing the ability for ASIS to train staff members of a limited number of approved agencies that are authorised to carry weapons in the use of weapons and self-defence and ensuring that ASIS is not restricted in limited circumstances from using a weapon or self-defence technique in a controlled environment (such as a gun club or rifle range or martial arts club)
- clarifying the DIGO's authority to provide assistance to Commonwealth, State and Territory authorities (and certain non-government bodies and foreign governments approved by the Minister for Defence)
- extending the protection available to a person who does an act preparatory to, in support of, or otherwise directly connected with, an overseas activity of an IS Act agency to an act done outside Australia, and
- enhancing protections for information and records acquired or prepared by or for an intelligence agency in connection with the performance of its functions by:
  - updating sections 39, 39A and 40 in the IS Act, and increasing the penalties for existing unauthorised communication of information offences in the ASIO Act and the IS Act from two to ten years, to better reflect the culpability inherent in such wrongful conduct
  - extending the existing unauthorised communication offences in the IS Act to the Defence Intelligence Organisation (DIO) and the Office of National Assessments (ONA)
  - creating a new offence in the ASIO Act and the IS Act, punishable by a maximum of three years imprisonment, where a person intentionally deals with a record in an unauthorised way (for example, by copying, transcription, retention or removal), and
  - creating a new offence in the ASIO Act and the IS Act, punishable by a maximum of three years' imprisonment, in relation to persons who

intentionally make a new record of information or matter without authorisation.

Human rights implications

6. The Bill engages the following human rights:

- the right to work in Article 6 of the *International Covenant on Economic, Social and Cultural Rights* (ICESCR)
- the right to just and favourable working conditions in Article 7 of the ICESCR
- the right to freedom from arbitrary detention and the right to liberty of the person in Article 9 of the *International Covenant on Civil and Political Rights* (ICCPR)
- the right to freedom of movement in Article 12 of the ICCPR
- the right to a fair trial, the right to minimum guarantees in criminal proceedings and the presumption of innocence in Article 14 of the ICCPR
- the right to protection against arbitrary and unlawful interferences with privacy in Article 17 of the ICCPR
- the right to freedom of expression in Article 19 of the ICCPR, and
- 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* (CAT).

Schedule 1–Modernising ASIO Act employment provisions

7. This Schedule implements the Government's response to PJCIS Recommendation 26 to modernise employment provisions in the ASIO Act, including in relation to secondment arrangements. Part V of the Act remains largely in the same form it did when the ASIO Act was first enacted and has not kept pace with changes in terminology nor increasing flexibility across the Australian public sector. The amendments in this Schedule will update the ASIO Act employment provisions to more closely align them with the APS standards and streamline the use of terms across the statute book in relation to persons working with ASIO for clarity and simplicity.

Rights to work and to just and favourable conditions of work – Articles 6 and 7 of ICESCR

8. The Bill engages Article 6 of ICESCR which requires States Parties to recognise the right to work, including the right of everyone to the opportunity to gain their living by work which they freely choose or accept and take appropriate steps to safeguard this right. It also engages Article 7 of ICESCR which provides the right of everyone to the enjoyment of just and favourable conditions of work, including safe and healthy working conditions, rest, leisure and reasonable limitation of working hours and periodic holidays with pay.

9. New section 89 will create a mechanism for ASIO employees to move to an APS agency in the same way that APS employees can voluntarily transfer from one APS agency to another under section 26 of the *Public Service Act 1999* (PS Act). These amendments also ensure that an ASIO employee who moves to an APS Agency under section 26 of the PS Act will be an APS employee for all purposes. New provisions will also provide for both

the secondment of ASIO employees to other bodies or organisations and secondment of persons to ASIO which will provide ASIO with greater flexibility and ASIO employees with greater job mobility (see new sections 86 and 87).

10. These changes are supported by a new section 88 that clarifies that, although ASIO employees are not employed under the PS Act, the Director-General must adopt the principles of that Act to the extent that he or she considers that they are consistent with the effective performance of the functions of ASIO. Further, new section 84 will allow for the employment practice of employment at a level and salary to ensure consistency with the PS Act.

11. These amendments promote the right to work and rights in work in Articles 6 and 7 of the ICESCR by making it easier for ASIO employees to meet their legal obligations under the ASIO Act not to disclose their relationship and broadening mobility opportunities for ASIO employees in the APS, by placing them in an equivalent position as other APS employees. Similar provisions were enacted in relation to ASIS employees in the *Foreign Affairs Portfolio Miscellaneous Measures Act 2013*.

Other amendments

12. The Bill will also streamline the terminology for persons in a form of employment relationship or arrangement with ASIO by the creation of two categories, being 'ASIO employee' and 'ASIO affiliate' (section 4). Reflecting the removal of the concept of office, it also alters the definition of 'Deputy Director-General' and creates a 'senior-position holder' (section 4). Consistent with these changes, the Schedule also makes a number of amendments to terminology used in other Acts. These are minor and technical amendments and do not have any human rights implications.

Schedule 2–Improving ASIO's powers including in relation to warrants

13. This Schedule of the Bill will implement the PJCIS's Recommendations 20 to 23, 29 to 32 and 35 and 36 by streamlining and improving the warrant provisions in Division 2 of Part III of the ASIO Act. Many of the powers set out below already exist in this Division.

14. The Schedule will amend sections 22 and 25A of the ASIO Act to include multiple computers operating in a network in the definition of 'computer' and to enable the target computer of a computer access warrant to extend to all computers at a specified location and all computers associated with a specified person. It will also amend the computer disruption limitations currently contained in subsections 25(6) and 25A(5) and section 25A to enable the use of a third party computer or communication 'in transit' for the purpose of accessing data on the target computer (new Subdivision C).

15. The Schedule will also modernise provisions in sections 26 to 26C of the ASIO Act related to surveillance devices to better align them with the *Surveillance Devices Act 2004* (Surveillance Devices Act) (section 4 and new Subdivision D) including new provisions providing for the use of a listening device, an optical surveillance device and a tracking device without a warrant (new sections 26C, 26D and 26E). The Director-General may exclude ASIO affiliates from exercising powers under these new provisions, to provide a safeguard as to who is appropriate to exercise these powers (new section 26F).

16. The Schedule will also create a new identified person warrant for ASIO to utilise multiple warrant powers against an identified person of security concern (new Subdivision G) and enable all of the types of warrants to be varied by the Attorney-General where changes in circumstances or administrative errors are identified (new section 29A). It also amends the provisions in section 27A of the ASIO Act in relation to warrants for the function of obtaining within Australia foreign intelligence.

17. It will also allow the Director-General to authorise a class of persons able to execute warrants rather than listing individuals (section 24), clarify that search warrants, computer access warrants and surveillance device warrants authorise access to third party premises to execute a warrant (sections 25, 25A and new section 26B), that reasonable force may be used at any time during the execution of a warrant, not just on entry (sections 25, 25A, 26A, 26B and 27J) and creates a new evidentiary certificate regime (new section 34AA).

Computer access warrants

18. The Schedule modernises the definition of 'computer' to address contemporary situations by enabling it to include a computer network, covers common situations where individuals are associated with multiple computers or networks and ensures that ASIO is able to obtain intelligence from a number of computers or networks under a single computer access warrant. The Schedule also expands what can be covered by the target computer of a computer access warrant to include any combination of one or more computers, computers on particular premises and computers associated with a specified person. The Schedule also amends section 25A so that ASIO will be able to use a third party computer or communication in transit (and add, copy, delete or alter data in the third party computer or communication in transit) for the purpose of obtaining access to data relevant to the security matter and held on the target computer. ASIO may only do so where it is reasonable in all the circumstances, having regard to other methods of obtaining access to the data which are likely to be as effective. ASIO will not be able to use third party computers or communications in transit for any other purpose.

19. It also amends the current limitation contained in subsection 25A(5) in respect of activities that disrupt or cause loss or damage to a computer. The limitation is extended to cover third party computers and communications in transit. The modified limitation also provides that a computer access warrant does not authorise the addition, deletion or alteration of data, or the doing of any thing that is likely to materially interfere with, interrupt or obstruct a communication in transit or the lawful use by other persons of a computer. An exception to the limitation has been included so that ASIO may undertake such actions where they are otherwise necessary to execute the warrant, such as those things set out in paragraph 25A(4)(a), including the deleting or altering of data, where to do so is necessary. The modified limitation also provides that a computer access warrant does not authorise the addition, deletion or alteration of data, or the doing of any thing that is likely to cause any other material loss or damage to other persons lawfully using a computer. Similar changes are also made to the limitation in the search warrant provisions in subsection 25(6) in respect of access to computers found on the premises being searched.

20. A new provision is also inserted to clarify the relationship between the computer access warrant provisions in section 25A and the *Telecommunications (Interception and Access) Act 1979* in order to align the safeguards under the ASIO Act with those in that Act.

For example, in the event that ASIO seeks to intercept communications, it will need to apply for a warrant under the TIA Act (unless otherwise exempted under the TIA Act).

Identified person warrants

21. The Schedule will establish an 'identified person warrants' scheme targeting a particular identified person, which will enable the Director-General to request that the Minister issue a single warrant authorising the exercise of multiple powers (IPWs). The Minister must be satisfied that the 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 the warrant in relation to the person, will, or is likely to, substantially assist the collection of intelligence relevant to security.

22. The warrant must specifically provide approval for ASIO to do one or more of the following things: access records or things in or on premises or data held on computers, use one or more kinds of surveillance devices and or access postal or delivery service articles. IPWs establish a single issuing process that will ensure the simultaneous availability of all powers sought under different types of warrants, while retaining the statutory thresholds for the issuing of individual types of warrants. Separate authorisation requirements will continue to apply to the issuing of these warrants and the exercise of particular powers under them. IPWs will be for a maximum duration of six months and the Minister may impose restrictions or conditions.

23. Powers under these warrants will include inspecting, copying or transcribing records, use of computers or other equipment to access data, associated powers to search for, inspect and copy records and acts reasonably incidental to exercising these powers and acts necessary to conceal the execution of powers under the warrant. Records can only be retained for as long as is reasonable unless the return of such records would be prejudicial to security. Computers can also be accessed where the Minister has approved such powers under the identified person warrant. Under an authority under an IPW for a computer access, similar types of powers apply as they do with a computer access warrant, similarly for an authority under an IPW in relation to surveillance, for the purposes of a surveillance devices warrant. Searches of a person who are on or near premises being searched can also be conducted, and if so, must (if practicable) be conducted by a person of the same sex. Strip searches and body cavity searches are prohibited. These are important human rights safeguards.

24. Two new provisions, sections 27G and 27H, set out the requirements for inspecting a postal or delivery service article under an IPW where the Attorney-General has conditionally approved the use of such powers. The Minister or Director-General can authorise the exercise of these powers in a particular instance if they are satisfied on reasonable grounds that this would substantially assist in the collection of intelligence relevant to the prejudicial activities of the identified person – for example, when the post is addressed to the person or posted by them. Relevant powers include inspecting and making copies of the articles or their contents.

25. Safeguards in relation to the authorisations to exercise powers under IPWs where conditional approval has been given by the Minister include that the Minister may impose restrictions or conditions, there must be particularisation of the subject premises or target computers, a higher threshold will apply to the issuing of an IPW than for individual warrants, the period for which search powers can be authorised is 90 days and the period

under authorisations cannot extend beyond the timeframe of the warrant itself. The time of which entry is permitted must also be specified, if entry to premises is authorised.

Surveillance devices warrants

26. The Schedule will enable a more appropriate alignment of the surveillance device provisions with the Surveillance Devices Act and to improve their functionality and operation, including creating a new definition of a 'surveillance device'. Surveillance device warrants may be issued in relation to one or more particular persons, particular premises or an object or class of object. They may also be issued in respect of multiple kinds of surveillance devices and in respect of multiple surveillance devices. In issuing these warrants, the Minister must be satisfied that the person or persons 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, that the premises is used, likely to be used or frequented by such a person, or the object or objects are used or worn, or likely to be used or worn by such a person and that the use of a surveillance device will, or is likely to, assist ASIO in carrying out its functions of obtaining intelligence. The warrant can only be in force for up to the maximum of six months.

27. The warrant will set out a range of authorised activities that can be taken in relation to a particular person, particular premises or an object or class of object. This includes the installation, use and maintenance of a surveillance device, entering premises including third party premises, altering objects and surveilling a person. It also sets out the powers of recovery of surveillance devices.

28. Consistent with the Surveillance Devices Act, the new provisions provide for the use of a listening device and an optical surveillance device without a warrant. The Director-General may determine that ASIO affiliates should not exercise powers under these new provisions (new section 26F).

Foreign intelligence warrants

29. The Schedule also makes a number of amendments, many of them minor and technical, to align the existing provisions relating to foreign intelligence warrants with the amended provisions for security intelligence warrants.

Right to protection against arbitrary and unlawful interferences with privacy – Article 17 of the ICCPR

30. These provisions engage the right to protection against arbitrary and unlawful interferences with privacy in Article 17 of the ICCPR. Article 17 of the ICCPR provides that no-one shall be subjected to arbitrary or unlawful interference with their privacy, family, home or correspondence. The use of the term 'arbitrary' means that any interference with privacy must be in accordance with the provisions, aims and objectives of the ICCPR and should be reasonable in the particular circumstances. The United Nations Human Rights Committee interpreted 'reasonableness' to imply that any limitation must be proportionate and necessary in the circumstances.

31. The exercise of powers under warrants engages the right to protection against arbitrary and unlawful interferences with privacy. These powers enable ASIO to exercise a

wide range of powers such as entering and searching people's homes and places of business, searching a person on or near specified premises, accessing their computer or computers at their workplace or computers of friends and associates at their premises, interfering with data and using surveillance devices to record, listen to or track a person.

32. ASIO's warrant-based powers will remain subject to significant safeguards which ensure that these powers are used consistently with the right to protection against arbitrary and unlawful interferences with privacy. Safeguards include the high thresholds prescribed by the statutory criteria for the issuing of warrants and the exercise of powers under them, Ministerial-level issuing decisions, and the independent oversight role of the Inspector-General of Intelligence and Security.

33. 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)* (the Attorney-General's Guidelines), issued under section 8A of the ASIO Act require ASIO, in the conduct of its inquiries and investigations, to ensure that the means used to obtain information are proportionate to the gravity of the threat posed and the probability of its occurrence. The more intrusive the investigation technique, the higher the level of officer required approving its use and wherever possible, the least intrusive techniques of information collection should be used before more intrusive techniques.

34. Further, in conducting inquiries and investigations into individuals and groups, ASIO should do so with as little intrusion into individual privacy as is possible consistent with the performance of its functions, with due regard for the cultural values, mores and sensitivities of individuals of particular cultural or racial backgrounds, consistent with the national interest. Additionally, ASIO only requests the issuing of warrants after considering the application of the Attorney-General's Guidelines, including the requirement that the use of powers under warrant is appropriate.

35. If the Director-General is satisfied that grounds on which a warrant was issued under Division 2 cease to exist, as soon as practicable, he or she must take steps to inform the Attorney-General and ensure that action under the warrant is discontinued. If a surveillance device warrant is issued in relation to a combination of a person, premises, and an object under paragraph 26(2)(a) and the Director-General is satisfied that the grounds on which the warrant was issued continue to apply to at least one of those matters, the obligation to discontinue action and notify the Attorney-General applies only in relation to the matters for which the grounds have ceased to exist.

36. The IGIS has broad powers under the *Inspector-General of Intelligence and Security Act 1986* (IGIS Act) to inquire into any matter relating to compliance by ASIO with laws of the Commonwealth, the States and Territories or with directions or guidelines issued by the responsible minister, the propriety of its actions and the effectiveness and appropriateness of procedures relating to legality or propriety, at the request of the responsible Minister, on his or her own motion or in response to a complaint. The IGIS has particularly strong powers to compulsorily obtain information and documents and enter premises, as well as obligations to provide procedural fairness. After completing an inquiry, the IGIS must complete a report.

37. These measures will ensure that interferences with privacy under warrants are reasonable, necessary and proportionate to achieving the outcome of protecting national security.

Authorisations of classes of person

38. The Schedule will enable the Director-General (or another person appointed by the Director-General) to authorise a class of persons to exercise powers under a warrant, not simply an individual. This will provide the Organisation with flexibility to encompass a broad range of appropriate persons to exercise powers under a warrant or request information or documents from operators of aircraft or vessels. This is a technical amendment and will not make any substantive changes to the operation of the ASIO Act and on this basis, does not engage any human rights obligations.

Use of reasonable and necessary force

39. The Schedule will clarify that the use of reasonable and necessary force provided for in current paragraphs 25(7)(a), 25(5A)(a) and 27A(2)(a) of the ASIO Act may be used at any time during the execution of a warrant, not just on entry, when it is authorised in the warrant. In the course of executing a warrant, it may be necessary to use force to obtain access to a thing on the premises, such as a door or cabinet lock or to use force to install or remove a surveillance device. The use of force would extend to using reasonable and necessary force against a person in situations where a person tries to obstruct the execution of a search warrant, for example.

Right to security of the person – Article 9 of ICCPR

40. The right to security of the person in Article 9 of the ICCPR requires States to provide reasonable and appropriate measures, within the scope of those available to public authorities, to protect a person's physical security. The use of reasonable and necessary force in executing a warrant can engage the right to security of the person where force could be used against a person in circumstances where it is legally authorised and is reasonable and necessary. In most cases, police officers accompany ASIO when undertaking searches and the police would exercise the power to use reasonable force against a person where it was both reasonable and necessary for the purposes of executing the warrant. Any use of force in accordance with these provisions would be lawful and would not be arbitrary as it would be reasonable and necessary in the particular circumstances. In these circumstances, it would also be proportionate. However, if any use of force was either not reasonable or not necessary, the ordinary criminal law would apply.

Access to third-party premises

41. The Schedule will include in the list of authorised activities that may be specified, in a warrant that authorises entry to premises, entry to any premises for the purpose of gaining entry to or exiting the subject premises. This clarifies ASIO's powers in situations where, because there is no other way to gain access to the target premises, for example, in an apartment complex, it may be necessary to enter the premises through shared or common premises. It may also occur where, for operational reasons, entry through adjacent premises is more desirable, such as where entry through a main entrance may involve a greater risk of detection.

Right to protection from arbitrary and unlawful interferences with privacy – Article 17 of the ICCPR

42. Article 17 of the ICCPR provides that no-one shall be subjected to arbitrary or unlawful interference with their privacy, family, home or correspondence. Any limitation on this right must be consistent with the provisions, aims and objectives of the ICCPR and proportionate and necessary in the circumstances.

43. Clarifying the existing regime to make clear the right of access to third-party premises will engage the right to protection against arbitrary and unlawful interferences with privacy in Article 17 of the ICCPR as it will enable ASIO to interfere with other persons' privacy by entering their home. These measures are authorised by law and will not be arbitrary as any interference will be limited to access that is necessary to ensure the efficient exercise of a warrant that authorises entry to premises. On this basis, these measures are reasonable, necessary and proportionate limitations.

Enabling the Attorney-General to vary the warrant where there are changes in circumstances

44. The Schedule will enable the Attorney-General to vary warrants. This is particularly important in situations where there is an administrative error or a change in circumstances. A warrant cannot be varied to extend the total period for which it is in force beyond 90 days for search warrants, and beyond a total period of six months for all other warrants issued by the Attorney-General under Division 2 of Part III. The Director-General's request must set out the relevant facts and grounds supporting the variation request. This is a technical matter and does not engage any human rights obligations.

Evidentiary certificates

45. The Schedule will enable evidentiary certificates to be issued under new section 34AA in relation to acts done by, on behalf of, or in relation to ASIO in connection with any matter in connection with a warrant issued under section 25A, 26, 27A, 27C or 29 or in accordance with subsection 26B(5) or (6), section 26C, 26D or 26E or subsection 27A(3A) or (3B) or 27F(5). Certificates are to be prima facie evidence of the matters stated in the certificate (that is, certificates issued under the regime will be persuasive before a court, as distinct from a conclusive certificate that cannot be challenged by a court or a defendant).

46. The regime is framed to ensure that an evidentiary certificate will only cover the manner in which the evidence was obtained and by whom but not the evidence itself. As such, the court will retain its ability to test the veracity of evidence put before it.

47. For operational security reasons, the proposed regime does not provide a conclusive list of the facts that the Director-General or a Deputy Director-General may include in an evidentiary certificate. The regime is not intended to provide a means for the prosecution to provide proof of any ultimate fact, or any fact so closely connected certificate. The regime is not intended to provide a means for the prosecution to provide proof of any ultimate fact, or any fact so closely connected with an ultimate fact so as to be indistinguishable from it, or facts that go to elements of the offence, without recourse for the course or the defendant to challenge the certificate and the facts it covers.

Right to a fair hearing – Article 14 of ICCPR and presumption of innocence – Article 14(2) of ICCPR

48. Article 14 of the ICCPR provides that in the determination of obligations in a suit at law, everyone shall be entitled to a fair and public hearing by a competent, independent and impartial tribunal established by law. The term 'suit at law' includes civil proceedings. This right can be permissibly limited provided that those limitations are reasonable, necessary and proportionate for achieving a legitimate objective.

49. Article 14(2) of the ICCPR provides that everyone charged with a criminal offence shall have the right to be presumed innocent until proved guilty according to law. However, such a limitation will be permissible when it is reasonable in the circumstances.

50. The Bill engages the right to a fair hearing and the presumption of innocence as an evidentiary certificate scheme creates a presumption as to the existence of the factual basis on which the certificate is issued which requires the defendant to disprove the matters certified in the evidentiary certificate if they seek to challenge them. In this case, these will only be details of sensitive information such as how the evidence was obtained and by whom but will not seek to establish the weight or veracity of the evidence itself. New section 34AA is based upon similar regimes operating under the *Telecommunications (Interception and Access) Act 1979* and the Surveillance Devices Act.

51. An accused person would not be prevented from leading evidence to challenge a certificate issued under the proposed section 34AA – he nature of a prima facie evidence certificate regime provides an ability for the accused to seek to establish 'illegality' – that is, to seek to establish that acts taken in order to give effect to a warrant contravened the ASIO Act should they choose to do so within the boundaries of the judicial framework, an put the party bringing the proceedings to further proof. However, regardless of the evidentiary certificate regime, the prosecution will still have to make out all elements of any offence that a person may be charged with.

52. For these reasons, the new evidentiary certificate provision engages, but does not limit, the right to a fair trial and the presumption of innocence.

Schedule 3 – Protection for Special Intelligence Operations

53. This Schedule implements the Government's response to Recommendation 28 of the PJCIS's Report by amending Part III of the ASIO Act to insert a new Division 4 which establishes a statutory framework for the conduct by ASIO of special intelligence operations (SIOs). This is similar to the controlled operations regime in Part IAB of the *Crimes Act 1914* (Crimes Act) in relation to activities of the Australian Federal Police, with appropriate modifications to reflect the discrete purposes to which SIOs and controlled operations are directed, being (respectively) the collection of intelligence for national security purposes, as opposed to the gathering of evidence in relation to serious criminal offences for law enforcement purposes.

54. Currently, some significant investigations either do not commence or are ceased due to the risk that an ASIO employee or ASIO affiliate, using the new terms in the Bill, could be exposed to criminal or civil liability. These amendments will ensure that ASIO can collect

relevant intelligence by ensuring its capacity to gain close access to sensitive information via covert means.

55. As the PJCIS recognised, a legislative framework for the conduct of SIOs is necessary to ensure that ASIO employees and affiliates will have appropriate legal protections if it is necessary to engage in authorised, covert activities and operations that involve otherwise unlawful conduct for the legitimate purpose of carrying out functions in accordance with the ASIO Act. For example, it is an offence under section 102.5 of the Criminal Code for a person to intentionally provide training to, or receive training from, a terrorist organisation where the person is reckless as to the organisation's status as a terrorist organisation. If an ASIO employee or affiliate is required to collect covert intelligence in relation to a terrorist organisation or its members, they may be exposed to criminal liability under section 102.5 if, in the course of collecting the relevant intelligence, they receive training from that organisation.

56. These activities can involve engaging and associating with those who may be involved in criminal activity and can expose ASIO employees or affiliates to criminal or civil liability in the course of their work. This includes capturing conduct ancillary to this conduct to prevent an arbitrary distinction in the treatment of participants in a SIO and persons who are required as part of their official duties to assist in, or support, a SIO.

57. While, in the absence of a limited statutory immunity, any commencement or continuation of a prosecution would be dependent on the exercise of prosecutorial discretion, a limited immunity is, as a matter of policy, considered preferable to prosecutorial and investigative discretion alone. The establishment of an appropriately limited statutory immunity removes the possibility that conduct in accordance with an authorised SIO could be investigated or referred for prosecution. A limited immunity, in the form of the SIO regime in new Division 4, is also considered preferable to the potential alternative of conferring upon SIO participants a wholesale immunity from criminal liability. Limiting the immunity to specifically authorised conduct in particular operations will ensure that it is enlivened only where a case has been established for its application.

58. Broadly, the scheme provides for the following elements:

- providing protection to a participant in an authorised SIO from civil and criminal liability in limited circumstances
- providing statutory guidance in the exercise of this discretion in relation to the admission in evidence in judicial proceedings of information obtained as part of a SIO
- allowing for a certificate to be issued under the scheme to create a rebuttable presumption as to the existence of the factual basis on which the criteria for issuing a SIO were satisfied, and
- creating two new offences, one being an aggravated offence, in relation to the unauthorised disclosure of information relating to a SIO. The maximum penalties for the offences are five and ten years imprisonment respectively. These offences also contain defences – including disclosures pertaining to the operation of the SIO scheme in new Division 4 or legal proceedings relating to Division 4, other legal obligations of disclosure and disclosures for the purpose of the performance by ASIO of its statutory functions.

59. A SIO is an operation that is carried out for a purpose related to the performance of one or more special intelligence functions (as defined in section 4) which may involve an ASIO employee or ASIO affiliate engaging in special intelligence conduct. Special intelligence functions are limited to four listed purposes relevant to ASIO's intelligence-gathering functions in section 17 of the ASIO Act. ASIO's advisory functions are excluded from the definition. While it is intended that any relevant information obtained from a SIO may be used for the performance of ASIO's advisory functions, it is not considered necessary for a SIO to be authorised specifically for these purposes.

60. Only the Director-General or a Deputy Director-General may grant a SIO authority. The issuing criteria include that the circumstances justify the conduct specified in the application, that the SIO will limit to the maximum extent possible unlawful conduct, that the SIO will not be conducted in such a way that a person is likely to be induced to commit an offence against a Commonwealth law or a State or Territory law that the person would not otherwise have intended to commit and the conduct will not cause death or serious injury to any person, or involve the commission of a sexual offence against any person, or result in significant loss of property or serious damage to property. The maximum duration for an authority is twelve months. This ensures that any limited immunities granted are proportionate to the intelligence-collection purposes to which they are directed, and do not extend beyond this.

61. Special intelligence conduct is that which is specified within a SIO authorisation. The scope of authority is particularised and appropriately limited. For example, conduct permitted to be authorised under a SIO cannot include that which would require authorisation under a warrant issued under the ASIO Act or a warrant or authorisation under the TIA Act. If conduct requires a warrant or authorisation, it will be necessary for ASIO to obtain a warrant or authorisation. The SIO scheme cannot be used in substitution of existing requirements in this respect. Immunity from liability applies exclusively to conduct engaged in as part of a SIO that is authorised and carried out in accordance with the legislative requirements. Only a 'participant' in a SIO will be granted limited protection from criminal and civil liability, being a person authorised to engage in special intelligence conduct. This definition ensures that both the SIO and an individual person's conduct must be authorised specifically in the SIO authority. Such authorisation cannot be granted retrospectively.

62. The scheme also enables the authorising officer (the Director-General or a Deputy Director-General) to impose any additional conditions for the application of immunity if he or she considers it appropriate to do so. Accordingly, a participant, or participants in a SIO generally, may be held to an even higher standard of conduct than that which is required under the above conditions.

63. The scheme also provides protection from criminal liability for a person connected with a SIO but who is not necessarily an authorised participant in the SIO, if that person has a belief that the activities in which they are engaging are ancillary to the authorised conduct of a participant in a SIO. It does so by establishing a limited immunity in respect of conduct that constitutes an 'ancillary offence' to the conduct of a SIO participant that would otherwise have constituted an offence. However, the person must be proven at the time to believe, at the time of engaging in the ancillary conduct, that the related conduct of the SIO participant was part of an authorised SIO.

64. An ancillary offence is defined as an offence against the law of the Commonwealth or of a State or Territory, consisting of conspiring to commit the offence constituted by the related conduct, or aiding, abetting, counselling or procuring, inciting or being in any way knowingly concerned in, the commission of the offence constituted by the related conduct. These provisions will, for example, have the effect of protecting persons who are required as part of their official duties to assist in, or support, a SIO.

65. The Division only has a prospective application. This is so even if an existing covert operation is later the subject of a SIO authority in accordance with the provisions of Division 4, once those provisions have commenced. Importantly, the provisions do not protect from liability intelligence conduct which would otherwise be unlawful prior to the commencement of the Division.

Right to an effective remedy – Article 2 of ICCPR and right to a fair trial – Article 14(1) of ICCPR

66. Article 2 of the ICCPR provides that States Parties should ensure that any person whose rights or freedoms in the ICCPR are violated must have an effective remedy, notwithstanding that the violation has been committed by persons acting in an official capacity and that right should be determined by competent authorities provided for by the legal system of the State. The right to property is not protected by the seven core human rights treaties but the right to security of the person is provided in Article 9 of the ICCPR.

67. Article 14(1) of the ICCPR provides that in the determination of obligations in a suit at law, everyone shall be entitled to a fair and public hearing by a competent, independent and impartial tribunal established by law.

68. The Bill engages the right to an effective remedy and a fair trial by providing an immunity, including immunity for ancillary conduct, in limited circumstances, for conduct that could otherwise found a criminal charge or a suit at law. It does so where that conduct is performed in accordance with specific authorisations for ASIO employees and ASIO affiliates who are engaged in authorised, covert activities and operations for the legitimate purpose of collecting useful and relevant intelligence on most serious threats to the security of Australia and Australians. This immunity does not extend to more serious offences against the person or property, or conduct that causes serious injury, loss or damage. It also excludes conduct that intentionally induces another person to commit an offence against the laws of the Commonwealth or a State or Territory that the person would not otherwise have intended to commit. Accordingly, the immunity does not preclude an individual from commencing proceedings in tort (or under another civil cause of action) against the participant (and the Commonwealth) in relation to serious injury, loss or damage. Participants in an SIO who engage in such conduct may also be liable to criminal prosecution.

69. There are a number of safeguards to the scheme. These include the high level of authorisation required for SIOs, being the Director-General or the Deputy-Director General, the exclusion of a range of offences for which immunity will be available, reporting requirements and the commencement provisions. It is subject to strict reporting requirements to both the Attorney-General and the IGIS and as part of ASIO's annual report. The IGIS has existing powers under the IGIS Act to examine ASIO's activities in regards to SIOs and the PJCIS's mandate includes conducting inquiries in relation to such activities on a reference from the Attorney-General or on a resolution of either House of Parliament.

70. The scheme is necessary to ensure the effective performance of the statutory functions of ASIO. Not providing these immunities would impair ASIO's capabilities to ensure a safe and secure Australia and expose individuals to liability for necessarily participating in actions to fulfil their role with regards to ASIO. There is also effective independent oversight of the entirety of the scheme. Of particular importance, at her discretion, the IGIS can recommend that ASIO pay compensation to a person in appropriate cases, such as persons who are unable to commence civil proceedings against ASIO through the operation of the immunity provision.

71. The limitation to the right to an effective remedy and a fair hearing is only limited to the extent that it is reasonable, necessary and proportionate to achieve the objective of facilitating the fulfilment of ASIO's statutory functions, including the gathering of intelligence on serious threats to the security of Australia and Australians. Complaints can be brought to the IGIS about the actions of the ASIO and the IGIS can recommend how ASIO should respond to these complaints if they are determined to be well-founded. Further, the general immunity provisions do not provide blanket immunity from Australian laws for all acts of ASIO.

New offences

72. The Schedule will create two new offences relating to the unauthorised disclosure of information relating to a SIO, one being an aggravated offence, with penalties of five and ten years imprisonment. The relevant aggravating elements are an intention of endangering the health or safety of any person, or prejudicing the effective conduct of a SIO or that the disclosure will endanger the health or safety of any person or prejudice the effective conduct of a SIO. The offences apply to disclosures by any person, including for example, participants in a SIO, other persons to whom information about a SIO has been communicated in an official capacity and persons who are the recipients of an unauthorised disclosure of information. The offences have statutory defences – including disclosures pertaining to the operation of Division 4 or legal proceedings relating to Division 4, other legal obligations of disclosure and the performance by ASIO of its statutory functions.

Right to a fair trial – Article 14(1) of the ICCPR, right to freedom from arbitrary detention – Article 9 of ICCPR, the prohibition on cruel, inhuman or degrading treatment or punishment in Article 7 of ICCPR and the CAT and right to freedom of movement – Article 12 of ICCPR

73. In addition to security of the person, Article 9 of the ICCPR also provides that no-one shall be subjected to arbitrary arrest or detention or deprived of their liberty except on such grounds and in accordance with such procedure as are established by law. The UN Human Rights Committee has stated that 'arbitrariness' includes the elements of inappropriateness, injustice and a lack of predictability. An arrest or detention must be reasonable and necessary in all circumstances with reference to the recurrence of crime, interference with evidence or the prevention of flight.

74. Article 12 of the ICCPR provides that everyone lawfully within the territory of a State shall, within the territory, have the right to liberty of movement. This right can be permissibly limited if the limitations are provided by law, are necessary to protect national security or the rights and freedoms of others and consistent with the other rights in the ICCPR.

75. Article 7 of the ICCPR and the CAT prohibit conduct which may be regarded as cruel, inhuman or degrading treatment or punishment ('ill treatment') and can be either physical or mental. The UN treaty bodies responsible for overseeing the implementation of these treaties have provided guidance on the sort of treatment that is prohibited. Examples of cruel, inhuman or degrading treatment include unduly prolonged detention that causes mental harm. Punishment may be regarded as degrading if, for instance, it entails a degree of humiliation beyond the level usually involved in punishment. These rights are absolute and cannot be limited in any way.

76. The Bill engages the rights to a fair trial, freedom from arbitrary detention, protection from cruel, inhuman or degrading treatment or punishment and freedom of movement on the basis that it creates these new offences with maximum penalties of five and ten years imprisonment.

77. Penalties of five and ten years imprisonment are not so significant that they would constitute arbitrary detention or cruel, inhuman or degrading treatment or punishment. Persons participating in a SIO do so on explicit and strict conditions that are additional to any other obligations applying to an ASIO affiliate or employee and are potentially subject to greater risks should information pertaining to an SIO be disclosed. The penalties implement a gradation consistent with established principles of Commonwealth criminal law policy, as documented in the *Guide to Framing Commonwealth Offences, Infringement Notices and Enforcement Powers*. The Guide provides that a heavier maximum penalty is appropriate where the consequences of an offence are particularly dangerous or damaging.

78. The penalty of maximum 5 years imprisonment applying to the primary offence reflects an appropriate gradation with new offences inserted by the Bill regarding unauthorised dealing. Those offences carry a maximum 3 year penalty. The unauthorised disclosure of information regarding a SIO is considered more culpable than the unauthorised dealing with information pertaining to ASIO's statutory functions.

79. The penalty of maximum 10 years imprisonment applying to the aggravated offence maintains parity with the penalty applying to the offence of unauthorised communication of records as amended by this Bill. The heavier penalty is appropriate considering the level of harm, both in the intentional or actual jeopardising of the safety of participants and in potentially limiting ASIO's intelligence gathering capability by compromising the integrity of the operation.

80. On this basis, these penalties are both appropriate and necessary in order to protect sensitive information.

Right to presumption of innocence – Article 14(2) of ICCPR

81. Article 14(2) of the ICCPR provides that everyone charged with a criminal offence shall have the right to be presumed innocent until proved guilty according to law. The presumption of innocence may be limited when an evidential burden is placed on the accused. However, such a limitation will be permissible when it is reasonable in the circumstances, such as where it relates to matters peculiarly in the knowledge of the defendant, and the law maintains the rights of the accused.

82. The Bill imposes an evidential burden on the accused in respect of the exception to the unauthorised disclosure of information relating to a SIO in relation to the offence-specific

defences. An evidential burden is created by confirming the application of subsection 13.3(3) of the Criminal Code which provides that a defendant who wishes to rely on any exception provided for by a law creating an offence bears an evidential burden in relation to that matter. Placing an evidential burden on the defendant in these circumstances is common practice with regards to existing secrecy offences, as illustrated in Division 91 of the Criminal Code. This is attributable to the nature of the exception in this type of offence.

83. Evidence suggesting a reasonable possibility of the authorised nature of the disclosure is readily available to the accused, who would have had such authority, or perceived such authority, in contemplation at the time he or she disclosed the relevant information. The requisite threshold applying to a 'reasonable possibility' as to the existence of a matter is relatively low. An element of the offence requiring the prosecution to prove, beyond reasonable doubt, that disclosure was not made pursuant to any of the available defences would impose a disproportionate burden on the prosecution.

84. In addition, the burden placed on the defendant is evidential only. The legal burden remains upon the prosecution to negate the possibility, once the evidential burden is discharged by the defendant. Hence, the imposition of an evidential burden on a defendant simply defers the point at which the prosecution must discharge the legal burden.

85. On this basis, the limitation on the right to the presumption of innocence is reasonable, necessary and proportionate to achieving the legitimate objective.

Evidentiary certificates

86. The Schedule will enable an authorising officer (being the Director-General or the Deputy Director-General) to issue an evidentiary certificate in relation to the factual basis for the granting of the SIO authority. This is treated as prima facie evidence of the matters in the certificate in any proceeding (federal or state judicial hearing or any administrative proceeding including tribunals or any other body, authority or person having the power to hear or examine evidence). A certificate creates a rebuttable presumption as to the existence of the facts contained in the certificate.

Right to a fair hearing – Article 14 of ICCPR and presumption of innocence – Article 14(2) of ICCPR

87. Article 14 of the ICCPR provides that in the determination of obligations in a suit at law, everyone shall be entitled to a fair and public hearing by a competent, independent and impartial tribunal established by law. Article 14(2) of the ICCPR provides that everyone charged with a criminal offence shall have the right to be presumed innocent until proved guilty according to law.

88. The Bill engages the right to a fair hearing and the presumption of innocence as an evidential certificate scheme means that the information in a certificate is taken to be prima facie evidence of the matters set out therein. This means that a party to any proceedings in which a certificate is tendered may, if desired, adduce evidence to challenge the matters in the certificate. However, the new evidentiary certificate scheme does not limit the right to a fair hearing or the presumption of innocence as a party to proceedings is afforded an opportunity to challenge the matters set out in the certificate, and it is a matter for the court to determine the appropriate weight to be accorded to the evidence placed before it

in individual proceedings. In addition, the certificate is limited to facts in relation to the granting of a special intelligence authority. The limitation to factual matters is consistent with settled Commonwealth policy on the issuing of certificates. In addition, certificates are not available in relation to intelligence information obtained in the course of a SIO. If a person is, for example, prosecuted for an offence on the strength of intelligence information that is admissible in evidence, an evidentiary certificate will not be available to certify actions undertaken in accordance with an authority.

89. In the event that a participant in a SIO acts outside the scope of his or her authority under the relevant SIO authorisation, the immunity in new section 35K will not apply and such persons will be subject to criminal or civil liability (unless new section 35M applies, if the conduct was authorised but the authority was varied or cancelled without the participant's knowledge, and the participant was not reckless as to this circumstance).

90. If a person involved in an SIO is subject to criminal investigation, charge or prosecution in relation to his or her conduct because he or she is said to have exceeded his or her authorisation under a SIO authority, a certificate under section 35R could be issued as prima facie evidence of the limited scope of his or her authorisation. This could be taken into consideration by investigative and prosecution authorities in assessing the sufficiency of available evidence to support a charge or a prosecution. In making such decisions, the police and prosecution would need to consider the availability and strength of any evidence that may be advanced by the person to challenge the matters in the certificate. For example, if there is ambiguity on the face of the authorisation and the certificate as to what conduct was authorised, and it may be open to the defendant to argue that his or her conduct was authorised with the result that the immunity in section 35K applies. If the matter proceeds to prosecution it would also be a matter for the court to determine the appropriate weight to be placed on the competing evidence.

91. Similarly, if a person involved in a SIO is subject to civil suit on the basis that he or she is said to have exceeded his or her authorisation under a SIO authority, he or she could challenge an evidentiary certificate addressing the scope of his or her authorisation, such as where he or she seeks to raise a defence or a collateral challenge on the basis that he or she is immune from liability under section 35K because his or her conduct was, in fact, authorised under the relevant SIO authority.

92. As such the evidentiary certificate provision in section 35R is consistent with the right to a fair trial. It provides a person who is the subject of criminal or civil proceedings, based on an allegation he or she acted outside his authorisation, to challenge a certificate to that effect.

Freedom of expression – Article 19 of ICCPR

93. Article 19(2) of the ICCPR provides that everyone has the right to freedom of expression, including the freedom to impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art or through any other media. Article 19(3) provides that this right may be limited on grounds including national security. However, any limitations must be prescribed by legislation and be reasonable, necessary and proportionate to achieve the desired purpose.

94. The Bill engages the right to freedom of expression through making it an offence to disclose information relating to a SIO. This is critical as the very nature of a SIO is covert.

Communicating such sensitive information can place the health and safety of participants at risk, negates the integrity of operations in general and affects the conduct of the operation in question. As such, the limitation on the right is necessary for the protection of national security and the health and safety of participants. It is reasonable as the offence provides appropriate defences and retains important safeguards facilitating the operation of oversight and accountability bodies. For example, the offence would not apply through subsection 18(9) of the IGIS Act if a document was dealt with for the purpose of producing information under subsection 18(1) of the IGIS Act. Further, the offence would not apply in accordance with section 10 of the *Public Interest Disclosure Act 2013* (PID Act) if information was dealt with for the purpose of making a public interest disclosure in accordance with the PID Act as it applies to ASIO. For example, a person could report a matter in relation to a SIO to the IGIS.

Schedule 4–Co-operation and information sharing

Breaches of section 92 of the ASIO Act

95. This Schedule of the Bill implements the Government's response to PJCIS Recommendation 34 by enabling a breach of section 92 of the ASIO Act, which criminalises the publication of the identity of an ASIO employee or affiliate, to be referred to law enforcement for investigation when it is not otherwise relevant to security.

96. Currently, section 18 of the ASIO Act limits the communication of intelligence, information or matters in the knowledge of, or acquired as a result of a person having been an ASIO employee or affiliate. Subsection 18(3) provides that the Director-General, or a person authorised by the Director-General, may communicate information that has come into the possession of ASIO in the course of performing its functions under section 17, to members of Commonwealth or State authorities (set out in subsection 18(4)), such as the Australian Federal Police (AFP), if it relates to the commission, or intended commission, of a 'serious crime', or where the Director-General or an authorised person is satisfied that the communication is required in the national interest and provided that the information relates to the performance of the functions, responsibilities or duties of the person to whom the information is being communicated. A 'serious crime' is defined in section 4 of the ASIO Act as an offence punishable by imprisonment exceeding 12 months.

97. As a result, the offence of publishing the identity of an ASIO employee or affiliate as set out in section 92 is practically unenforceable as it is not a 'serious crime' due to it only having a penalty of imprisonment for 12 months. The Schedule will insert a new subparagraph 18(3)(b)(ia) into the ASIO Act to provide that a person may communicate information under that section if the information has come into ASIO's possession in the course of performing functions under section 17 and the information relates to, or appears to relate to, the commission or intended commission of an offence against section 92 in relation to the categories of ASIO employees and affiliates, consistent with the changes in Schedule 1. The communication of any breach of section 92 would only be made by the Director-General or a person authorised by the Director-General in accordance with section 18 of the ASIO Act. Further, a prosecution could only be instituted by or with the consent of the Attorney-General as is required in subsection 92(3) of the Act.

Right to protection against arbitrary and unlawful interferences with privacy – Article 17 of ICCPR, right to freedom of expression – Article 19 of ICCPR and rights to work – Article 6 of ICESCR

98. The current provisions of the Act engage and limit the right to freedom of expression for individuals as they generally prohibit the publication or the making public of information relating to the identity of an ASIO employee or affiliate. This limitation is prescribed by law and permissibly limits the right to freedom of expression for the purposes of national security in order to protect the identification of individuals employed by, or associated with, ASIO. Such identification could jeopardise their ability to work for ASIO and the protection of national security more generally. Further, revealing the identity of ASIO employees or affiliates may also have detrimental effects on these employees' and affiliates' privacy, their personal and family life and could put their personal safety at risk. These amendments enabling the communication of the commission or intended commission of an offence against section 92 of the ASIO Act are both reasonable and necessary to achieve this objective. They are also proportionate in that they retain two important exceptions in the ASIO Act. They exclude action being taken in relation to the offence when a former ASIO employee or affiliate has consented to the taking of the action or caused or permitted the fact that they were a former ASIO employee or affiliate to be made public and in relation to broadcasting, datacasting or reporting the proceedings of Parliament.

99. These amendments do not create a new criminal offence, affect fair trial rights for defendants or impermissibly limit the right to freedom of expression. However, they will promote the rights of ASIO employees and affiliates to protection against unlawful and arbitrary interferences with their privacy and rights to work in employment of their choice by ensuring that there is a greater disincentive to publish or otherwise make public an ASIO employee or affiliates' identity by way of providing a more effective sanction. These amendments will also promote the right to freedom of expression for the Director-General or a person authorised to communicate information in accordance with the new subsection.

Co-operation with the private sector

100. This Schedule of the Bill implements the Government's response to PJCIS Recommendation 33 by confirming ASIO's ability to co-operate with the private sector. It does so by including a reference to 'any other person or body whether within or outside Australia' in relation to ASIO's ability to co-operate with other authorities in connection with the performance of its functions. ASIO's functions are set out in section 17 of the ASIO Act and include:

- obtaining, correlating and evaluating intelligence relevant to security
- communicating that intelligence to such persons and in such manner as is appropriate
- advising Ministers and Commonwealth authorities on matters relating to security so far as those matters are relevant to their functions and responsibilities
- furnishing security assessments
- advising Ministers, Commonwealth authorities and other persons as the Minister determines, on protective security
- obtaining within Australia foreign intelligence and communicating that intelligence in accordance with the ASIO Act or the TIA Act, and

- co-operating with and assisting bodies referred to in section 19A (which includes other members of the Australian Intelligence Community).

101. ASIO already has the ability to co-operate with authorities of the Commonwealth, Departments, police forces and authorities of the State and authorities of other countries approved by the Minister. However, it is not explicit that ASIO can co-operate with organisations outside of Government. The Bill will amend subsection 19(1) of the ASIO Act to confirm this.

102. Currently, ASIO's Business Liaison Unit provides an interface between Australian business and the Australian Intelligence Community in order to ensure that the owners and operators of critical infrastructure and other members of the Australian business community can access timely ASIO information on matters affecting the security of the assets and personnel for which they are responsible. The ability to co-operate is important given that the private sector owns and operates large amounts of Australia's critical infrastructure, which is vulnerable to security threats such as terrorism or cyber-attack. In addition, BLU has established a Register of Australian Interests Overseas which enables them to inform nominated persons of national security threats such as politically motivated violence, espionage and the promotion of communal violence. However, many of these private sector organisations are multinational companies with broader business interests. These amendments will clarify, for example, the role that ASIO can play in liaising with them to protect critical infrastructure and personnel in relation to its functions.

Right to freedom of expression – Article 19 of ICCPR

103. The right to freedom of expression in Article 19 of the ICCPR includes the freedom to both impart and receive information. The amendment to clarify that ASIO can co-operate with any other person or body inside or outside of Australia, subject to any arrangements made or directions of the Minister, will facilitate owners and or operators of critical infrastructure receiving timely ASIO information on matters affecting the security of their assets. To the extent that this includes individuals, to whom human rights are inherent, these amendments will promote the right to freedom of expression through the provision of essential information.

Right to protection against arbitrary and unlawful interferences with privacy – Article 17 of ICCPR

104. The amendments in this Schedule clarify ASIO's ability to co-operate with the private sector in connection with the performance of its functions. To the extent that this may involve the sharing of personal information, these amendments will permissibly limit that right.

105. Wherever ASIO seeks to co-operate with the private sector outside of Australia, that co-operation would be subject to arrangements made or directions given by the responsible Minister as required under subsection 19(1) of the ASIO Act. Any arrangements made or directions given by the Minister may also be subject to written Guidelines under section 8A of the ASIO Act. For example, Item 13 of the Attorney-General's Guidelines, in relation to the treatment of personal information, requires the Director-General to take all reasonable steps to ensure that personal information shall not be collected, used, handled or disclosed by ASIO unless that collection, use, handling or disclosure is reasonably necessary for the

performance of its statutory functions or otherwise authorised or required by law. These obligations would apply to engagement between ASIO and the private sector.

106. Formalising co-operation between ASIO and the private sector, which may include the sharing of personal information, will be lawful and necessary to promote the legitimate objective of securing critical infrastructure and personnel, which is consistent with the aims and objectives of the ICCPR. However, there are a range of safeguards that ensure that the limitations on privacy are proportionate in the circumstances. For example, subsection 18(2) of the ASIO Act makes it an offence for an ASIO employee or affiliate to communicate intelligence to a person other than in the course of their duties or in accordance with a contract, agreement or arrangement or with the approval of the Director-General. This ensures that there should not be unnecessary or unauthorised sharing of sensitive personal information. Further, the amendments are proportionate in that they do not go any further than is strictly required to ensure that critical infrastructure and personnel are protected. The IGIS can inspect all records and has oversight of the functions of ASIO to ensure that it acts legally and complies with ministerial directions and Guidelines. The PJCIS can also review ASIO's administration and any matter referred to it by the responsible Minister or a resolution of either House of Parliament.

107. On this basis, any limitations on the right to protection against arbitrary and unlawful interferences with privacy are for a legitimate objective which is that ASIO can only co-operate under subsection 19(1) so far as it is necessary or conducive to the performance of its functions, including securing critical infrastructure or personnel. These limitations go no further than is necessary to enable ASIO to meet its functions. They are also proportionate as the Guidelines provide guidance to ASIO in relation to the handling of personal information. On that basis, these limitations are compatible with the right.

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

108. This Schedule of the Bill implements the Government's response to PJCIS Recommendations 27 and 38 to 40 to amend the IS Act to amend the functions and activities of some of the agencies under the IS Act, particularly ASIS and DIGO. There are four main amendments related to ASIS – enabling ASIS to collect intelligence on persons involved in activities in relation to its operational security (section 3 and new subsections 9(1A) and 9(1B)), permitting ASIS to co-operate with ASIO without Ministerial authorisation when undertaking activities to collect intelligence relevant to ASIO's functions in relation to an Australian person overseas (new paragraph 6(1)(db) and sections 13B, 13D-13G), allowing ASIS to train certain individuals in use of weapons and self-defence techniques and a limited exception for use of a weapon or self-defence technique by an ASIS staff member or agent in a controlled environment (subsection 13(1A) and amendments to Schedule 2 of the IS Act).

109. The Schedule will also extend the limited protection in subsection 14(2) of the IS Act to persons who assist an IS Act agency outside Australia. The Schedule also clarifies DIGO's existing authority to provide assistance.

ASIS' collection of intelligence on persons involved in activities in relation to its operational security

110. The Schedule will enable the Minister to authorise ASIS to produce intelligence on an Australian person, or undertake an activity that will, or is likely to have a direct effect on an

Australian person, where the Minister is satisfied that the person is involved in, 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. Operational security means the protection of the integrity of ASIS's operations from interference by a foreign person or entity or reliance on inaccurate or false information. Protecting the integrity of ASIS's operations is part of ASIS's counter-intelligence function.

Right to protection against arbitrary and unlawful interferences with privacy and reputation – Article 17 of ICCPR

111. To the extent that a person will be in Australia's territory and subject to its jurisdiction, enabling ASIS to produce intelligence on an Australian person who is or is likely to be involved in activities posing a risk to ASIS's operational security, may engage a person's right to protection against arbitrary and unlawful interferences with privacy and reputation. The new ground of authorisation is for a legitimate objective – to assist ASIS in performing its existing function of conducting counter-intelligence activities under the IS Act. The limitation is authorised by law and is consistent with the objectives of the ICCPR, which include State sovereignty and protection of the nation state, including national security.

112. Any interference will be limited, in that the Minister will only be able to issue an authorisation if he or she is satisfied that the 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. Any interference will be proportionate through the requirement in subsection 9(1) that the Minister, before giving an authorisation must be satisfied that any activities which may be done in reliance on the authorisation will be necessary for the proper performance of a function of the agency, there are satisfactory arrangements in place to ensure that nothing will be done in reliance on the authorisation beyond what is necessary for the proper performance of a function of the agency; and there are satisfactory arrangements in place to ensure that the nature and consequences of acts done in reliance on the authorisation will be reasonable, having regard to the purposes which they are carried out.

113. There are appropriate safeguards and oversight mechanisms in place to ensure the proportionality of this new ground of authorisation. The IGIS has oversight of these authorisations, ensuring the in exercise is reasonable and necessary in the circumstances. Further, this assessment also includes an assessment of the propriety of the activity.

114. Further, any intelligence produced will only be retained and communicated in accordance with the rules to protect the privacy of Australians made by the Minister under section 15 of the IS Act. In making the rules, the Minister must have regard to the need to ensure the privacy of Australian persons is preserved as far as is consistent with the proper performance by the agency of its functions. Before making the rules the Minister, in the case of ASIS, must consult with the Director-General of ASIS, the IGIS and the Attorney-General. The IS Act also requires that agencies must not communicate intelligence information concerning Australian persons, except in accordance with the rules. The IGIS must brief the PJCIS on the content and effect of the rules if requested or if the rules change. The rules are publicly available on the website of ASIS..

Permitting ASIS to co-operate with ASIO

115. The Schedule will enhance ASIS's ability to cooperate with ASIO when undertaking less intrusive activities to collect intelligence on Australian persons overseas. ASIS will not be able to undertake any act for which ASIO would require a warrant if it undertook the act in Australia. Any activities must be undertaken only to support ASIO in the performance of its functions, and must be covered by a notice from the Director-General or another authorised person, setting out ASIO's intelligence requirements (except in urgent circumstances where it is not practicable for such a notice to be obtained).

116. These amendments also enable ASIS to incidentally produce intelligence relating to the involvement, or likely involvement, of an Australian person in one or more of the activities set out in paragraph 9(1A)(a) of the IS Act, such as activities for, or on behalf of, a foreign power, activities in contravention of a UN sanction enforcement law or related to the proliferation of weapons of mass destruction.

Right to protection against arbitrary and unlawful interferences with privacy and reputation – Article 17 of ICCPR

117. To the extent that a person will be in Australia's territory and subject to its jurisdiction, enabling ASIS to co-operate with ASIO may engage a person's right to protection against arbitrary and unlawful interferences with privacy and reputation. The new ground of authorisation is for a legitimate objective – to assist ASIO performing its functions under section 17 of the ASIO Act in relation to security. The limitation is authorised by law and consistent with the objectives of the ICCPR, which include State sovereignty and protection of the nation state, including national security. The interference will be both proportionate to and limited to the obtaining of information necessary to achieve this purpose.

118. The interference will be both proportionate to and limited to the obtaining of information necessary to achieve this purpose. Importantly, the limited softening of the requirement to obtain a Ministerial authorisation to produce intelligence on an Australian person only applies where ASIO is already able to produce intelligence on that person without the need to obtain a warrant or other Ministerial authorisation. It effectively creates a common standard based on the ASIO Act, where the agencies are cooperating to support ASIO in the performance of its functions. Further, section 13E will require the Director-General of ASIS to be satisfied there are satisfactory arrangements in place to ensure that activities will be undertaken under section 13B only for the specific purpose of supporting ASIO in the performance of its functions and there are satisfactory arrangements in place to ensure that the nature and consequences of acts done under section 13B will be reasonable, having regard to the purposes for which they are carried out. This will ensure that activities done under section 13B are solely for the purpose of supporting ASIO in the performance of its functions and the nature and consequences of acts done are reasonable, having regard to the purposes for which they are carried out.

119. There are a range of appropriate safeguards and oversight mechanisms in place to ensure the proportionality of this new ground of authorisation, including requirements for the communication of intelligence to ASIO, notification of the IGIS, annual reporting to the responsible Minister and the ability of the responsible Minister and the Attorney-General to jointly issue written guidelines in relation to undertaking activities. Further, the conduct of

each activity is subject to the oversight of the IGIS both in terms of compliance with the law and propriety.

ASIS – use of weapons for self-defence and use in a controlled environment

120. The Schedule enhances the ability for ASIS to train staff members of a limited number of approved agencies that are authorised to carry weapons in the use of weapons and self-defence by providing a specific power of authorisation for ASIS to co-operate with foreign authorities in providing weapons training. However, the Minister must consult the Prime Minister and the Attorney-General in relation to such authorisations. The Bill also ensures that ASIS staff members and agents are not restricted from using a weapon in a controlled environment (such as at a gun club or a rifle range) whether this use is in accordance with the Director-General's Guidelines and in the proper performance of an ASIS function.

121. These measures are in response to identified inconsistencies in the existing regime. Currently, ASIS is only permitted to provide training in the use of weapons to ASIS staff members and agents. This is inconsistent with ASIS's ability to protect others who are cooperating with ASIS in the performance of its functions under section 13 of the IS Act. This restricts joint training activities as ASIS cannot run training that includes individuals who are not ASIS staff members or agents. Further, ASIS staff member 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.

122. There are a number of safeguards to limit the scope of authority and to facilitate effective independent oversight. These include Ministerial authorisation and consultation with other Ministers and IGIS notification.

123. These measures are minor and technical in nature and consequently, do not engage human rights obligations.

Protection from liability for acts done outside Australia

124. The Schedule will also extend the limited protection in subsection 14(2) of the IS Act to a person who undertakes an act outside Australia which is preparatory to, in support of, or otherwise directly connected with, the overseas activities of an IS Act agency, where that act is done in the proper performance of a function of the agency.

Right to an effective remedy – Article 2 of ICCPR and right to a fair trial – Article 14 of ICCPR

125. The extension of the immunity may engage the right to an effective remedy and to a fair hearing, discussed above.

126. Subsection 14(1) provides IS Act agency staff members or agents with a protection from any civil or criminal liability for any act done outside Australia if the act is done in the proper performance of an IS Act agencies' functions. The IS Act also provides a protection to persons in Australia who assist IS Act agencies with their overseas functions from Australian complicity and conspiracy offences, where the persons actions are preparatory to,

in support of, or otherwise directly connected with, overseas activities of the agency concerned and the act is done in the proper performance of a function of the agency. However, currently there is no corresponding protection for persons who assist IS Act agencies overseas from Australian complicity and conspiracy offences, in circumstances where the person committing the primary offence, the ASIS staff member or agent, has immunity. The amendment will address this arbitrary distinction in the application of this protection based on geographical location and is necessary to allow IS Act agencies to perform their functions in a manner intended and required by Government.

127. This amendment will not provide blanket immunity from Australian laws for all acts of those people who assist IS Act agencies. The protection only applies to those activities that are directly related or preparatory to the proper performance of an IS Act agencies' functions and only where those acts are in accordance with the other limits on the IS Act agencies' functions, which are set out in the IS Act.

128. The IGIS will also continue to provide effective independent oversight of the provision, and in any proceedings involving its operation may certify any acts relevant to the question of whether an act was done in the proper performance of an agency's functions. In any proceedings, a certificate given by the IGIS is prima facie evidence of the facts certified.

129. The limitation to the right to an effective remedy and a fair hearing is only limited to the extent that it is reasonable, necessary and proportionate to ensure the proper functioning of IS Act agencies. If the person's act was not done in the proper performance of a function of an IS Act agency, including in accordance with the other limits in the IS Act, they will not be protected from civil or criminal liability under Australian law.

Clarification of DIGO's authority to provide assistance

130. This Schedule of the Bill also implements the PJCIS's Recommendation 27 by clarifying the activities that can be undertaken by DIGO in relation to its functions of co-operation and assistance. DIGO is part of the Department of Defence and its role is to provide geospatial and imagery intelligence to support Australia's defence and national interests. Its functions are set out in section 6B of the IS Act and include functions under subsection 6B(e) to provide to Commonwealth and State and Territory authorities and bodies approved by the Minister for Defence:

- imagery and other geospatial products that are not intelligence information
- assistance in relation to the use and production of such imagery or products, and
- assistance in relation to the performance by those authorities or bodies of emergency response functions.

131. This measure is purely technical and for purposes of clarification. As the reference to 'imagery and products' may not adequately cover the full range of assistance and co-operation that DIGO is able to provide, a reference to 'technologies' is included as technologies are arguably distinct to 'products' as they are used to produce and make use of imagery and products. This amendment will avoid any doubt that DIGO is able to assist in this way and explicitly defining the scope of DIGO's statutory authority will improve accountability. On this basis, this measure does not have any human rights implications.

Schedule 6–Protection of information

132. This Schedule of the Bill will strengthen protections for sensitive information by creating two new types of offence, each punishable by a maximum of three years imprisonment. The first type of new offence applies if an employee or a person who has entered into a contract, agreement or arrangement with ASIO, ASIS, Defence Signals Directorate (DSD), DIGO, Defence Intelligence Organisation (DIO) and Office of National Assessments (ONA)) intentionally copies, transcribes, retains, removes or deals with a record in any other matter without authority (not in the course of their duties) ('unauthorised dealing') (new section 18A of the ASIO Act and new sections 40C, 40E, 40G, 40J and 40L of the IS Act). The relevant records must have been acquired or prepared by, or for, the relevant agency in connection with the performance of its functions. The second type of new offence applies if one of these people intentionally makes a record of any information or matter without authorisation (new section 18B of the ASIO Act and new sections 40D, 40F, 40H, 40K, 40M of the IS Act). An example would be where a person intentionally writes down a record of a conversation based on his or her recollection of it without authority to do so.

133. These amendments will also increase the maximum penalty for unauthorised communication offences in subsection 18(2) of the ASIO Act and sections 39, 29A and 40 of the IS Act from two to ten years imprisonment. The necessity for increasing the penalty has become apparent through recent domestic and international incidents involving the unauthorised disclosure of security intelligence-related information. 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.

134. Further, new section 18C of the ASIO Act applies Category D extended geographical jurisdiction to offences against sections 18, 18A and 18B and new section 41A of the IS Act applies Category D extended geographical jurisdiction (under section 15.4 of the Criminal Code) to offences against new Division 1 of Part 6, which means that a prosecution could be brought for behaviour engaged in extraterritorially by persons who have no connection to Australia, and irrespective of whether the relevant conduct also constitutes an offence in the local jurisdiction in which it is engaged. However, the Bill provides that prosecutions of the new offences may only be commenced with the Attorney-General's consent. This is additional to the general requirement in section 16.1 of the Criminal Code that the Attorney-General's consent is required to prosecute offences under extended geographical jurisdiction. The offences in new Division 1 of Part 6 of the IS Act only apply in relation to intentional unauthorised conduct engaged in after the amendments commence, irrespective of whether the relevant records or information were legitimately accessed or obtained by the person prior to commencement.

Unauthorised dealing with records offences, and unauthorised recording of information offences

135. The creation of an unauthorised dealing offence is necessary to address the current legislative gap in existing protections for conduct that carries a significant risk of jeopardising Australia's national security but stops short of communication of that information to third parties. There is an inherent harm in placing the particular type of information held by those agencies at risk. This offence will apply to all members of the

Australian Intelligence Community and to information peculiar to these roles. Members of intelligence agencies are in a unique position of trust and power, and receive, often highly classified, information for the purpose of performing official duties and are aware of the procedures of handling such information and the consequences of disclosing that information. Given this, there is a strong and legitimate expectation that those persons will handle that information lawfully – that is, in strict accordance with their authority – at all times.

Unauthorised communication offence

136. The penalty for unauthorised communication is being increased to reflect a contemporary assessment of the gravity of the conduct on the basis that the offence provision and the associated penalty in the ASIO Act have not been increased since 1979. Unauthorised communication is a serious offence that jeopardises the lives and safety of those engaged in intelligence-gathering operations and compromises Australia's intelligence-gathering capabilities, including by undermining relationships of trust and confidence with foreign intelligence partners and human sources. These capabilities are essential in assisting the Australian Intelligence Community to fulfil their roles in protecting Australia's national security.

Right to a fair trial – Article 14(1) of the ICCPR, right to freedom from arbitrary detention – Article 9 of ICCPR, the prohibition on cruel, inhuman or degrading treatment or punishment in Article 7 of ICCPR and the CAT and right to freedom of movement – Article 12 of ICCPR

137. The Bill engages the rights to a fair trial, freedom from arbitrary detention, protection from cruel, inhuman or degrading treatment or punishment and freedom of movement on the basis that it create a new offence which can result in a period of imprisonment of up to three years should a person be charged, tried, convicted and sentenced to a period of imprisonment by a court of law. It also significantly increases the penalty for the existing offence of unauthorised disclosure from two to ten years.

138. The penalty for the new offence of unauthorised dealing with records or information is proportionate and reflects the gravity of the offence. While the conduct is less culpable than unauthorised disclosure offences, the risk of harm can still be very high, particularly when conduct relating to this offence is preparatory to a more serious offence. On that basis, it is appropriate that unauthorised dealings with records and information is subject to a specific offence, even if no harm or prejudice to security interests actually results.

139. The penalty is consistent with the established principle of Commonwealth criminal law policy as set out in the *Guide to Framing Commonwealth Offences, Infringement Notices and Enforcement Powers* by imposing a heavier penalty where the consequences of the offence are particularly dangerous or damaging.

140. Further, the penalty of ten years is not such a significant penalty that it would constitute arbitrary detention or cruel, inhuman or degrading treatment or punishment. It reflects an appropriate gradation with the penalties applying to espionage offences in Division 91 of the Criminal Code with penalties of 25 years imprisonment. The higher penalty in those offences reflect the requirement that a person must form a specific intent that a particular unauthorised communication should cause harm, or prove that a foreign government or organisation was the recipient, or likely recipient, of an unauthorised communication.

141. Persons who are charged with the offences created or amended by Schedule 6 may be remanded in custody or released on bail as the court determines appropriate. The Bill confirms that the requirement for the Attorney-General to consent to prosecution does not preclude the arrest, charge, remanding or releasing on bail of a person in relation to the offences, prior to prosecutorial consent being obtained from the Attorney-General. The arrest, charge and remand in custody of a person in such circumstances may limit an accused's freedom of movement, since he or she would have no case to answer should the Attorney-General decline to consent to a prosecution. The discretion of a court to remand the accused in custody pending trial or place them on bail depending on the individual's circumstances is necessary to prevent interference with the evidence, the communication of information already within the knowledge or possession of the accused, and to prevent flight. The granting or refusal of bail is determined by the court in accordance with usual rules and principles of criminal procedure.

142. In practical terms, this means that a person may be arrested, charged and remanded in custody or released on bail prior to the Attorney-General's consent to prosecution when the risks to national security and to the rights and freedoms of other individuals, are great enough to warrant the curtailment of the accused's rights in this manner. The Bill further confirms that nothing in the relevant provisions authorising arrest, charge, remand or release prior to the Attorney-General's consent will prevent the discharging of the accused if proceedings are not continued within a reasonable time. As such, if there is a significant delay between a person's arrest, charge, remand or release, and the decision of the Attorney-General, a person may be discharged. These measures ensure that any limitations on the right to freedom of movement are reasonable, necessary and proportionate to protect national security.

143. These offences are subject to a number of safeguards which ensure their appropriate application. The offences will not apply retrospectively and, as mentioned, the commencement of a prosecution requires the consent of the Attorney-General. Consequently, a proposed prosecution is scrutinised and a judgment made about its appropriateness, having regard to broader public policy considerations that the Commonwealth Director of Public Prosecutions (CDPP) is permitted to take into account under the Prosecution Policy of the Commonwealth. This individualised assessment ameliorates any strict or unwarranted application of the offence. An accused retains a right to a fair trial and their matter will be heard by a competent, independent and impartial tribunal established by law in accordance with the protections in Article 14 of the ICCPR.

144. Further, exceptions are available regarding both relevant existing offences of intentional unauthorised communication of information (as amended and extended to cover new intelligence agencies by Schedule 6) and the new offences of intentional unauthorised dealings with records or recording of information or matter. The offences also contain elements that allow for communication to be made lawfully, for example in the course of duty, to ensure there is no overly onerous burden placed upon members of the Australian Intelligence Community. This means that the prosecution must prove, to the legal standard, that the conduct was not engaged in with authorisation. They also do not apply to information that has already been communicated or made available to the public with the authority of the Commonwealth. This is inserted as an exception to the relevant offences, which means that the defendant bears an evidential burden to adduce or point to evidence suggesting a reasonable possibility of prior, lawful public communication or disclosure, by reason of subsection 13.3(3) of the Criminal Code. The prosecution must then negate this possibility beyond reasonable doubt. The imposition of an evidential burden on the

defendant in these circumstances is appropriate and consistent with Commonwealth criminal law policy, in relation to matters that are readily within the knowledge of the defendant, but may be significantly more difficult or costly for the prosecution to disprove in all cases, even where the relevant matter is not in issue.

145. There are also other protections available in respect to the existing offence provisions. Provisions in the legislation of oversight and accountability bodies confer immunity from criminal or civil liability upon persons who produce documents or provide information to the relevant body in accordance with an obligation to do so. For example, subsection 18(9) of the IGIS Act provides that a person is not liable to penalty under any law of the Commonwealth or of a Territory by reason only of the person having given information, produced a document, or answered a question when required to do so in accordance with a written notice issued by the Inspector-General under subsection 18(1) of the IGIS Act.

146. The statutory safeguards in relation to these rights will ensure that the limitations on these rights go no further than is necessary, reasonable and proportionate to achieving a legitimate objective.

Right to freedom of expression – Article 19 of ICCPR

147. The creation of a new unauthorised dealing offence limits the right to freedom of expression by restricting the circumstances in which persons can impart information and does so permissibly on the basis that it is necessary to protect sensitive national security information. The provisions are reasonable in that they only apply to persons working for or with security and intelligence organisations who receive sensitive information in the course of their employment or engagement with the relevant agency, are constantly subject to a duty or requirement to handle it strictly in accordance with the scope of their authority to do so, and therefore understand the importance of handling this information appropriately. The prosecution is required to prove, to the legal standard, that the relevant conduct (such as communication, dealing with a record or the recording of information) was not authorised. The prosecution must additionally prove that the person intended to engage in the conduct and was reckless as to this circumstance – that is, the person was aware of a significant risk that the relevant conduct was not authorised, but nonetheless and unjustifiably in the circumstances took the risk of engaging in the relevant conduct.

148. The limitation on freedom of expression is proportionate in that it does not limit the operation of relevant oversight and accountability bodies which confer immunities from criminal or civil liability upon persons acting within the scope of their obligations, including in making a public interest disclosure. For example, the offence would not apply through the operation of subsection 18(9) of the IGIS Act if a document was dealt with for the purpose of producing information under subsection 18(1) of the IGIS Act. Further, the offence would not apply in relation to protection of disclosers in section 10 of the PID Act if information was dealt with for the purpose of making a public interest disclosure in accordance with the PID Act as it applies to ASIO. As noted above, the offences are subject to safeguards, including the consent of the Attorney-General to a prosecution, the discretion of the CDPP in accordance with the requirements of the Prosecution Policy of the Commonwealth, and exceptions applying to the offences themselves.

149. On this basis, these amendments are compatible with the right to freedom of expression.

Right to presumption of innocence – Article 14(2) of ICCPR

150. Article 14(2) of the ICCPR provides that everyone charged with a criminal offence shall have the right to be presumed innocent until proved guilty according to law. The presumption of innocence may be limited when an evidential burden is placed on the accused.

151. The Bill imposes an evidential burden on the accused in respect of the exception to the offence in the ASIO Act and IS Act as amended or inserted by Schedule 6. The exception states that the offence does not apply to information or records that have already been communicated or made available to the public with the authority of the Commonwealth. An evidential burden is created by reason of subsection 13.3(3) of the Criminal Code which provides that a defendant who wishes to rely on any exception provided for by a law creating an offence bears an evidential burden in relation to that matter. This is confirmed by the insertion of a note to the relevant exceptions, to ensure that persons who are potentially subject to these offences are aware of this matter. Placing an evidential burden on the defendant in these circumstances is common practice with regards to existing secrecy offences, as illustrated in Division 91 of the Criminal Code and is attributable to the nature of the exception in this type of offence.

152. Evidence suggesting a reasonable possibility of a prior, authorised public disclosure of the relevant record or information is readily available to the accused as it is necessarily a matter of public record. Further, an element of the offence requiring the prosecution to prove, beyond reasonable doubt, that there was no prior authorised communication of the record or information would be an unacceptably onerous burden. This would even be so where the element was not in contention. The rights of the accused are otherwise unaffected as the prosecution will still be required to prove each element of the offence beyond reasonable doubt.

153. On this basis, the limitation on the right to the presumption of innocence is reasonable, necessary and proportionate to achieving the legitimate objective of protecting national security.

Schedule 7–Renaming of Defence agencies

Renaming of DIGO and DSD

154. This Schedule of the Bill will rename DIGO as the Australian Geospatial-Intelligence Organisation (AGO) and the DSD as the Australian Signals Directorate (ASD) to better reflect the national roles that these organisations play in support of Australia's security. The measure also makes consequential amendments to a range of other Acts. These are minor and technical amendments that do not result in the alteration of these organisations' functions, and on this basis, this measure does not have any human rights implications.

Conclusion

155. 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.

NOTES ON CLAUSES

Preliminary

Clause 1 – Short title

1. This clause provides for the Bill to be cited as the *National Security Legislation Amendment Act (No. 1) 2014*.

Clause 2 – Commencement

2. This clause provides for the commencement of each provision in the Bill, as set out in the table. Schedules 1 to 6 commence the 28th day after the Act receives Royal Assent. This is to ensure that all appropriate determinations are in effect prior to commencement.

3. Items 1 to 110 of Schedule 7 commence the day after the Act receives Royal Assent. Items 111 to 114 commence the day after the Act receives Royal Assent. However, if item 1 of Schedule 1 to the *Independent National Security Legislation Monitor Repeal Act 2014* commences at or before that time, these provisions will not commence at all. Otherwise, the remaining items of Schedule 7 commence the day after this Act receives Royal Assent.

Clause 3 – Schedules

4. Each Act specified in a Schedule to this Act is amended or repealed as is set out in the applicable items in the Schedule. Any other item in a Schedule to this Act has effect according to its terms.

Schedule 1— ASIO employment etc.

Overview of measures

5. Schedule 1 amends Part V of the *Australian Security Intelligence Organisation Act 1979* (ASIO Act) which currently provides for the employment of Australian Security Intelligence Organisation (ASIO) officers and employees and includes amendments to other sections of the ASIO Act.

6. This Schedule will modernise the employment provisions contained in Part V of the ASIO Act, to amongst other things, more closely align the provisions with the Australian Public Service (APS) employment framework.

7. The amendments to Part V of the ASIO Act include measures to:

(a) provide for the Director-General of Security (Director-General) to employ persons as employees, under the concept of a level, rather than as officers holding an 'office'

(b) provide for consistency in the differing descriptors of persons who work within ASIO

(c) modernise the Director-General's powers in relation to employment terms and conditions

(d) provide for secondment arrangements, and

(e) include provisions to facilitate the transfer of ASIO employees into APS agencies.

Part 1 – Main amendments

Australian Security Intelligence Organisation Act 1979

Item 1 – Section 4

8. There are currently a number of terms used to describe persons employed by or performing functions or services for the Organisation in the ASIO Act and other Acts. Consistent with the aims of the amendments to Part V, this item inserts two new definitions for describing the categories of persons who work within ASIO: an 'ASIO affiliate' and an 'ASIO employee'. These amendments will both streamline and provide consistency in relation to the use of descriptors in the Act.

9. An 'ASIO affiliate' is defined to mean a person performing functions or services for the Organisation in accordance with a contract, agreement or other arrangement, and includes secondees, consultants and contractors engaged under Part V as amended by this Bill. The definition excludes the Director-General or an ASIO employee.

10. An 'ASIO employee' is defined to mean a person employed under new sections 84 or 90.

Item 2 – Section 4 (definition of *Deputy Director-General*)

11. This item substitutes the current definition of 'Deputy Director-General' with a new definition meaning a 'person who holds, or is acting in, a position known as Deputy Director-General of Security'. This new definition is consistent with the removal of the concept of the engagement of ASIO officers in an office.

Item 3 – Section 4

12. This item inserts a new definition of 'senior position-holder'. This term is defined as meaning an ASIO employee, or an ASIO affiliate, who holds, or is acting in, a position in the Organisation that is equivalent to or higher than a position occupied by an SES employee or a position known as Coordinator. The definition of senior position-holder reflects a range of persons who hold senior management positions within the Organisation.

Item 4 – Paragraph 8A(1)(b)

13. This item amends paragraph 8A(1)(b) of the ASIO Act. Section 8A provides that the Minister may, from time to time, give written Guidelines to the Director-General to be observed by ASIO in performing its functions or the exercise of its powers, or by the Director-General in the exercise of his powers under sections 85 and 86.

14. The reference to 'sections 85 and 86' is omitted and substituted by reference to 'sections 84, 85, 86 and 87', being references to the new sections in Part V in relation to which the Minister may give written guidelines to be observed by the Director-General.

Item 5 – Section 16

15. This item repeals current section 16 of the ASIO Act, which enables the Director-General to delegate to an officer of the Organisation, all or any of his or her powers relating to the management of the staff of ASIO or the financial management powers provided under the ASIO Act.

16. New subsection 16(1) will provide that the Director-General may, by signed writing, delegate to a person, any of the Director-General's powers, functions or duties under or for the purposes of the ASIO Act that relate to the management of ASIO employees or ASIO affiliates (as opposed to 'staff') or the financial management of the Organisation. This amendment is consistent with the operational requirements of the Organisation.

17. A note to new subsection 16(1) refers to the delegation sections of the *Acts Interpretation Act 1901* (sections 34AB and 34A) which detail aspects of the effect of a delegation.

18. New subsection 16(2) provides that a delegate under new section 16 is required to act in accordance with any direction from the Director-General in the exercise of a delegated power.

19. The delegation of any management powers, functions or duties of the Director-General, other than those arising under the ASIO Act, would continue to be made in accordance with the specific Act conferring those powers, such as the delegation of financial management under the Public Governance, Performance and Accountability Act 2013.

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

21. Providing the delegation of 'powers, functions or duties' removes any doubt that the Director-General can delegate not only powers, but also functions and duties.

22. A transitional provision is provided in item 78 preserving those delegations made under section 16 that were in force immediately before the commencement of this item, to ensure they continue to have effect after the item's commencement.

Item 6 – Subsection 18(2)

23. Section 18 of the ASIO Act provides that the Director-General, or a person acting within the limits of authority conferred on the person by the Director-General, may communicate intelligence or information on behalf of the Organisation.

24. Subsection 18(2) currently provides an offence for a person to communicate information which has come to the knowledge or into the possession of the person by reason of the person being, or having been, an officer or employee of the Organisation or having entered into any contract, agreement or arrangement with the Organisation.

25. This item repeals and replaces subsection 18(2), other than the applicable penalty for the offence. New subsection 18 (2) ensures that the offence for unauthorised communication of information reflects the new defined terms of 'ASIO employee' and 'ASIO affiliate'. The effect of this amendment is to provide that particular communications by an ASIO affiliate or other person who has entered into a contract, agreement or arrangement with ASIO, are captured by the offence in section 18.

26. The offence for unauthorised communication of information is not made out where:

(i) an ASIO employee (in the course of their duties)

(ii) an ASIO affiliate (in accordance with the contract, agreement or other arrangement under which the ASIO affiliate is performing functions or services for the Organisation), or

(iii) a person who has entered into a contract, agreement or arrangement with ASIO (otherwise than as an ASIO affiliate), in accordance with the contract, agreement or arrangement

communicates information to the Director-General, another ASIO employee or an ASIO affiliate.

27. This item uses the words 'a person' instead of 'an officer of the Organisation' in subparagraph 18(2)(d)(iii). The effect of this amendment is to permit the Director-General to confer authority to any person to give approval for a person to communicate information.

28. This amendment is necessary to accommodate the broad range of persons who may work in association with the Organisation that could be reasonably expected to be authorised by the Director-General to communicate information, consistent with the efficient and effective performance of the Organisation.

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

Item 7 – Subsection 19A(3)

30. This item amends subsection 19A(3). Section 19A provides that the Organisation may co-operate with intelligence and law enforcement agencies in connection with the performance of their functions.

31. In co-operating with a body referred to in subsection 19(1), the Organisation may currently make the services of officers and employees, and other resources, of the Organisation available to the intelligence and law enforcement agency.

32. This item substitutes the words 'officers and employees, and other resources, of the Organisation' with 'ASIO employees and ASIO affiliates, and other resources of the Organisation'. This amendment reflects the new defined terms of 'ASIO employee' and 'ASIO affiliate', as defined in section 4 of the ASIO Act (see item 1 of this Schedule).

Item 8 – Subsection 23(1)

33. This item amends subsection 23(1) to remove the reference to 'officers'. Section 23 currently provides that an authorised officer or employee of the Organisation may request information or documents from operators of aircraft or vessels, for the purposes of carrying out the Organisation's functions. The effect of this amendment is to provide that the Director-General or an 'authorised person' (see item 11 of this Schedule) can make such a request of an aircraft or vessel operator.

34. A transitional provision is provided in paragraph (1) of item 79 preserving the authority of a person who was an authorised officer or employee under section 23, immediately before the commencement of this item, to ensure the person is still authorised after the commencement of this Schedule.

Item 9 – Subsection 23(6)

35. This item repeals existing subsection 23(6) and substitutes a new subsection 23(6). The effect of this amendment is to provide that the Director-General, or a person appointed under new subsection 23(6A), may authorise, in writing, a person, or a class of persons, for the purposes of this section.

36. New subsection 23(6A) provides that the Director-General may, in writing, appoint a 'senior position-holder', or a class of senior position-holders, for the purposes of subsection 23(6).

37. The term 'senior position-holder' is defined in section 4 of the ASIO Act to mean an ASIO employee or an ASIO affiliate, who holds or is acting in, a position in the Organisation that is equivalent to or higher than a position occupied by an SES employee or a position known as Coordinator (see item 3 of this Schedule).

38. The effect of this amendment is that the Director-General, or a senior position-holder (defined in section 4) appointed by the Director-General to be an authorising person for the purposes of section 23, could authorise a person, or a class of persons, to make a request under that section.

39. This amendment is necessary to accommodate the broad range of persons who could be reasonably expected to be authorised by the Director-General or an authorising person, to make a request for information or documents from operators of aircraft or vessels, consistent with the efficient and effective performance of the Organisation.

40. This amendment reflects the operational requirements of the Organisation, is consistent with the exercise of other powers across the ASIO Act. It is conferred on the basis that the Director-General, or an authorising person, believes such a person should reasonably be able to exercise that power.

41. A transitional provision is provided in paragraph (2) of item 79 preserving the authorisation of a person as an authorising officer for the purposes of subsection 23(6), immediately before the commencement of this Schedule, to be a person appointed under subsection 23(6A) after commencement of this Schedule.

Item 10 – Subsection 23(7) (definition of *authorised officer or employee)*

42. This item repeals the definition of 'authorised officer or employee', as it has been replaced by the new term 'senior position-holder' (see item 3 of this Schedule), as defined in section 4.

Item 11 – Subsection 23(7)

43. This item inserts a definition of 'authorised person' in subsection 23(7). The term is defined as meaning a person who is authorised under subsection 23(6) for the purposes of this section (see item 9 of this Schedule). This amendment also makes the range of persons who can be authorised under section 23 consistent with the range of persons who can be authorised to execute a warrant in accordance with section 24 of the ASIO Act.

Item 12 – Subsection 23(7) (definition of *senior officer of the Organisation)*

44. This item repeals the definition of 'senior officer of the Organisation'. A new term, 'senior position-holder', and the definition of that term is provided for in section 4 (see item 3 of this Schedule).

Item 13 – Subsection 25A(4) (note)

45. This item makes a technical amendment to the note to subsection 25A(4) by substituting 'an ASIO officer' with 'a person', consistent with amendments to section 24 (see item 8 in Part 1 of Schedule 2).

Item 14 – Subsection 25A(4) (note)

46. This item makes a technical amendment to the Note by substituting 'the ASIO officer' with 'the person', consistent with amendments to section 24 (see item 8 in Part 1of Schedule 2).

Item 15 – Subsections 27(1) and 27AA(1)

47. This item makes technical amendments to subsections 27(1) and 27AA(1) by substituting 'an officer, employee or agent of the Organisation' with 'the Director-General, an ASIO employee or an ASIO affiliate'.

48. This amendment reflects the new terminology of Part V of the ASIO Act as amended by this Bill and continues to provide that it is unlawful, under subsections 27(1) and 27AA(1), for the Director-General, an ASIO employee or an ASIO affiliate to seek access to postal articles (in the case of subsection 27(1)) or to inspect delivery service articles (in the case of subsection 27AA(1)) except in accordance with, or for the purposes of, a warrant under sections 27 or 27A.

Item 16 – Paragraph 34ZC(2)(c)

49. This item repeals and replaces paragraph 34ZC(2)(c) to ensure that 'an ASIO employee' continues to be within the categories of person who are unable to represent the interests of a person who is the subject of a warrant under Division 3 of Part III of the ASIO Act. Consistent with the policy intention of this Division, the amendment will additionally include an 'ASIO affiliate' within the category of persons who are unable to represent the person's interests.

Item 17 – Subparagraph 34ZE(7)(c)(iii)

50. This item repeals and replaces subparagraph 34ZE(7)(c)(iii) to provide that an ASIO employee or an ASIO affiliate are included in the category of persons not able to be present when a person who is aged over 16 but under 18, is questioned under a warrant issued under Division 3 of Part III of the ASIO Act.

Item 18 – Part V (heading)

51. This item replaces the heading to Part V of the ASIO Act, 'Part V —Staff of Organisation' with the heading 'Part V —ASIO employees etc.', to more accurately reflect that it deals with matters relating to ASIO employees and the engagement of others to perform work for ASIO (such as consultants, contractors, and secondees).

52. In Part V, whilst the term 'staff' of the Organisation is used to collectively describe those persons who are engaged as officers or employees of ASIO, these individuals will now be collectively referred to as 'ASIO employees'. The updated provisions include references to ASIO affiliates.

Item 19 – Sections 84 to 89

53. To give effect to the broad policy intention of modernising and updating the provisions in Part V, sections 84 to 89 are being replaced by a new employment framework, contained in new sections 84 to 89.

54. A transitional provision is provided in item 80 preserving the employment status and terms and conditions of employment an officer or employee under section 84, immediately before commencement of this item.

New section 84 – Employees of the Organisation

Employees

55. New subsection 84(1) provides that the Director-General may, on behalf of the Commonwealth, employ such persons ('ASIO employees') as he or she considers necessary for the performance of the Organisation's functions and the exercise of the Organisation's powers.

56. New subsection 84(2) provides that the Director-General may from time to time determine in writing the terms and conditions of employment applying to persons employed under subsection (1). This subsection is consistent with subsection 24(1) of the *Public Service Act 1999* (PS Act) which provides that 'an Agency Head may from time to time determine in writing the terms and conditions of employment'.

57. New subsection 84(3) provides that the Director-General has all the rights, duties and powers of an employer on behalf of the Commonwealth.

58. New subsection 84(4) provides that without limiting subsection (3), the Director-General has, in respect of persons employed under subsection (1), the rights, duties and powers prescribed by regulation.

Termination of employment

59. New subsection 84(5) provides for the termination of employees under Part V of the ASIO Act.

60. Subsection 84(5) provides that the Director-General may, at any time, by written notice, terminate the employment of a person employed under subsection (1).

61. While the power to terminate employees is an employer power at common law, new subsection 84(5) clarifies that there is a legislative basis for the termination of an ASIO employee's employment. Including this provision makes it clear that the Director-General does not have to rely on common law powers to terminate the employment of ASIO employees.

62. A new note to subsection 84(5) refers to the rules and entitlements that apply to the termination of an ASIO employee's employment, as provided for in the *Fair Work Act 2009*.

New section 85 – Consultants and contractors

63. New subsection 85(1) provides the Director-General with an express power to engage persons as consultants or contractors to the Organisation. New subsection 85(2) provides that the engagement of a person as a consultant or contractor is on behalf of the Commonwealth, and must be by written agreement. This item gives effect to the broad policy intention of modernising and updating the provisions in Part V of the ASIO Act.

New section 86 – Secondment of ASIO employees

64. New sections 86 and 87 provide an express secondment mechanism within the ASIO Act. The inclusion of new secondment arrangements in the ASIO Act implements the

Government's response to Recommendation 26 of the PJCIS's *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation*.

65. New section 86 provides an express power for the Director-General to enter arrangements to second ASIO employees.

66. New subsection 86(1) allows the Director-General, in writing, to arrange for an ASIO employee to be seconded to another body or organisation. The effect of a secondment arrangement would be to facilitate an ASIO employee performing work as directed by that body or organisation. For example, the Director-General may arrange for an ASIO employee to work for:

- an APS agency
- another member of the Australian Intelligence Community,
- a non-Commonwealth employer, or
- an employer outside of Australia.

67. New subsection 86(1) provides that the secondment arrangement allows the Director-General to second the employee for a specified period. The details of the secondment arrangement would be determined on a case-by-case basis, as is appropriate in the particular circumstances.

68. While an ASIO employee would remain an ASIO employee for the duration of the secondment, his or her duties would be those assigned by the body or organisation for whom the ASIO employee is directed to work (or as specified in the written agreement with the Director-General) and would be performed in accordance with the body or organisation's legal or legislative requirements.

69. New subsection 86(2) provides that the Director-General may terminate the secondment of an ASIO employee at any time. However, the Director-General would be required to give notice to the other agency or employer.

70. The new secondment provisions in sections 86 and 87 are distinct from the existing provisions in section 19A, which enable the Organisation to co-operate with and assist intelligence and law enforcement agencies and prescribed Commonwealth and State agencies.

71. Section 19A provisions were included in the ASIO Act by the *Telecommunications Interception and Intelligence Services Legislation Amendment Act 2011*. These co-operation functions differ to a secondment arrangement because section 19A enables ASIO to co-operate with and assist other agencies in the performance of the other agencies' functions, while performing the Organisations' functions.

72. The secondment arrangements under sections 86 and 87 may be subject to Ministerial Guidelines under section 8A of the ASIO Act.

New section 87 – Secondment of persons to the Organisation

73. New subsection 87(1) allows the Director-General, in writing, to arrange for an officer or employee of another employer to perform work as directed by ASIO. The services that the secondee performs (as an ASIO affiliate) would be in connection with the

performance or exercise of ASIO's functions and powers, and performed in accordance with ASIO's legal and legislative requirements.

74. New subsection 87(2) provides that the terms and conditions of the secondee are those specified in the written agreement with the Director-General.

New section 88 – Applicability of principles of the *Public Service Act 1999*

75. New section 88 includes a provision requiring the Director-General to adopt the principles of the PS Act in relation to ASIO employees, to the extent the Director-General considers the principles are consistent with the effective performance of ASIO's functions. The new section supports the APS transfer mechanism in new section 89 and is consistent with section 35 of the *Intelligence Services Act 2001* (IS Act).

76. The effect of this new section is to include a mechanism within the ASIO Act that, where appropriate given the role and functions of ASIO, supports the application of aspects of the APS' employment principles within ASIO. Due to the operational requirements of ASIO as an intelligence agency, the new section provides that these principles are adopted only to the extent the Director-General considers it is consistent with the effective performance of ASIO's functions.

New section 89 – Voluntary moves to APS

77. New section 89 creates a mechanism for ASIO employees to move to an APS agency in the same way that APS employees can voluntarily transfer from one APS agency to another under section 26 of the PS Act. The effect of this provision would be to treat an ASIO employee who moves to an APS Agency as if they were an APS employee, allowing for an ASIO employee's voluntary move to an APS Agency to be facilitated by section 26 of the PS Act. This protects the identity of ASIO as the transferee's previous employer when transferring to an APS Agency. New section 89 is consistent with section 36A of the IS Act, which facilitates the transfer of employees of the Australian Secret Intelligence Service (ASIS) to APS agencies.

78. Under new subsection 89(2), the Australian Public Service Commissioner and the Director-General would agree on how ASIO classifications correspond to the APS classifications. This would ensure that ASIO levels have an equivalent APS level for the purposes of the operation of the new provision.

Item 20 – Section 90 (heading)

79. This item replaces the heading to section 90 to refer to 'Regulations relating to employment of persons', to more accurately reflect the subject matter of the amended section.

Item 21 – Subsection 90(1)

80. This item amends subsection 90(1). Subsection 90(1) currently provides that regulations made under section 90 may provide for the employment of officers other than under agreements in writing, and may, provide from time to time, for their terms and conditions of employment (including salaries).

81. This item omits ‘officers otherwise than under agreements in writing and may, in respect of officers’, and substitutes ‘persons otherwise than under section 84 and may, in respect to persons’.

82. The effect of this amendment is to update section 90 by removing the reference to ‘officers’.

Item 22 – Subsection 90(2)

83. This item repeals subsection 90(2), which currently enables regulations to be made relevant to terms and conditions for temporary and casual employees, as this terminology is no longer used in the new employment framework.

Item 23 – Subsection 90(2A)

84. This item amends subsection 90(2A) to omit ‘persons who are or have been officers or temporary or casual employees’ and substitutes ‘persons who are ASIO employees, ASIO affiliates, former ASIO employees or former ASIO affiliates’.

85. The effect of this amendment is to allow for regulations made under section 90 to provide for the establishment of a body or for a person, to review actions of the Organisation affecting ASIO employees (see items 1 and 19 of this Schedule), and additionally provide for the body or person to review actions affecting ASIO affiliates, former ASIO employees or former ASIO affiliates.

Item 24 – Subsection 90(3)

86. This item makes a technical amendment to subsection 90(3) by omitting ‘notwithstanding sections 84, 85 and 86’ and substituting ‘despite section 84’ to clarify that regulations made in accordance with section 90 have effect despite section 84.

Item 25 – Subsection 90(4)

87. Subsection 90(4) currently provides that regulations made under section 90 shall not apply to the employment of an officer employed under an agreement made before the commencement of the first section 90 regulations except to the extent agreed in writing by the officer and the Director-General.

88. It is unnecessary to provide that section 90 does not apply to the employment of persons employed under section 84 as section 90 clearly provides that it applies to the employment of persons who are employed other than under section 84. As such, subsection 90(4) is unnecessary and is repealed.

Item 26 – Section 91

89. This item amends section 91 by omitting ‘officers and employees of the Organisation’ and substituting ‘ASIO employees and ASIO affiliates’. Section 91 currently provides that the Director-General and officers and employees of the Organisation shall be deemed to be Commonwealth officers for the purposes of the *Crimes Act 1914* (Crimes Act). The effect of the amendment does not alter the intent of section 91 which is to ensure the application of

the provisions of the Crimes Act dealing with Commonwealth officers, to the Director-General and those performing work for ASIO.

Item 27 – Section 92 (heading)

90. This item makes a technical amendment to the current heading of section 92 by omitting a reference to 'officer of Organisation' and substituting 'ASIO employee or ASIO affiliate' to make clear that the offence of publishing the identity of ASIO employee also relates to the publication of the identify of an ASIO affiliate.

Item 28 – Subsection 92(1)

91. This item amends subsection 92(1) to include the protection of the identity of ASIO affiliates and former ASIO affiliates. Section 92 protects the identity of officers or former officers by making it an offence to engage in certain actions that might reveal the identity of an ASIO officer. In addition to updating this section to refer to 'ASIO employees', it is also amended to provide that the offence applies to a person who reveals the identity of ASIO affiliates or former ASIO affiliates. This is consistent with the policy intention of the provision – being to protect the identity of those who perform work for ASIO.

92. A transitional provision is provided in item 82 ensuring that a person who was a former officer, employee or agent of the Organisation, before commencement, continues to be taken to be a former ASIO employee or former ASIO affiliate on and after commencement of this Schedule.

Item 29 – Subsection 92(1A)

93. This item amends subsection 92(1A) to include the protection of the identity of ASIO affiliates and former ASIO affiliates. Section 92(1A) protects against the revealing of the identity of officers or former officers by a member of the PJCIS. In addition to updating this section to refer to 'ASIO employees', subsection 92(1A) is amended to provide that the offence applies to a member of the PJCIS who reveals the identity of an ASIO affiliate or former ASIO affiliate. This is consistent with the policy intention of the provision – to protect the identity of those who perform work for ASIO.

Item 30 – Subsection 92(1B)F

94. Subsection 92(1B) provides that the offences do not apply in respect of former officers, employees or agents who have consented to the taking of action or have caused or permitted the fact that they are a former officer, employee or agent of the Organisation to be made public.

95. This item amends subsection 92(1B) by omitting 'former officer, employee or agent of the Organisation' and substituting 'former ASIO employee or former ASIO affiliate'. In addition to updating this section to refer to former ASIO employees, it also provides that subsections (1) and (1A) do not apply in relation to former ASIO affiliates. This is consistent with the policy intention of the provision.

Part 2 Other amendments

Administrative Appeals Tribunal Act 1975

Item 31 – Subsection 3(1)

96. This item amends subsection 3(1) of the *Administrative Appeals Tribunal Act 1979* (AAT Act) to insert the new definitions of 'ASIO affiliate' and 'ASIO employee' in the ASIO Act (see item 1 of this Schedule). Inserting these definitions into the AAT Act ensures that the terms, 'ASIO affiliate' and 'ASIO employee', have the same meaning as in the ASIO Act.

Item 32 – Subsections 19(3B), 21AA(3) and 21AB(3)

97. This item makes technical amendments to subsections 19(3B), 21AA(3) and 21AB(3) to replace references to 'an officer, employee or agent of the Australian Security Intelligence Organisation' to apply the new terms of 'an ASIO employee or ASIO affiliate'.

98. This ensures that, for the purposes of subsection 19(3B), a person who is or has been an 'ASIO employee' or 'ASIO affiliate' is included within listed persons who, if the person is a non-presidential member of the Administrative Appeals Tribunal (AAT), must not be assigned to the Security Appeals Division of the AAT.

99. For the purposes of subsections 21AA(3) and 21AB(3), this amendment will ensure that a presidential member must not participate in a proceeding in the Security Appeals Division if he or she is or has been an 'ASIO employee or ASIO affiliate'.

Item 33 – Subsection 39A(15)

100. Section 39A provides for the procedure at hearings of a review of a security assessment in the Security Appeals Division of the AAT.

101. Existing subsection 39A(15) provides, relevantly, that where a person who is invited or summoned to give evidence before the AAT is an officer or employee of ASIO, subsection 39A(8) applies to ensure that any evidence given by the person were treated as though it were evidence proposed to be adduced by or on behalf of the Director-General. Subsection 39A(8) empowers the Attorney-General to certify that evidence proposed to be adduced by on behalf of the Director-General is of such a nature that its disclosure would be contrary to the public interest as it would prejudice the security or defence of Australia.

102. This item repeals subsection 39(15) and substitutes a new provision to provide that if a person invited or summoned to give evidence under subsection 39A(14) is:

(a) an ASIO employee or ASIO affiliate, or

(b) an officer or employee of the Commonwealth agency to which the assessment was given,

subsection 29A(8) applies as if any evidence to be given by the person were evidence proposed to be adduced by or on behalf of the Director-General or that agency, as the case may be.

103. This amendment ensures that the protections granted under subsection 39(15) to the evidence of officers or employees of ASIO will apply to the evidence of ASIO employees and ASIO affiliates.

Australian Postal Corporation Act 1989

Item 34 – Subsection 90F(1)

104. Subsection 90F defines an 'authorised ASIO officer' for the purposes of Part 7B of the *Australian Postal Corporation Act 1989* (APC Act) as an 'officer or employee of ASIO' authorised in writing in subsection 90F(2) to receive disclosures under Part 7B.

105. This item amends the current definition of 'authorised ASIO officer' in subsection 90F(1) by omitting the reference to 'an officer or employee of ASIO' and substituting 'a person'.

106. The effect of this amendment is to accommodate the broad range of persons who may need to be authorised by the Director-General as an 'authorised ASIO officer' to receive disclosures under Part 7B of the APC Act. This amendment is consistent with the operational requirements of the Organisation and the exercise of powers across the ASIO Act.

107. Item 83 provides a transitional provision to preserve an authorisation made before the commencement of this Schedule under the APC Act by an authorised ASIO officer, to ensure that authorisation continues in force under that Act after the commencement of this Schedule.

Item 35 – Paragraph 90F(2)(b)

108. Paragraph 90F(2)(b) identifies those persons may authorise an 'authorised ASIO officer' for the purposes of subsection 90F(1). This item omits the reference to 'an officer or employee of ASIO' and substitutes 'a person' Paragraph 90F(2)(b) states that those persons who are an 'authorised ASIO officer' for the purposes of Division 2 of Part 7B. This item omits the reference to 'an officer or employee of ASIO' and substitutes 'a person'.

109. This will accommodate the broad range of persons who may need to be authorised in writing by the Director-General to give an authorisation under 90F(1) and is consistent with the operational requirements of the Organisation and the exercise of powers across the ASIO Act.

Item 36 – Paragraph 90LD(2)(a)

110. Subdivision C of Division 2 of Part 7B applies to the secondary use or disclosure of information under the APC Act. This item repeals existing paragraph 90LD(2)(a) and substitutes a new paragraph 90LD(2)(a) to provide that Subdivision C does not apply if 'the person is an ASIO employee (within the meaning of the ASIO Act) or an ASIO affiliate (within the meaning of that Act) and the information or document is or may be relevant to security (within the meaning of that Act)'.

111. This amendment ensures that paragraph 90LD(2)(a) applies the new terms, 'ASIO employee' and 'ASIO affiliate' as provided for in the ASIO Act.

Crimes Act 1914

Item 37 – Subsection 15LH(3) (paragraph (f) of the definition of *senior officer*)

112. Section 15LH provides for the delegation of the functions of the chief officer to a senior officer of a law enforcement or intelligence agency.

113. This item amends the definition of 'senior officer' of ASIO by omitting the words 'senior officer of the Australian Security Intelligence Organisation as defined in section 24 of the *Australian Security Intelligence Organisation Act 1979*, or a person occupying an equivalent or higher position in the Australian Security Intelligence Organisation' and substituting 'any senior position-holder within the meaning of the *Australian Security Intelligence Organisation Act 1979*'.

114. A 'senior position-holder' is defined in section 4 of the ASIO Act as an ASIO employee or ASIO affiliate, who holds or is acting in, a position in the Organisation that is equivalent to or higher than a position occupied by an SES employee or the position known as Coordinator (see item 1 of this Schedule).

Criminal Code Act 1995

Item 38 – Subsection 100.1(1)

115. This item inserts new definitions of 'ASIO employee' and 'ASIO affiliate' into subsection 100.1(1) of the Criminal Code. These definitions provide that the terms have a consistent meaning with the ASIO Act.

Item 39 – Subparagraph 105.39(2)(b)(vi)

116. This item amends subparagraph 105.39(2)(b)(vi) by omitting 'officer or employee of the Australian Security Intelligence Organisation' and substituting 'ASIO employee or an ASIO affiliate'. This amendment applies the new terms 'ASIO employee' and 'ASIO affiliate'. The effect of this amendment is that a person is entitled, while being detained under a preventative detention order, to have contact with certain persons, but not an 'ASIO employee' or 'ASIO affiliate'.

Item 40 – Subsections 105.42(2) and (3)

117. Section 105.42 places restrictions on the questioning of a person detained under a preventative detention order. Subsections 105.42(2) and (3) provide that an officer or employee of ASIO must not question a person while they are detained under a prevention detention order or an order made under a corresponding State preventative detention law.

118. This item omits 'officer or employee of the Australian Security Intelligence Organisation' and substitutes the new terms 'ASIO employee' and 'ASIO affiliate, as defined in the ASIO Act.

Item 41 – Subparagraph 105.43(11)(c)(iv)

119. Subsection 105.43 places restrictions on the taking of identification material from a person who is detained under a preventative detention order, and includes provisions to

ensure the taking of identification material from such a person must be done in the presence of a parent or guardian or another appropriate person.

120. Subparagraph 105.43(11)(c)(iv) provides that an 'appropriate person' does not include an officer or employee of ASIO.

121. This item amends subparagraph 105.43(110(c)(iv) by omitting 'officer or employee of the Australian Security Intelligence Organisation' and applies the new terms 'ASIO employee or an ASIO affiliate', as defined in the ASIO Act.

Inspector-General of Intelligence and Security Act 1986

Item 42 – Subsection 3(1)

122. This item amends subsection 3(1) of the *Inspector-General of Intelligence and Security Act 1986* (IGIS Act) to provide definitions of the terms 'ASIO affiliate' and 'ASIO employee'. Both these terms, 'ASIO affiliate' and 'ASIO employee', have the same meaning as in the ASIO Act.

Item 43 – Paragraph 8(1)(b)

123. Section 8 sets out the functions of the Inspector-General of Intelligence and Security (IGIS) in relation to ASIO.

124. Paragraph 8(1)(b) provides that a function of the IGIS is, at the request of the responsible Minister or on the Inspector-General's own motion, to inquire into the procedures of ASIO relating to redress of grievances of employees of ASIO.

125. This item omits 'employees of ASIO' and substitutes 'ASIO employees (within the meaning of the *Australian Security Intelligence Organisation Act 1979*) and ASIO affiliates (within the meaning of that Act)'. This effect of this item is that the IGIS may inquire into the procedures of ASIO relating to redress of grievances of 'ASIO employees' and 'ASIO affiliates', as defined in the ASIO Act. This amendment ensures consistency in respect of the IGIS's functions in respect of all categories of persons who work for ASIO.

Item 44 – Paragraph 8(7)(a)

126. Item 44 omits 'Director-General of Security or ASIO employees' and substitutes 'Director-General of Security, ASIO employees and ASIO affiliates'. The effect of this item is to provide that the Inspector-General shall not inquire into the matters to which a complaint made by an employee of ASIO relates, to the extent that the employee was or is able to have those matters reviewed by a body constituted by, or including, persons other than the Director-General, ASIO employees or ASIO affiliates.

Item 45 – After subsection 8(7)

127. This item inserts new subsection 8(8) after subsection 8(7) to provide that the functions of the Inspector-General include inquiring into a matter arising from a complaint from an ASIO affiliate. This amendment ensures consistency in respect of the IGIS's functions in respect of all categories of persons who work within ASIO. Subsection 8(7), for example, provides for the inquiry functions of the IGIS in respect to an employee of ASIO.

128. New subsection 8(8) provides that the functions of the IGIS include inquiring into a matter to which a complaint to the Inspector-General made by an ASIO affiliates relates to the extent that the matter is related to:

(a) the contract, agreement or other arrangement under which the ASIO affiliate is performing functions or services for ASIO, or

(b) the performance of functions or services by the ASIO affiliate under the contract, agreement or other arrangement.

129. This item also inserts new subsection 8(8A). New subsection 8(8A) provides that the Inspector-General may decide not to inquire into a matter referred to in new subsection (8) to the extent that the ASIO affiliate can have the matter reviewed by a body constituted by, or including, persons other than the Director-General of Security, ASIO employees or ASIO affiliates.

Item 46 – Paragraph 11(5)(a)

130. Paragraph 11(5)(a) provides that the IGIS shall not inquire into the matters to which a complaint of the kind referred to in subsection 8(6) relates if the IGIS is satisfied that the procedures of the intelligence agency relating to redress of grievances of employees are adequate and effective, the complainant has not pursued those procedures, or the matter is not sufficiently serious to justify an inquiry.

131. This item omits 'employees of that agency' and substitutes 'ASIO employees or ASIS employees (as the case may be)' to provide that paragraph 11(5)(a) applies to the grievances of ASIO employees or ASIS employees, rather than 'employees of that agency' more generally.

Item 47 – At the end of paragraph 11(5)(a)

132. This item inserts the word 'or' at the end of paragraph 11(5)(a) to allow for the inclusion of a new subsection 11(6).

Item 48 – At the end of subsection 11

133. This item adds new subsection 11(6) to provide that the IGIS may decide not to inquire into the matters to which a complaint of the kind referred to in subsection 8(8) relates in respect of action taken by ASIO if the IGIS is satisfied that:

(a) the procedures of ASIO relating to redress of grievances of ASIO affiliates are adequate and effective

(b) the complainant has not pursued those procedures as far as practicable, or

(c) the matters to which the complaint relates are not of sufficient seriousness or sensitivity to justify an inquiry into those matters.

134. This amendment ensures consistency in respect of the IGIS's ability to inquire into complaints made by all categories of persons who work within ASIO.

Public Interest Disclosure Act 2013

Item 49 – Subparagraph 41(1)(f)(i)

135. Subsection 41(1) of the *Public Interest Disclosure Act 2013* (PID Act) defines the term 'intelligence information'. This item omits the words 'or the Australian Security Intelligence Organisation' from subparagraph 41(1)(f)(i) of the definition of 'intelligence information' in subsection 41(1) of the PID Act. The definition of 'intelligence information' in relation to ASIO is in new subparagraph 41(1)(fa) (see item 50 of this Schedule).

Item 50 – After paragraph 41(1)(f)

136. This item inserts new subparagraph 41(fa) in subsection 41(1) to provide that 'intelligence information' includes information:

(i) that identifies a person as an ASIO employee (within the meaning of the ASIO Act), or an ASIO affiliate (within the meaning of that Act), a former ASIO employee, or a former ASIO affiliate, other than a person referred to in new subsection 44(4) (see item 51 of this Schedule) or

(ii) from which the identity of a person who is an ASIO employee, an ASIO affiliate, a former ASIO employee or a former ASIO affiliate could reasonably be inferred, or

(iii) that could reasonably lead to the identity of an ASIO employee or ASIO affiliate being established.

137. This amendment provides that the meaning of 'intelligence information' in subsection 41(1) captures information relating to the identity of current and former ASIO employees and ASIO affiliates, as would be defined by the ASIO Act.

Item 51 – Subsection 41(3)

138. Subsection 41(3) excludes certain information from the meaning of 'intelligence information' in section 41 by providing that paragraph 41(3)(1)(f) does not apply to the Director-General of ASIS, the Director-General of Security, or to persons determined by them.

139. This item repeals subsection 41(3) and substitutes separate new subsections 41(3) and (4). These subsections have the same effect as paragraphs (a) and (b) of the current subsection 41(3). This amendment is necessary given changes to the structure of the definition of 'intelligence information' in subsection (1) which result from the proposed inclusion of paragraph 41(1)(fa) (see item 50 of this Schedule).

Item 52 – Section 66 (after table item 7)

140. This item amends item 7 of the Table in section 66 by omitting the reference to 'agency to which the agent or member of the staff referred to in that paragraph belongs' and substituting 'Australian Secret Intelligence Service'. This item is necessary as a consequence of the changes proposed in item 53.

Item 53 – Section 66 (table item 7)

141. This item inserts new item 7A in the Table in section 66.

142. The effect of this item is to include a reference to new paragraph 41(1)(fa) which proposes a separate subparagraph with specific reference to the identity of persons within the Organisation.

Surveillance Devices Act 2004

Item 54 – Subparagraph 45(4)(e)(i)

143. Section 45 creates offences on the use, recording, communication or publication of protected information or its admission in evidence.

144. Subparagraph 45(4)(e)(i) provides that the offences in section 45 do not apply to the use, recording or communication of protected information by an officer or employee of ASIO.

145. This item updates the categories of persons referred to in subparagraph 45(4)(e)(i) by omitting 'officer or employee of the Australian Security Intelligence Organisation' and substituting 'ASIO employee (within the meaning of the *Australian Security Intelligence Organisation Act 1979*) or an ASIO affiliate (within the meaning of that Act)'. This amendment applies the new terms as defined in the ASIO Act.

Taxation Administration Act 1953

Item 55 – Paragraph 355-70(2)(b) in Schedule 1

146. Division 355 provides for the protection of taxpayer information. Section 355-70 provides that the offence in section 355-25 (of disclosure of protected information by a taxation officer) does not apply if the disclosure is made to an authorised ASIO officer.

147. This item amends the definition of 'authorised ASIO officer' in paragraph 355-70(2)(b) by omitting 'any other individual employed under paragraph 84(1)(a) or (b) of that Act' and substituting 'an ASIO employee (within the meaning of that Act) or an ASIO affiliate (within the meaning of that Act)'.

148. This amendment applies the new terms as would be defined in the ASIO Act (see item 1 of this Schedule).

Item 56 – Paragraphs 355-185(1)(c) and (2)(c) in Schedule 1

149. Section 355-185 provides that the offence of on-disclosure of protected information (provided in section 355-155), does not apply if:

- the on-disclosure is by an 'authorised ASIO officer' to, the IGIS or a member of staff appointed to assist the IGIS under the IGIS Act, and the record or disclosure is for the purpose of performing the IGIS's, or the member of staff's, duties in relation to ASIO, or officers or employees of ASIO (subsection 355-185(1)),

- the on-disclosure is by the IGIS or a member of staff appointed to assist the IGIS under that Act, and that information was acquired under subsection (1) or subsection (2), and the record or disclosure is for the purpose of performing the IGIS's, or the officer's duties in relation to ASIO or officers or employees of ASIO (subsection 355-185(2))

150. This item omits 'officers or employees of ASIO' and substitutes the new terms 'ASIO employees (within the meaning of the *Australian Security Intelligence Organisation Act 1979*) or ASIO affiliates (within the meaning of that Act)'.

Telecommunications (Interception and Access) Act 1979

Item 57 – Subsection 5(1)

151. This item inserts new definitions of 'ASIO employee' and 'ASIO affiliate' into subsection 5(1) of the *Telecommunications (Interception and Access) Act 1979* (TIA Act). These definitions provide that the terms 'ASIO employee' and 'ASIO affiliate' have the same meaning as in the ASIO Act.

Item 58 – Subsection 5(1) (definition of *Deputy Director-General of Security)*

152. Subsection 5(1) defines the 'Deputy Director-General of Security' as meaning an officer of the Organisation who holds office as Deputy Director-General of Security (Deputy Director-General). This item amends the definition by omitting 'an officer of the Organisation who holds office' and substitutes 'a person who holds, or is acting in, a position known'. This amendment will ensure that the definition of Deputy Director-General in the TIA Act is consistent with the definition in section 4 of the ASIO Act (see item 2 of this Schedule).

Item 59 – Section 5AD

153. Section 5AD provides that the Director-General may authorise, in writing, a senior officer of the Organisation (within the meaning of section 24 of the ASIO Act) to be a 'certifying person' under the TIA Act.

154. This item omits 'senior officer of the Organisation' and substitutes 'senior position-holder'.

155. Amendments to section 24 of the ASIO Act (see item 8 in Part 1 of Schedule 2) provide that a 'senior position-holder or classes of senior position-holders' may exercise authority under a relevant warrant or relevant device recovery provision. A 'senior position-holder' is defined in section 4 of the ASIO Act to mean 'an ASIO employee, or an ASIO affiliate, who holds, or is acting in, a position in the Organisation that is equivalent to or higher than a position occupied by an SES employee or a position known as Coordinator.

156. The effect of this item is to ensure that changes to the terminology in the ASIO Act are reflected in the TIA Act.

Item 60 – Paragraph 7(2)(ac)

157. Section 7 outlines the circumstances in which a person shall not intercept a communication passing over a telecommunications system.

158. Subsection 7(2)(ac) provides that section 7 does not apply in relation to 'the interception of a communication where the interception results from, or is incidental to, action taken by an officer of the Organisation, in the lawful performance of his or her duties' for certain purposes.

159. This item makes a technical amendment to paragraph 7(2)(ac) to omit 'officer of the Organisation' and substitute 'ASIO employee'. This amendment ensures consistency with the ASIO Act in the use of the term ASIO employee.

Item 61 – After paragraph 7(2)(ac)

160. This item inserts a new paragraph 7(2)(ad) after paragraph 7(2)(ac) to provide that section 7 does not apply in relation to the interception of a communication where the interception results from, or is incidental to, action taken by an ASIO affiliate, in accordance with the contract, agreement or other arrangement under which the ASIO affiliate is performing functions or services for the Organisation, for the purpose of:

(i) discovering whether a listening device is being used at, or in relation to, a particular place, or

(ii) determining the location of a listening device.

161. The effect of this item is to ensure that section 7 does not apply to interception of a communication by an ASIO affiliate who is acting in accordance with the contract, agreement or other arrangement under which the ASIO affiliate is performing functions or services for the Organisation. The item reflects the meaning of ASIO affiliate in section 4 of the ASIO Act.

Item 62 – Section 12

162. Section 12 provides for the authorization, by certain ASIO officers, of officers and employees of ASIO as persons authorized to exercise the authority conferred by Part 2-2 warrants.

163. This item omits 'an officer of the Organisation' and substitutes 'an ASIO employee or ASIO affiliate', to provide that the Director-General of Security can appoint an ASIO employee or ASIO affiliate to be an authorising officer for the purposes of this section.

164. The effect of this amendment is to provide that an ASIO employee and ASIO affiliate may be authorised by the Director-General to approve persons to exercise authority of a Part 2-2 warrant.

165. Paragraph (2) of item 87 provides a transitional provision providing that a person approved under section 12 of the TIA Act before the commencement of this item, is taken, after commencement, to be approved under section 12, as amended by Schedule 1.

Item 63 – Section 12

166. Section 12 provides for the authorisation of persons to intercept communications for the Organisation.

167. This item omits 'officers and employees of the Organisation and other persons' and substitutes 'any persons' in section 12. The effect of this amendment is to provide that the Director-General or an authorising officer appointed under section 12, may, by writing, approve any persons as being authorised to exercise the authority conferred by Part 2-2.

168. The amendment is needed to accommodate the operational requirements of the Organisation regarding the range of persons who may need to be authorised in writing by the Director-General of Security or an ASIO employee or ASIO affiliate to exercise the authority of a warrant issued under Part 2-2.

169. Paragraph (3) of item 87 provides a transitional provision providing that a person authorised to exercise the authority of a warrant under section 12 of the TIA Act before the commencement of this item, is taken, after commencement, to be approved under section 12, as amended by Schedule 1.

Item 64 – Subsection 18(4)

170. Section 18 provides for the use of evidentiary certificates for warrants issued under Part 2-2 of Chapter 2 of the TIA Act.

171. Subsection 18(4) provides that the Director-General or the Deputy Director-General may issue a written certificate setting out matters relating to things done by an officer or employee of the Organisation in connection with the execution of a warrant, or things done by an officer or employee of the Organisation in connection with the listed actions involving information obtained by the execution of a warrant issued under Part 2-2.

172. This item amends subsection 18(4) to provide that the written certificate signed by the Director-General or the Deputy Director-General may set out matters with respect to anything done by an ASIO employee or an ASIO affiliate.

Item 65 – Paragraph 55(3)(c)

173. Section 55 provides who may exercise the authority conferred by a warrant issued to a law enforcement agency under Division 4 of Part 2-5 of the TIA Act.

174. Subsection 55(3) lists the classes of persons who can be approved to exercise the authority of warrants (or classes of warrants) issued under Part 2-5.

175. This item repeals paragraph 55(3)(c), which currently refers to 'officers or employees', and substitutes a new paragraph 55(3)(c) to apply the term 'ASIO employees' as is defined in the ASIO Act (see item 1 of this Schedule).

176. Paragraph (4) of item 87 is a transitional provision preserving the authority of a person approved under paragraph 55(3)(c) of the TIA Act, to exercise the authority conferred by warrants (or classes of warrants), to continue to be approved under paragraph 55(3)(c), as amended, after commencement of this item.

Item 66 – Subsection 55(8)

177. Subsection 55(8) is an avoidance of doubt provision providing that, if a person assisting the Organisation in the performance of its functions, is not an officer or employee of the Organisation, the Organisation exercises the authority of that warrant.

178. This item makes a technical amendment to apply the term 'ASIO employee' consistent with the definition of that term in the ASIO Act.

Item 67 – Subsection 64(2)

179. Subsection 64(2) provides that the Director-General, or an officer or employee of ASIO, may communicate foreign intelligence information to another person (in connection with the Organisation's performance of its functions).

180. This item omits 'officer or employee of the Organisation' and substitutes the new terms 'ASIO employee or ASIO affiliate' in subsection 64(2).

181. The effect of this amendment is to provide that the Director-General of Security or an ASIO employee or ASIO affiliate may, in connection with the performance by the Organisation of its functions, communicate to another ASIO employee or ASIO affiliate, make use of, or make a record of, foreign intelligence information. This amendment accommodates the operational requirements of the Organisation regarding the range of persons who work with ASIO and who may need to deal with foreign intelligence information.

Item 68 – Paragraph 108(2)(g)

182. Section 108 generally prohibits access to stored communications. Subsection 108(2) lists certain classes of conduct to which the offence in subsection 108(1) does not apply.

183. This item omits a reference to 'an officer of the Organisation' in paragraph 108(2)(g) and substitutes 'an ASIO employee', to provide that the offence in subsection 108(1) does not apply in relation to accessing a stored communication if the access results from, or is incidental to, action taken by an ASIO employee, in the lawful performance of his or her duties for the purposes of discovering whether a listening device is being used at, or in relation to, a particular place, or determining the location of a listening device.

Item 69 – After paragraph 108(2)(g)

184. This item inserts a new paragraph 108(2)(ga) after paragraph 108(2)(g) to provide that the offence in subsection 108(1) does not apply in relation to accessing a stored communication if the access results from, or is incidental to, action taken by an ASIO affiliate, in accordance with the contract, agreement or other arrangement in accordance with which the ASIO affiliate is performing functions or services for the Organisation, for the purpose of:

i. discovering whether a listening device is being used at, or in relation to, a particular place, or

ii. determining the location of a listening device

185. The effect of this item is to provide an exception to the offence outlined in subsection 108(1) for 'ASIO affiliates' who are acting in accordance with a contract, agreement or other arrangement with ASIO for the performance of functions or services for ASIO.

Item 70 – Subsections 136(2) and (3)

186. Subsection 136(2) provides that the Director-General may communicate foreign intelligence information to an officer or employee of the Organisation. Subsection 136(3) provides that an officer or employee of the Organisation may, in connection with the performance by the Organisation of its functions, communicate foreign intelligence information to the Director-General of Security or to another such officer or employee.

187. This item omits 'officer or employee of the Organisation' in subsection 136(2) and substitutes 'ASIO employee or ASIO affiliate' to provide that the Director-General may, in connection with the performance by the Organisation of its functions, communicate foreign intelligence to ASIO employees and ASIO affiliates. This amendment accommodates the operational requirements of the Organisation regarding the range of persons who work with ASIO.

188. This item also omits 'officer or employee of the Organisation' in subsection 136(3) and substitutes 'ASIO employee or ASIO affiliate' to provide that an ASIO employee or ASIO affiliate may, in connection with the performance of the Organisation of its functions, communicate foreign intelligence information. This amendment accommodates the range of persons who work with ASIO and who may need to communicate foreign intelligence information.

Item 71 – Subsection 136(3)

189. This item amends subsection 136(3) by omitting 'such officer or employee' and substituting 'ASIO employee or ASIO affiliate'. The effect of this amendment is to provide that the Director-General or an ASIO employee or ASIO affiliate may receive foreign intelligence information from another ASIO employee or ASIO affiliate. This amendment accommodates the operational requirements of the Organisation regarding the range of persons who work with ASIO.

Item 72 – Subsection 136(4)

190. Subsection 136(4) provides that the Director-General or an officer or employee of the Organisation may, in connection with the performance by the Organisation of its functions, make us of, or make a record of, foreign intelligence information.

191. This item amends subsection 136(4) by omitting 'officer or employee of the Organisation' and substituting 'ASIO employee or ASIO affiliate'. The effect of this amendment is to provide that the Director-General or an ASIO employee or ASIO affiliate may, in connection with the performance by the Organisation of its functions, make use of, or make a record of, foreign intelligence information. This amendment accommodates the operational requirements of the Organisation regarding the range of persons who work with ASIO and who may need to deal with foreign intelligence information.

Item 73 – Subsection 174(2)

192. Section 174 provides for voluntary disclosure of information or a document to the Organisation where the disclosure is in connection with the performance of the Organisation's functions.

193. Subsection 174(2) limits the operation of section 174 by providing that the section does not apply if the Director-General, the Deputy Director-General or an officer or employee of the Organisation requests the holder to disclosure the information or document.

194. This item amends subsection 174(2) by omitting 'officer or employee of the Organisation' and substituting 'ASIO employee or ASIO affiliate', applying the terms as defined in the ASIO Act.

Item 74 – Section 175

195. Section 175 provides that the disclosure of information or a document to the Organisation is not prohibited by sections 276, 277 and 278, if the information or document is covered by an authorisation in force under subsection 175(2).

196. This item amends section 175 by omitting 'officer or employee of the Organisation' (wherever occurring) and substituting 'ASIO employee or ASIO affiliate', applying the terms as defined in the ASIO Act.

Item 75 – Paragraph 176(2)(c)

197. Section 176 provides that the disclosure of information or a document to the Organisation is not prohibited by sections 276, 277 and 278, if the information or document is covered by an authorisation in force under section 176.

198. Subsection 176(2) provides that the Director-General, the Deputy Director-General or an officer or employee of the Organisation who holds, or is acting in, a position that is equivalent to, or higher than, an SES Band 2 position in the Department, is an 'eligible person' who may authorise disclosure of specified information or specified documents under section 176.

199. This item amends paragraph 176(2)(c) to omit 'officer or employee of the Organisation' and substitute 'ASIO employee or ASIO affiliate'.

200. The effect of this amendment is to provide that an 'eligible person' includes an ASIO employee or ASIO affiliate who holds, or is acting in, a position that is equivalent to, or higher than, an SES Band 2 position in the Organisation may authorise the disclosure of specified information or specified documents under subsection 176(2) (applying the terms as defined in the ASIO Act).

Item 76 – Subsections 184(1) and (2)

201. Section 184 provides for the notification of authorisations or revocations under Division 3 of Part 4-1.

202. This item amends subsection 184(1) and (2) to omit 'officer or employee of the Organisation' and substitute 'ASIO employee or ASIO affiliate'. This amendment applies the terms as defined in the ASIO Act, to provide that if a person makes or revokes an authorisation under Division 3 of Part 4-1, an ASIO employee or ASIO affiliate must notify the person from whom the disclosure is sought, or notify the person who was notified of the authorisation.

Item 77 – Paragraphs 185B(1)(a) and (b)

203. Section 185B provides for the issue of evidentiary certificates in relation to things done by an officer or employee of the Organisation in connection with an authorisation under Divisions 3 or 4 of Part 4-1.

204. This item amends paragraphs 185B(1)(a) and (b) by omitting 'officer or employee of the Organisation' and substituting 'ASIO employee or ASIO affiliate'. This amendment applies the terms as defined in the ASIO Act, to provide that the Director-General or the Deputy Director-General may issue a signed written certificate setting out relevant facts with respect to anything done by an ASIO employee or ASIO affiliate in connection with an authorisation in force under Division 3 or 4 of Part 4-1 or the matters referred to in subparagraphs (i) to (v) of paragraph 185B(1)(b).

Part 3—Transitional and application provisions

Item 78 – Transitional—delegations

205. This transitional provision applies to a delegation made under section 16 of the ASIO Act that was in force immediately before the commencement of this item. The item provides that these delegations continue to have effect after the commencement of this item, as if the delegation had been made under section 16, as amended by this Schedule.

Item 79 – Transitional—requesting information or documents from operators of aircraft or vessels

206. Paragraph (1) of this transitional provision provides that a person who was an authorised officer or employee within the meaning of section 23 of the ASIO Act, immediately before the commencement of this Schedule, is taken, after commencement, to be an authorised person within the meaning of section 23, as amended by this Schedule.

207. Paragraph (2) of this transitional provision provides that a person who was an authorising officer for the purposes of subsection 23(6) of the ASIO Act, immediately before the commencement of this Schedule, is taken, after commencement, to be a person appointed under subsection 23(6A) of the ASIO Act, as inserted by this Schedule.

Item 80 – Application and transitional—employees of the Organisation

208. This transitional provision provides that a person who was employed immediately before the commencement of this Schedule as an officer or employee of the Organisation under section 84, is immediately after the commencement of this item, taken to be employed under subsection 84(1) and on the terms and conditions applying to the person immediately before the commencement of this item.

Item 81 – Employees of the Organisation—acquisition of property

209. This item applies to a person who, immediately before the commencement of this Schedule, was an officer or employee of the Organisation employed under section 84 of the ASIO Act.

210. This item provides that section 84, as substituted by this Schedule, does not apply to the extent (if any) to which operation of the section would result in acquisition of property (with the meaning of paragraph 51(xxxi) of the Constitution) from the person, otherwise than on just terms (within the meaning of the paragraph).

Item 82 – Transitional—former officers, employees or agents

211. This item provides that if immediately before the commencement of this Schedule, a person was a former officer, employee or agent of the Organisation, the person is, on and after that commencement, taken to be a former ASIO employee or former ASIO affiliate.

Item 83 – Transitional—authorisations under the *Australian Postal Corporation Act 1989*

212. This item preserves authorisations made to an authorised ASIO officer under section 90F of the APC Act made immediately before the commencement of this Schedule, to ensure the person is taken after commencement, to be an authorised ASIO officer within the meaning of that section as amended by this Schedule.

Item 84 – Transitional—delegations under the *Crimes Act 1914*

213. This item preserves a delegation made under section 15LH of the Crimes Act in relation to a person referred to in paragraph (f) of the definition of 'senior officer' in subsection 15LH(3) of the Crimes Act.

214. The item provides that the delegation has effect after the commencement of this Schedule, as if the delegation had been made under section 15LH.

Item 85 – Transitional—determinations under the *Public Interest Disclosure Act 2013*

215. Paragraph (1) of this item provides that a person who, immediately before the commencement of this Schedule, was determined by the Director-General of ASIS under paragraph 41(3)(a) of the PID Act, is taken, after commencement, to be a person determined by the Director-General of ASIS under subsection 41(3) of that Act as substituted by this Schedule.

216. Paragraph (2) of this item provides that a person who, immediately before the commencement of this Schedule, was determined by the Director-General of Security under paragraph 41(3)(b) of the PID Act, is taken, after commencement, to be a person determined by the Director-General of Security under subsection 41(4) of that Act as inserted by this Schedule.

Item 86 – Transitional—authorisations under the *Taxation Administration Act 1953*

217. This item provides that a person who, immediately before the commencement of this Schedule, was an authorised ASIO officer within the meaning of paragraph 355-70(2)(b) of the Taxation Administration Act, is taken, after commencement, to be an authorised ASIO officer within the meaning of that paragraph as amended this Schedule.

Item 87 – Application and transitional provisions—*Telecommunications (Interception and Access) Act 1979*

218. Paragraph (1) of this item provides that a person who was authorised to be a certifying person immediately before the commencement of this Schedule, under section 5AD of the TIA Act, is taken, on and after that commencement, to be a person authorised to be a certifying person under section 5AD as amended by this Schedule.

219. Paragraph (2) provides that if immediately before the commencement of this Schedule, a person was an authorising officer for the purposes of section 12 of the TIA Act, after commencement of this Schedule the person is taken to be an authorising officer for the purposes of section 12, as amended.

220. Paragraph (3) of this item provides that if immediately before the commencement of this Schedule, a person was approved under section 12 of the TIA Act, the person is taken to be a person approved under section 12 as amended, after commencement of this Schedule.

221. Paragraph (4) provides that if before the commencement of this Schedule, a person was approved under paragraph 55(3)(c) of the TIA Act to exercise the authority conferred by warrants (or classes of warrants), the person is taken, after commencement of this Schedule, to be approved under paragraph 55(3)(c), as amended.

Schedule 2—Powers of the Organisation

Overview of measures

222. Schedule 2 amends Division 2 of Part III of the *Australian Security Intelligence Organisation Act 1979* (ASIO Act) to improve ASIO's warrant provisions to address a number of practical difficulties identified in the powers (special powers) that ASIO can use under warrant in carrying out its statutory functions. The powers available to ASIO in Division 2 of Part III include search warrants, computer access warrants, listening and tracking device warrants and the power to inspect postal or delivery service articles. Although there have been several amendments to these powers in the past, the amendments have been piecemeal and have not kept pace with technological advancements. To maintain effective intelligence gathering techniques and capabilities, ASIO's powers require modernising to provide a statutory framework which facilitates intelligence collection by the most technologically effective and efficient means. These amendments will provide ASIO with improved statutory powers to uphold Australia's vital national security interests.

Item 1 – Section 4 (definition of *certified copy*)

223. This item repeals the existing definition of 'certified copy' and substitutes it with a broader definition to cover warrants under Division 2, authorisations under section 27G and instruments varying or revoking a warrant or an authorisation under new section 27G. As the existing definition of 'certified copy' only applies in relation to a warrant or instrument revoking a warrant, this amendment is consequential to the ability for the Minister to vary a warrant issued under new section 29A. This amendment clarifies that 'certified copy' also applies in relation to an instrument varying a warrant.

Item 2 – Before section 22

224. This item separates Division 2 into subdivisions and inserts the title of the first subdivision, 'Subdivision A – Preliminary'.

Item 3 – Section 22

225. This item inserts the definition of 'communication in transit' in to section 22. A computer access warrant, identified person warrant or foreign intelligence warrant may authorise the use of a 'communication in transit' for the purpose of accessing data held in the target computer. The definition refers to the definitions of 'communication' and 'telecommunications network' in the *Telecommunications Act 1997,* to ensure that the definition captures the broad range of electronic communications that may take place in the modern communications environment (for example, emails passing over a wi-fi network).

Item 4 – Section 22 (definition of computer)

226. This item repeals the existing definition of 'computer' and substitutes it with a more modern definition.

227. As currently defined, it is unclear whether 'computer system' includes a computer network (that is, in the sense of a group of linked computers). When narrowly interpreted, a

'computer system' could be interpreted as capturing only a single computer and the devices connected to that computer.

228. The new definition is relevant to search, computer access, identified person and foreign intelligence warrants which may authorise ASIO to use or access data on a 'computer' for certain purposes.

229. In an environment of rapidly evolving technology, it is important that the capability of ASIO not be limited by a definition of computer which will soon become obsolete. In particular, since the definition of computer was inserted into the ASIO Act, the use of multiple computing devices and networked computer systems has become increasingly prevalent.

230. This amendment clarifies the ambiguity around the current definition of a computer in relation to a 'computer system' by extending the definition to 'computer networks' and by making it clear that the definition of 'computer' under the ASIO Act, means all, or part of, or any combination of, one or more computers, computer systems and computer networks.

Item 5 – Section 22

231. This item inserts new definitions which have a particular meaning in this Division: 'device', 'enhancement equipment', 'identified person warrant' and 'install'. The definitions of 'device' and 'enhancement equipment' mirror those already in use under the *Surveillance Devices Act 2004* (Surveillance Devices Act).

232. This item implements the Government's response to Recommendation 30 of the Parliamentary Joint Committee on Intelligence and Security's (PJCIS) *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation* of May 2013 (PJCIS Report). This recommendation recognised that the surveillance devices regime under the ASIO Act has not kept pace with technological advancements. These new definitions seek to modernise the regime by adopting definitions already in use in the Surveillance Devices Act.

233. The new definition of 'identified person warrant' explains that this new type of warrant is available under Division 2 at new section 27C, while the new definition of 'install' mirrors the definition already in use under the Surveillance Devices Act and extends the definition to include the word, 'apply'. The extension of the definition of 'install' to incorporate 'apply' recognises that some tracking devices are substances that must be 'applied' to an object in order to install them.

Item 6 – Section 22 (definition of listening device)

234. This item updates the definition of a 'listening device', for clarity, by removing the reference to optical surveillance devices. The definition draws on elements of the definition of a 'listening device' already in use under the Surveillance Devices Act, while retaining elements from the existing ASIO Act definition, 'whether alone or in conjunction with any other device' and 'sounds and signals'.

Item 7 – Section 22

235. This item inserts the following new definitions which have a particular meaning in Division 2: 'maintain', 'object', 'optical surveillance device', 'prejudicial activities', 'surveillance device', 'surveillance device warrant', 'track', 'tracking device' and 'use'.

236. The new definition of 'maintain' in relation to a surveillance device mirrors the definition already in use under the Surveillance Devices Act and extends the definition to include the word, 'improve'.

237. The existing definition of 'object' under subsection 26A(3) remains unchanged.

238. The new definition of 'optical surveillance device' mirrors the definition already in use under the Surveillance Devices Act and extends the definition to include the new words, 'whether alone or in conjunction with any other device'. This definition has been introduced to address previous interpretational difficulties which arose from the inclusion of optical surveillance device in the previous definition of a listening device. The new definition of an 'optical surveillance device' includes devices that, when used alone or in conjunction with any other device, are capable of recording or observing (visually) the activities of a person.

239. The new definition of 'prejudicial activities' in the context of a person is used in relation to identified person warrants under Subdivision G of this Schedule.

240. The new definition of a 'surveillance device' is based on the definition of 'surveillance device' under the Surveillance Devices Act. The definition categorises, as a surveillance device, a combination of various devices, including a device prescribed by regulation to be a surveillance device for the purposes of this Subdivision.

241. The new definition of 'surveillance device warrant' clarifies the scope of this warrant, while the existing definitions of 'track' under subsection 26A(3) and 'tracking device' under existing subsection 26A(3) remain unchanged.

242. The new definition 'use' in relation to a surveillance device draws on elements of the definition under the Surveillance Devices Act. The definition seeks to clarify ASIO's ability to use a surveillance device for the purpose of collecting intelligence relating to the words, sounds or signals communicated to or by a person, the activities of a person, or to track an object or a person. One of the key objectives underpinning these amendments is to enable ASIO to utilise modern technologies. Accordingly, this definition should not be read as an exhaustive list, and should instead be interpreted broadly to mean any other use that is consistent with the operation of the device.

Item 8 – Section 24

243. This item repeals and replaces section 24 to provide that the Director-General of Security (Director-General) (or a senior position-holder or class thereof authorised by the Director-General) may approve a person or class of persons as being able to exercise the authority of a warrant under Divisions 2 or 3 of Part III.

244. Currently, section 24 provides that the Director-General (or senior officer authorised in writing by the Director-General for the purposes of this section) may approve certain people to exercise authority conferred by warrants issued under Divisions 2 or 3 of Part III.

245. The requirement to maintain a list of the individual names of each person involved in exercising authority under a warrant creates inefficiencies for ASIO. Sometimes, the execution of a warrant takes place in unpredictable and volatile environments requiring ASIO to expand the list of individually authorised persons at very short notice (for example, an operational opportunity to exercise the authority of a warrant may be lost before the authorisation list can be updated).

246. This item will allow classes of people to be authorised to exercise authority conferred by warrants to address this operational inefficiency. For example, the Director-General could authorise ASIO employees of a certain level, ASIO employees within a particular Division or Branch or ASIO employees working on a particular operation to exercise authority under a warrant issued under Division 2 or Division 3 of Part III.

Item 9 – Before section 25

247. This item separates Division 2 into subdivisions and inserts the title of the second subdivision, 'Subdivision B – Search warrants'.

Item 10 – After paragraph 25(4)(a)

248. This item inserts new subparagraph 25(4)(aa) to make it clear that third party premises can be entered in order to gain entry to or exit the subject premises for the purposes of executing a search warrant.

249. Currently, paragraph 25(4)(f) enables an authorised person in the execution of a search warrant to do things 'reasonably incidental' to the things specified in the warrant. However, it is unclear whether these incidental things would include entry onto a third party's premises for the purposes of executing the search warrant.

250. Subparagraph 25(4)(aa) clarifies that when executing a search warrant, it may occasionally be necessary for an authorised person to enter premises (specifically, third party premises) other than the subject premises in order to enter or exit the subject premises. This may be because there is no other way to gain access to the subject premises (for example, in an apartment complex where it is necessary to enter the premises through shared or common premises). It may also occur where, for operational reasons, entry through adjacent premises is more desirable (for example, where entry through a main entrance may involve a greater risk of detection). The need to access third party premises may also arise in emergency circumstances (for example, where a person enters the subject premises unexpectedly during a search and it is necessary to exit through third party premises to avoid detection and conceal the fact that things have been done under a warrant).

Item 11 – Paragraph 25(5)(a)

251. Currently, paragraph 25(5)(a) provides that the powers under a search warrant may include the power to add, delete or alter other data (that is not relevant to the security matter) in a computer or other electronic equipment, or data storage device, where doing so is necessary for the purpose of obtaining access to data that is relevant to the security matter. This amendment clarifies that ASIO may also 'copy' other data (for example, where for technical reasons, it is necessary to 'copy' data as distinct to 'adding' new data or 'deleting'

existing data). In doing so, the purpose must be to access data relevant to the security matter and held on a computer or other electronic equipment, or data storage device.

Item 12 – Subsection 25(6)

252. This item repeals subsection 25(6) and substitutes a modified limitation on ASIO's powers authorised in a search warrant under subsection 25(5). Under the modified limitation, subsection 25(5) does not authorise the addition, deletion or alteration of data, or the doing of any thing that is likely to 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 premises being searched.

253. An exception to the limitation has been included so that ASIO will be able to undertake such actions where they are otherwise necessary to execute the warrant.

254. The modified limitation also provides that subsection 25(5) does not authorise the addition, deletion or alteration of data, or the doing of any thing that is likely to cause any other material loss or damage to other persons lawfully using the computer, equipment or device.

255. Currently, subsection 25(6) restricts ASIO from doing anything under subsection 25(5) including adding, deleting or altering data, that interferes with, interrupts or obstructs the lawful use by other persons of a computer or other electronic equipment, or a data storage device, found on the subject premises, or that causes any loss or damage to other persons lawfully using the computer, equipment or device. This limitation operates even for minor interferences, interruptions, obstructions, losses or damage. The subsection also creates uncertainty if it is not possible to determine whether doing something may in fact interfere with, interrupt or obstruct the lawful use of the computer, equipment or device, or cause loss or damage to other persons using the computer, equipment or device.

256. This amendment is consistent with the amendment to subsection 25A(5). It is intended to address the difficulties in executing search warrants caused by advancements in technology. Persons being investigated by ASIO are increasingly security conscious and technically proficient, requiring innovative methods to access their computers, including methods that may cause a temporary interruption to a computer. This amendment allows ASIO to undertake an action under a search warrant that is likely to cause immaterial interference, interruption or obstruction to the lawful use of a computer or other electronic equipment, or a data storage device, found on the subject premises in executing the warrant (for example, using a minor amount of storage space).

257. This amendment will also allow ASIO to undertake an action that is likely to cause, in the course of executing the warrant, other immaterial loss or damage to other persons lawfully using the computer, equipment or device.

Item 13 – Subsection 25(7) (heading)

258. This item repeals the existing heading to subsection 25(7) and substitutes the new heading, 'Warrants must provide for certain matters'.

259. Currently, paragraphs 25(7)(a) and (b) provide that the warrant must authorise the use of any force that is necessary and reasonable to do the things specified in the warrant and state the time of day or night for entry onto the premises.

260. The current heading, 'Authorisation of entry measures', suggests that the powers are limited to entry to the subject premises (following the amendments to the *Acts Interpretation Act 1901* (Acts Interpretation Act) in 2011, the heading is now treated as part of a section within an Act). It was not intended that paragraph 25(7)(a) (relating to the use of force) be limited to entry measures as is current suggested by the heading to this subsection (for example, reasonable force may be necessary to do other things, such as access a locked safe, drawer or room on the premises).

261. This item makes it clear that the use of force that is necessary and reasonable to do the things specified in the warrant is not limited to entry, but can be exercised at any time during the execution of the warrant.

262. The use of force against a person is subject to strict safeguards, including those that apply to the use of force against property under a search warrant. A search warrant cannot be issued for the purpose of using force against a person. Force may only be used against a person where it is necessary and reasonable to do the things specified in a warrant for the purposes of executing that warrant (for example, the need to use reasonable force against a person may arise where a person was seeking to obstruct an ASIO employee in the execution of a search warrant). Any unauthorised use of force against a person that does not comply with these requirements may attract criminal and civil liability.

Item 14 – Paragraph 25(7)(a)

263. This item inserts the new words, 'against persons and things' after 'any force' and is consequential to the amendment to the change to the heading in subsection 25(7) in item 13 of this Schedule. This item clarifies that the Organisation or persons or another agency acting on behalf of the Organisation in executing warrants under this section, such as the Australian Federal Police or a State or Territory police force, can use reasonable force against both persons and things in executing that warrant where the use of force is both reasonable and necessary.

Item 15 – Before section 25A

264. This item separates Division 2 into subdivisions and inserts the title of the third subdivision, 'Subdivision C – Computer access warrants'.

Item 16 – Subsections 25A(2)

265. This item complements the new definition of a 'computer' by removing the word, 'particular' from subsection 25A(2). This, in conjunction with other amendments, will enable ASIO to apply for a single section 25A computer access warrant to obtain intelligence relating to a matter that is important in relation to security from a number of computers, systems or networks.

Item 17 – At the end of subsection 25A(2)

266. This item inserts a note at subsection 25A(2) which refers to the new definition of computer in section 22.

Item 18 – Subsection 25A(3)

267. This item complements the new definition of 'computer' and amends section 25A to enable the target computer of a computer access warrant to include any one or more of the following: a particular computer or computers specified in the warrant, computers on particular premises specified in the warrant or computers associated with, used or likely to be used by a person specified in the warrant, whose identity may or may not be known.

268. Currently, computer access warrants under section 25A of the ASIO Act authorise access to data that is held in a 'particular computer'. If an individual has more than one computer which is not part of the same computer system, more than one warrant will be necessary (for example, if there are multiple computers on a premises and it is only discovered upon entering the premises for the purpose of executing a warrant that a particular computer is not connected to the computer system specified in the warrant, ASIO would be required to seek another warrant and enter the premises a second time, in order to access the data on that particular computer). Also, with the variety of computers and electronic devices now commonly used by individuals, it is highly probable that a person may store data on a number of computers (for example, a laptop, a phone and a tablet pc).

269. These amendments update the warrants process under the ASIO Act to better reflect the way people use computer technology in the modern world, by allowing ASIO to seek computer access warrants to identify the computers, computer systems or computer networks to which access is authorised by reference to a specified person or premises. In combination with the updated definition of computer in section 22, this amendment will enable a computer access warrant to authorise ASIO to use computers, computer systems and computer networks located at a particular premises or associated with a nominated person in order to obtain intelligence relevant to a matter that is important in relation to security and held in the relevant computers, computer systems or computer networks.

Item 19 – After paragraph 25A(4)(aa)

270. This item amends sections 25A to make clear that premises other than the premises specified in a warrant (that is, third party premises) can be entered for the purpose of gaining access to or exiting the subject premises for the purposes of executing the computer access warrant.

271. Section 25A currently enables ASIO, in the execution of the warrant, to do anything that is reasonably incidental to the exercise of powers under that warrant. However, it is not apparent whether this power includes entry to a third party's premises for the purposes of executing the warrant.

272. This amendment is intended to clarify that when executing some warrants, it may be necessary for ASIO to enter third party premises to access or exit the subject premises. This may be because there is no other way to gain access to the subject premises (for example, in an apartment complex where it is necessary to enter the premises through shared or common

premises). It may also occur where, for operational reasons, the best means of entry might be through adjacent premises (for example, where entry through the main entrance may involve too great a risk of detection).

273. The need to access third party premises may also arise due to 'emergency' and unforeseen circumstances (for example, where a person arrives at the subject premises unexpectedly during a search and it is necessary to exit through third party premises to avoid detection).

Item 20 – Subparagraph 25A(4)(a)(i)

274. This item replaces the words, 'a computer' with 'the target computer' in subparagraph 25A(4)(a)(i). This amendment is necessary as a consequence of a computer access warrant authorising use of a computer other than the target computer (that is, a third party computer) in the circumstances set out in new paragraph 25A(4)(ab).

Item 21 – Paragraph 25A(4)(a)

275. This item defines the term, '(the *relevant data*)' for the purposes of new paragraph 25A(4)(ab).

Item 22 – Paragraph 25A(4)(a)

276. Currently, paragraph 25A(4)(a) provides that the powers under a computer access warrant may include the power to add, delete or alter other data (that is, data not relevant to the security matter) held in the target computer where doing so is necessary for the purpose of obtaining access to data that is relevant to the security matter and is held in the target computer. This amendment is intended to clarify that ASIO may also 'copy' other data (for example, where for technical reasons, it is necessary to 'copy' data as distinct to 'adding' new data or 'deleting' existing data). In doing so, the purpose must be to access data relevant to the security matter and held in the target computer.

Item 23 – After paragraph 25A(4)(a)

277. This item inserts new paragraph 25A(4)(ab) that amends the existing power found under current paragraph 25A(4)(a) to use a third party computer, and adds the new power to use a communication in transit.

278. ASIO will only be able to use the third party computer or communication in transit for the purpose of obtaining access to data relevant to the security matter and held in the target computer. ASIO will not be authorised to use the third party computer or communication in transit for any other purpose.

279. A computer access warrant will also authorise ASIO to add, copy, delete or alter data in the third party computer or communication in transit. This is consistent with what ASIO can do under a computer access warrant in relation to the target computer and is necessary to ensure ASIO's ability to effectively use a third party computer and communication in transit. The power to add, copy, delete or alter other data will only be able to be used where necessary for the purpose of obtaining access to data that is relevant to the security matter and held in the target computer.

280. This amendment updates the computer access warrant provisions to keep track with technological developments which have made it increasingly difficult for ASIO to execute its computer access warrants. In some cases, it may not be possible (or it may be very difficult) to gain direct access to data relevant to the security matter held in the target computer. The use of third party computers and communications in transit to add, copy, delete or alter data in the computer or the communication in transit will facilitate that access (by way of comparison, the use of a third party computer or communication in transit is akin to using a third party premises to gain access to a subject premises, where direct access is not possible under a search warrant).

281. In recognition of the privacy implications for third parties, additional safeguards apply to the use of a third party computer or communication in transit under a computer access warrant. Specifically, the use of a third party computer or communication in transit will need to be reasonable in all the circumstances, having regard to any other methods of obtaining access to the data held in the target computer which are likely to be as effective. To clarify, this does not require ASIO to exhaust all other methods of accessing the target computer. In considering whether to use a third party computer or communication in transit, ASIO must have regard to all the circumstances, which could potentially include the intrusiveness of ASIO's actions, the risk of detection, complexity of implementation and risk of harm.

282. Other relevant amendments to this item include the new section 22 definition of 'communication in transit', new section 33 which deals with the relationship with the TIA Act, and the modified limitation in subsection 25A(5).

Item 24 – Subsection 25A(4) (note)

283. This item modifies the existing note under subsection 25A(4), to clarify that ASIO's powers under a computer access warrant may extend beyond the target computer. This amendment is consistent with the new paragraph 25A(4)(ab).

Item 25 – Subsection 25A(5)

284. This item repeals subsection 25A(5) and substitutes a modified limitation on ASIO's powers under a computer access warrant. Under the modified limitation, a computer access warrant does not authorise the addition, deletion or alteration of data, or the doing of any thing that is likely to materially interfere with, interrupt or obstruct a communication in transit or the lawful use by other persons of a computer. An exception to the limitation has been included so that ASIO may undertake such actions where they are otherwise necessary to execute the warrant.

285. The modified limitation also provides that a computer access warrant does not authorise the addition, deletion or alteration of data, or the doing of any thing that is likely to cause any other material loss or damage to other persons lawfully using a computer.

286. Currently, subsection 25A(5) applies only to the doing of any thing in relation to 'the target computer'. This item complements new paragraph 25A(4)(ab) by expanding the scope of the limitation to apply to 'a computer', which includes a third party computer, and a communication in transit.

287. Currently, subsection 25A(5) restricts ASIO from doing anything under subsection 25A(4), including adding, deleting or altering data, that interferes with, interrupts or obstructs

the lawful use by other persons of the target computer, or that causes any loss or damage to other persons lawfully using the target computer. This limitation operates for even minor interferences, interruptions, obstructions, losses or damage. The subsection also creates uncertainty if it is not possible to determine whether doing something may in fact interfere with, interrupt or obstruct the lawful use of the target computer by other persons, or cause loss or damage to other persons using the target computer.

288. This amendment is consistent with the amendment to subsection 25(6), and is intended to address the difficulties in executing computer access warrants caused by advancements in technology. Persons being investigated by ASIO are increasingly security conscious and technically proficient, requiring innovative methods to access their computers, including methods that may cause a temporary interruption to a computer. This amendment allows ASIO to undertake an action under a computer access warrant that is likely to cause immaterial interference, interruption or obstruction to a communication in transit or the lawful use of a computer (for example, using a minor amount of bandwidth or storage space). It also allows ASIO to undertake an action that is likely to cause, in the course of executing the warrant, other immaterial loss or damage to other persons lawfully using a computer.

Item 26 – Subsection 25A(5A) (heading)

289. This item repeals the existing heading to subsection 25A(5A) and inserts a new heading 'Warrant must provide for certain matters'. The purpose of this amendment is to remove any doubt arising as a consequence of changes made in 2011 to section 13 of the Acts Interpretation Act 1901, resulting in the headings of sections now forming part of an Act.

290. The amendment clarifies that ASIO's power to use reasonable force during the execution of a computer access warrant, extends to all of the acts undertaken for the purpose of the execution of the warrant, not just on entry to the premises. This includes authority for the use of reasonable force against a person where necessary for the purpose of the execution of the warrant (for example, the need to use reasonable force against a person may arise where a person was seeking to obstruct an ASIO employee in the execution of a computer access warrant).

291. The use of force against a person is subject to strict safeguards, including those that apply to the use of force against property. A computer access warrant cannot be issued for the purpose of using force against a person. Force may only be used against a person where it is necessary and reasonable to do the things specified in a properly-issued warrant for the purposes of executing that warrant. Any unauthorised use of force against a person that does not comply with these requirements may attract criminal and civil liability.

Item 27 – Paragraph 25A(5A)(a)

292. This item inserts the new words, 'against persons and things' after 'any force' and clarifies that the Organisation or persons or another agency acting on behalf of the Organisation in executing warrants under this section, such as the Australian Federal Police or a State or Territory police force, can use reasonable force against both persons and things in executing that warrant where the use of force is both reasonable and necessary.

Item 28 – Paragraph 25A(5A)(b)

293. This item amends paragraph 25A(5A)(b) by inserting the words, 'if the warrant authorises entering premises – ' to clarify that a computer access warrant is only required to state whether entry is authorised to be made at any time of the day or night or during stated hours if the warrant authorises entry to premises.

Item 29 – Sections 26 to 26C

Subdivision D – Use of surveillance devices

294. This item implements Recommendation 30 of the PJCIS Report to modernise the warrant provisions of the ASIO Act to align the surveillance device provisions with the Surveillance Devices Act. This subdivision regulates ASIO's use (with and without a warrant) of the following kinds of surveillance devices: listening devices, tracking devices, optical surveillance devices and surveillance devices prescribed by regulation. It also introduces a single surveillance device warrant authorising the use of multiple numbers, combinations and kinds of devices (listening, tracking and optical surveillance devices or devices prescribed by regulation) in relation to a particular person, particular premises or an object or class of objects. This single surveillance device will replace the existing listening device warrants in relation to a person, listening device warrants in relation to a particular premises, tracking device warrants relating to persons and tracking device warrant in relation to objects. To avoid doubt, a surveillance device warrant under the ASIO Act does not permit the use of a data surveillance device within the meaning of the Surveillance Devices Act.

295. Consistent with the Surveillance Devices Act, Subdivision D also removes the general prohibition on ASIO's use of listening devices, tracking devices and optical surveillance devices and identifies the circumstances under which ASIO can use a surveillance device without a warrant. As the use of surveillance devices is primarily regulated by State and Territory law (constitutionally, the Commonwealth Parliament has no general power to legislate in relation to crime) any use of a surveillance device by ASIO outside this framework will, generally, be regulated by State and Territory law.

296. This item separates Division 2 into subdivisions and inserts the title of the fourth subdivision, 'Subdivision D – Use of surveillance devices' and repeals and replaces sections 26 to 26C.

297. These amendments replace the existing framework regulating ASIO's use of listening devices, tracking devices and optical surveillance devices and are modelled, broadly, on Division 2 of the Surveillance Devices Act. In doing so, appropriate modifications to these provisions have been made to reflect the differences between a law enforcement operation – the purpose of which is to investigate a relevant offence in order to obtain evidence versus a covert intelligence collection operation – the purpose of which is to collect security intelligence consistent with ASIO's statutory functions.

298. Under subdivision D, the Minister may issue a single surveillance device warrant in relation to one or more of the following: a particular person (whether or not that person has been identified), particular premises and an object or a class of objects, where the Minister is satisfied that the respective threshold relating to each subject has been met. The existing

thresholds under the ASIO Act remain for these subjects and are incorporated into this Subdivision.

299. Before the Minister may issue a surveillance device warrant in respect of a particular person, the Minister must be satisfied that the person is engaged in or is reasonably suspected by the Director-General of Security of being engaged in or of being likely to engage in, activities prejudicial to security, and that ASIO's use of a surveillance device in relation to that person will or is likely to assist ASIO in carrying out its security intelligence-collection function.

300. Further, if the Minister wishes to also authorise the use of surveillance devices in respect of particular premises under the same warrant, the Minister must be satisfied that the premises are used or are likely to be used or frequented by a person (whether or not that person has been identified) engaged in or reasonably suspected by the Director-General of being engaged in or of being likely to engage in, activities prejudicial to security, and that ASIO's use of surveillance devices in or on those premises will or is likely to assist ASIO in carrying out is security intelligence-collection function.

301. Under the same warrant, the Minister may also authorise the use of surveillance devices in relation to an object or a class of object. In order to do so, the Minister would need to be satisfied that the object or an object of a class of objects is used or worn or is likely to be used or worn by a person (whether or not that person has been identified) who is engaged in or reasonably suspected by the Director-General of being engaged in or of being likely to engage in, activities prejudicial to security, and that ASIO's use of the surveillance device in respect of the object will or is likely to assist it in carrying out its security intelligence collection function.

302. A single surveillance device warrant will replace the need for ASIO to obtain multiple surveillance device warrants for the purpose of using surveillance devices against a person who is the subject of an investigation, and will allow ASIO to use different kinds of surveillance devices in respect of him or her. Currently, for example, in order for ASIO to monitor a person's conversations, activities and location, ASIO would need to obtain two separate warrants, a listening device warrant in respect of the person to record or listen to words, images, sounds or signals on the premises where the person is or is likely to be, and a tracking device warrant in respect of the person in order to track the person. For both these warrants, the relevant threshold for which the Minister must be satisfied, is 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 activities prejudicial security and that ASIO's use of a listening device to listen to the person's conversations, or a tracking device applied to an object they use or wear, is likely to assist ASIO to carry out its function of obtaining intelligence relevant to security.

Issue of surveillance device warrant

303. Subsection 26(2) clarifies that a surveillance device warrant may be issued in respect of multiple kinds of surveillance devices (for example, to include various combinations of listening, tracking, optical and other surveillance devices as provided for in the regulations) and multiple numbers of any particular device, while subsection 26(3) lists the test for issuing these warrants.

304. Subsection 26(4) is an avoidance of doubt provision which clarifies that the identity of a person referred to in paragraph 26(3)(a) or subparagraphs 26(3)(b)(i) or (c)(i) need not be known in order for the test for issue of warrant to be met. In circumstances where the person's identity may not be known, there would still need to be sufficient intelligence available about the person in order satisfy the test for the issuance of a surveillance device warrant under section 26.

305. This item repeals subsections 26(1) and 26A(1) that made it unlawful for an ASIO officer, employee or agent to use a listening device, certain optical surveillance devices (that is, devices that fall within the current definition of a 'listening device') and a tracking device, where it would otherwise have been permissible in some States and Territories. These amendments are consistent with the Surveillance Devices Act.

306. These amendments regulate the circumstances where ASIO may use a surveillance device with and without a warrant. As the use of surveillance devices is primarily regulated by State and Territory law, any inconsistent use of a surveillance device by ASIO under this framework will, generally, be regulated by State and Territory law.

Requirements for surveillance device warrants

307. Section 26A lists what a surveillance device warrant must include, specifically: the kind of surveillance device (for example, listening devices, optical surveillance devices, tracking devices or some other device as prescribed by regulation), whether the warrant is in relation to one or more of a particular person, particular premises or an object or class of objects and the duration of the authority (that is, the period during which the warrant is to remain in force, but not to exceed 6 months).

308. Paragraph 26A(1)(c) retains ASIO's existing power to use force that is necessary and reasonable to do the things authorised under a warrant, and must be specifically stated in the warrant authorised by the Minister.

309. Consistent with subsection 17(2) of the Surveillance Devices Act, subsection 26A(2) provides that where the warrant authorises the use of a surveillance device on premises which includes a vehicle, the warrant may specify a class of vehicle. This would enable the warrant to specify all vehicles used or likely to be used by a person suspected of being engaged in activities prejudicial to security as a class of vehicle, which would minimise the risk of surveillance being thwarted by frequent vehicle changes (for example, a class of vehicle might include, 'a vehicle likely to be used by a specified person' which would avoid the need for ASIO to seek multiple new, or varied, warrants for each vehicle used).

310. Subsection 26A(3) preserves the existing duration of warrant provisions found under subsections 26(6), 26B(5) and 26C(5), which permit a warrant issued under this subdivision to remain in force for a period not exceeding 6 months.

311. Subsection 26A(4) clarifies that subsection 26A(3) does not prevent the issue of any further warrant in relation to the same subject matter.

Authorisation in warrant – particular person

312. Section 26B clarifies what can be done under the authority of a warrant. Subsections 26B(1), 26B(2) and 26B(3) outline the various powers that are authorised by a warrant in respect of particular persons, particular premises or objects or classes of objects.

313. Paragraphs 26B(1)(a) and (b) preserve the powers authorised under a listening device warrant issued under existing subsection 26(3) and adopt paragraph 18(2)(c) of the Surveillance Devices Act, which expands ASIO's ability to install, use and maintain a surveillance device of the kind specified in the warrant, in or on the premises, where the particular person is reasonably believed to be, or likely to be.

314. Subparagraph 26B(1)(a)(i) has been expanded to include a reference to optical surveillance devices.

315. Paragraph 26B(1)(c) supplements paragraph (b) by allowing entry onto premises for the purpose of installing, using or maintaining a surveillance device (for example, this may include entry onto premises for the purposes of determining whether it is operationally viable to carry out an installation, and to minimise risks to the safety of ASIO employees).

316. Paragraphs 26B(1)(d), (e) and (f) preserve the powers authorised under a tracking device warrant issued under existing subsection 26B(3).

317. Paragraph 26B(1)(g) provides for a separate power to enter any other premises for the purpose of entering or exiting the premises for which ASIO is authorised to enter, as there may be circumstances where ASIO employees have no other way to gain access to the premises (for example, where the subject premises are in an apartment block and entry is through common areas or adjoining premises, or due to emergency or unforeseen circumstances where a person unexpectedly returns to the premises during the search).

318. Subsection 26B(1)(h) authorises ASIO to do anything reasonably incidental to the exercise of a power under the warrant (for example, this may permit an ASIO employee to temporarily move third party property that obstructs access to the relevant premises, or to disable security measures in order to gain entry onto the premises).

Authorisation in warrant – particular premises

319. Subsection 26B(2) is broadly based on paragraph 18(2)(a) of the Surveillance Devices Act and preserves ASIO's ability under subsection 26(4) of the ASIO Act to install, use and maintain a device on other specified premises from which the words, sounds or signals communicated by a person can be listened to, recorded, observed or monitored while that person is in the subject premises.

320. Subparagraph 26B(2)(a)(ii) has been expanded to cover ASIO's power to obtain a warrant to use an optical surveillance device.

321. Paragraph 26B(2)(c) includes a separate power to enter any other premises for the purpose of entering or exiting the specified premises. This amendment is consistent with paragraph 26B(1)(g).

Authorisation in warrant – object or class of object

322. Subsection 26B(3) permits the things authorised in paragraph 18(2)(b) of the Surveillance Devices Act and existing subsection 26C(3) of the ASIO Act.

323. Paragraph 26B(3)(d) includes a separate power to enter any other premises for the purpose of entering or exiting premises for which ASIO is authorised to enter.

Authorisation in warrant – general

324. Subsection 26B(4) specifies other powers that are authorised for the performance of each type of warrant, irrespective of whether it relates to persons, premises or objects, and is based broadly around subsection 18(3) of the Surveillance Devices Act. This includes a power to replace an object with an equivalent object where it is operationally conducive or necessary for the installation or maintenance of the surveillance device or enhancement equipment. While it may be possible for ASIO to rely on the power to temporarily remove an object from premises for the installation or maintenance of a surveillance device, this power confirms that ASIO is authorised to replace the object, including where there is no operationally viable method of returning the removed part (for example, replacing a screw that is damaged during the course of an ASIO operation).

Recovery of surveillance devices

325. Subsection 26B(5) permits ASIO to recover a surveillance devices during the life of the warrant, or within 28 days after the warrant ceases to be in force, or otherwise as soon as is reasonable practicable. This subsection is modelled on existing subsections 26(6A), 26B(7) and 26C(7) and includes a reference to various powers authorised under subsection 26(1) of the Surveillance Devices Act.

326. Paragraph 26B(5)(h) provides for the use of a nominal amount of electricity from any source to power the surveillance device or equipment. In some instances, the drawing of a nominal amount (that is, an insignificant or minimal amount) of electricity by the device or enhancement equipment, while the device or equipment is on site, is necessary before it can be recovered (for example, using a nominal amount of electricity to recover information stored on a surveillance device before it is reasonably practicable to recover the device). As a safeguard, this would only occur where the use of the device in that manner does not involve listening to, recording, observing or monitoring the words, sounds or signals communicated to or by a person, or the activities of a person.

Use etc. of listening device without warrant

327. Subdivision D also removes the provisions that previously made it unlawful for an ASIO officer, employee or agent to use a listening device, certain optical surveillance devices and a tracking device, where it would otherwise have been permissible in some States or Territories. Instead, this Subdivision regulates the circumstances where ASIO may use a surveillance device with and without a warrant. Any use outside this framework will generally be regulated by State or Territory law.

328. Subsection 26C replaces the existing subsection 26(1) and permits the use of a listening device, without warrant, by an ASIO employee acting in the course of his or her

duties or an ASIO affiliate (as defined in section 4) acting in accordance with the contract, agreement or other arrangement under which he or she is performing functions or services for ASIO. This amendment is modelled on paragraph 38(1)(d) of the Surveillance Devices Act.

329. The ability to use a listening device without warrant has been amended to permit a person to listen to or record words, sounds or signals being communicated by another person where they do so with the consent of a participant of the conversation, or in circumstances where the communicator intends or should reasonably expect those words, sounds or signals to be communicated to the first person or a class or group of persons in which the first person is included (for example, this would permit an ASIO employee, who is not part of a conversation, to monitor that conversation involving another ASIO employee, in real time, where that ASIO employee consents, for the purpose of ensuring that employee's personal security).

Use etc. of optical surveillance device without warrant

330. New subsection 26D provides that, where the use of an optical surveillance device will not involve entry onto premises without permission, or interference without permission with any vehicle or thing, a person carrying out a function of ASIO may, without a warrant, use such a device (for example, this may include an ASIO employee taking a photograph or video of a building or a vehicle from a public location, or taking a video of a vehicle moving to and from premises). This provision is modelled on section 37 of the Surveillance Devices Act.

Use etc. of tracking device without warrant

331. Subsection 26E preserves ASIO's ability to use a tracking device without warrant, where the person, or the person using the object, consents to the tracking (for example, to track an ASIO employee undertaking a particular operation).

Director-General may determine that certain provisions do not apply to specified ASIO affiliates

332. Section 26F allows for the Director-General to determine that specified powers under the ASIO Act cannot be exercised by specified persons.

333. Subsection 26F(1) provides that the Director-General may make a determination, by signed writing, that one or more of new sections 26C and 26D or subsections 26E(1) or (2) do not apply to specified ASIO affiliates, or a specified class of ASIO affiliates.

334. The persons subject to a determination under this subsection are those persons who are within the new definition of ASIO affiliate. This subsection allows for the Director-General, where appropriate for operational reasons, or in the interests of national security, to exclude certain ASIO affiliates or certain classes of ASIO affiliates, from exercising the powers conferred under sections 26C and 26D or subsections 26E(1) or (2) (that is, the provisions providing for the use of surveillance devices without warrant).

335. This measure is an important safeguard in ensuring that, while a particular individual, or class of individuals, may be appropriately performing certain functions or services for

ASIO, they are not within the categories of persons who can perform ASIO's powers by use of surveillance devices without warrant.

336. Subsection 26F(2) provides that the determination has the effect according to its terms.

337. Subsection 26F(3) makes it clear that determinations made under section 26F are not legislative instruments. This provision is merely declaratory in nature. Determinations of this type are administrative in character because they are merely the application of a legal power in a particular case, they do not determine or alter the content of the law itself.

338. Subsection 26F(4) provides for the Director-General to delegate his power to make a determination to senior management within ASIO. The Director-General's delegation would be limited to a Deputy Director-General, or a person holding a position equivalent to an SES employee with a classification of SES Band 2. This is consistent with the operational requirements of the Organisation.

339. Subsection 26F(5) provides a safeguard for the appropriate use of delegated powers, specifically, that the delegate must comply with any written direction of the Director-General when exercising his or her powers under a delegation.

Item 30 – Before section 27

340. This item separates Division 2 into subdivisions and inserts the title of the fifth subdivision, 'Subdivision E – Inspection of postal and other articles'.

Item 31 – Subsection 27(1)

341. This item removes the existing words, 'this section or section 27A' and substitutes the words, 'this Division'. The intention of this amendment is to extend the exception for ASIO to inspect postal articles under the new identified person warrant.

Item 32 – Before section 27A

342. This item separates Division 2 into subdivisions and inserts the title of the sixth subdivision, 'Subdivision F – Foreign intelligence'.

Subdivision F – Foreign intelligence

343. These amendments update the warrant framework in regards to foreign intelligence collection by replicating the amendments to the warrant provisions that deal with security intelligence.

344. This includes changes to the surveillance devices provisions to enable the Minister to authorise a surveillance device warrant in relation to one or more of the following: a particular person, a particular premises, or an object or a class of objects, in accordance with the performance of ASIO's functions under paragraph 17(1)(e), which permits ASIO obtain foreign intelligence in Australia and to communicate that intelligence.

Item 33 – Paragraph 27A(1)(a)

345. This item removes the existing words, 'computer or a thing' and substitutes 'computer or an object' in order to update the language to align with other amendments in sections 26, 26A and 26B.

Item 34 – Paragraph 27A(1)(a)

346. This item removes references to, '26(3) or (4), 26B(3), 26C(3)' and substitutes '26B(1), (2), (3) or (4)'. These amendments update the provision to mirror the powers now available to ASIO under the security intelligence provisions.

Item 35 – Subsection 27A(1)

347. This item removes the words, 'those things' and substitutes 'those objects' in order to order to update the language to align with other amendments in sections 26, 26A and 26B.

Item 36 – Paragraph 27A(2)(a)

348. This item inserts the new words, 'against persons and things' after 'any force' and clarifies that the Organisation or persons or another agency acting on behalf of the Organisation in executing warrants under this section, such as the Australian Federal Police or a State or Territory police force, can use reasonable force against both persons and things in executing that warrant where the use of force is both reasonable and necessary.

Item 37 – Paragraph 27A(2)(b)

349. This item inserts the new words, 'if the warrant authorises entering premises–' before the existing words, 'state whether' to clarify that a warrant for the performance of functions under paragraph 17(1)(e) is only required to state whether entry is authorised to be made at any time of the day or night or during stated hours, where the warrant authorises entry to premises.

Item 38 – Paragraph 27A(3)(b)

350. This item removes references to, '26(3) or (4), 26B(3), 26C(3)' and substitutes '26B(1), (2), (3) or (4)'. These amendments update the provision to mirror the powers now available to ASIO under the security intelligence provisions.

Item 39 – Subsections 27A(3A) and (3B)

351. This item repeals and replaces subsection 27A(3A) in order to clarify that a warrant issued under section 27A (Warrants for the performance of functions under paragraph 17(1)(e)) which authorises the doing of acts referred to in new subsections 26B(1), (2), (3) or (4) also authorises the acts permitted to be carried out in subsection 26B(5). This subsection is modelled on existing subsections 26(6A), 26B(7) and 26C(7) and includes a reference to various powers authorised under subsection 26(1) of the Surveillance Devices Act.

352. This item also repeals and replaces subsection 27A(3B) to align with new subsection 26B(6), which permits the use of a surveillance device and any enhancement

equipment solely for the purposes of locating and recovering the listening device. This provision does not permit ASIO to use the device for an ulterior purpose (for example, to track the person or object once the warrant period has expired) rather, it is intended that a minimal reading will be taken to locate the device, and where possible, use the device in a manner that does not track the person.

Item 40 – Subsection 27A(5)

353. This item repeals subsection 27A(5) which provides that nothing in current section 27A or a warrant issued under that section applies to or in relation to the use of a listening device that would constitute the interception of a communication passing over a telecommunications system operated by a carrier or a carriage service provider for the purposes of the TIA Act.

354. This item is consequential to the amendments in Item 46 which create new subsection 33(2) which preserves the operation of this subsection.

Item 41 – After section 27B

Subdivision G – Identified person warrants

355. This item separates Division 2 into subdivisions and inserts the title of the seventh subdivision, 'Subdivision G—Identified person warrants' and inserts new sections 27C, 27D, 27E, 27F, 27G, 27H and 27J.

356. These amendments implement the Government's response to Recommendation 29 of the PJCIS to establish a single, named person warrant that enables ASIO to request multiple powers against a particular person.

357. This new warrant (an identified person warrant) will enable ASIO to utilise multiple warrant powers to collect intelligence in relation to activities of an identified person that are, or are likely to be, prejudicial to security.

358. In many cases, ASIO will seek more than one type of warrant power in relation to a person of security concern. An identified person warrant will enable the Minister to issue a single warrant which authorises (subject to conditions) the use of more than one type of warrant power if the Minister is satisfied that the legislative threshold is met.

359. The thresholds (tests) for the Minister to consider in issuing an identified person warrant in relation to a particular person, are:

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

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

360. Once these thresholds are met, the Minister may issue an identified person warrant which gives ASIO 'conditional approval' to exercise one or more of the broad types of warrant powers in Division 2 of Part III which are specified in the warrant. To be clear, conditional approval does not, of itself, permit ASIO to do those things under an identified

person warrant. Before a warrant power can be exercised under an identified person warrant, a specific authorisation must be granted by either the Director-General of Security or the Minister (for example, see subsections 27D(2), 27E(2), 27F(2), 27G(2) and 27H(2) for the things that may be authorised under the warrant).

361. The threshold test for granting the authorisation is that the use of the particular power in the particular circumstances will substantially assist the collection of intelligence in relation to the activities prejudicial to security of the identified person.

362. Consistent with Recommendation 29 of the PJCIS Report, the same test applies for all authorisations given under identified person warrants. In fact, the test for an identified person warrant is more stringent than the various tests that currently apply to the issuing of warrants authorising ASIO to do comparable things under Division 2 of Part III.

363. The PJCIS recommended that, '[t]he thresholds, duration, accountability mechanisms and oversight arrangements for [identified person] warrants should not be lower than other existing ASIO warrants.' Subdivision G implements this recommendation in the following ways:

(a) The 2-part test for the issue of an identified person warrant by the Minister, set out in subsection 27C(2), is more stringent than the test for the issue of warrants under Division 2 of Part III of the ASIO Act, which authorises ASIO to do things comparable to those for which conditional approval may be granted under the identified person warrant. The Minister or Director-General must then be satisfied of a similar test under sections 27D, 27E, 27F, 27G or 27H before he or she may authorise ASIO to do specific things for which 'conditional approval' has been given under the warrant. Importantly, the purposes for which the Minister or Director-General may authorise ASIO to do specific things under an identified person warrant are at least as strict, and in many cases stricter than, the purposes for which ASIO may be authorised to do comparable things under other warrants issued under Division 2 of Part III of the ASIO Act.

(b) The maximum period for which an identified person warrant may remain in force, 6 months, is equivalent to that for most comparable ASIO warrants. The exception is that for a search warrant issued under section 25, which has a maximum duration of 90 days. This inconsistency is addressed by paragraph 27J(5)(a), which provides that the maximum duration of an authorisation under section 27D (search of premises and persons) is 90 days. The Minister may revoke an identified person warrant at any time while it remains in force. Further, updated section 30 of this Bill requires the Director-General to discontinue action under the identified person warrant if he or she is satisfied that the grounds on which the warrant was issued have ceased to exist.

(c) The accountability mechanisms that apply to an identified person warrant are as least as strict as those that apply to comparable ASIO warrants. Identified person warrants may only be issued by the Minister at the request of the Director-General. Unlike the existing ASIO warrants issued under sections 25, 25A, 26, 27 or 27AA or sections 9 or 9A of the TIA Act, the Director-General may not issue an emergency identified person warrant. However, new section 29A enables the Minister to vary a warrant issued under

Part III Division 2 of the ASIO Act, including an identified person warrant, at the request of the Director-General.

(d) The Inspector-General of Intelligence and Security's (IGIS) oversight powers in relation to the new identified person warrant are identical to his or her powers to oversight all existing ASIO warrants.

364. The operation of Subdivision G is outlined in greater detail, below.

Section 27C – Issue of identified person warrants

365. Section 27C deals with the issue of an identified person warrant.

Test for issue of warrant

366. Subsection 27C(2) requires the Minister to satisfy a 2-part test before issuing an identified person warrant in relation to a person. First, the Minister must be satisfied 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, 'activities prejudicial to security' (defined in section 4). Secondly, the Minister must be satisfied that the issuing of the warrant in relation to the person will, or is likely to, substantially assist the collection of intelligence relevant to security.

Requirements for warrant

367. Subsection 27C(3) sets out the requirements for the identified person warrant.

368. Paragraph 27C(3)(b) provides that the warrant must identify the person by name, if the name of the person is known, or otherwise by including other details sufficient to identify the person (for example, ASIO will not always know the true name of a person engaged in prejudicial activities at the time the Director-General requests the Minister to issue a warrant). The ability to issue a warrant in respect of a person whose name is not known, but who can be identified through other means, is necessary to prevent undue delay in investigating the person's prejudicial activities.

369. Paragraph 27C(3)(c) provides that an identified person warrant must give 'conditional approval' for ASIO to do one or more of the following things: 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 the post or access articles that are being delivered by a delivery service provider. However, the Minister must not grant 'conditional approval' under an identified person warrant for ASIO to exercise foreign intelligence collection powers (akin to those contained in existing section 27A) or exercise questioning and questioning-detention powers (akin to those contained in subdivisions B or C of Division 3 of Part III of the ASIO Act).

370. Once again, 'conditional approval' does not, of itself, authorise ASIO to do the things for which 'conditional approval' has been given. Separate authorisation must be obtained from the Minister or the Director-General before undertaking one or more of the things for which conditional approval has previously been granted.

Duration of warrant

371. Subsection 27C(4) provides that an identified person warrant must specify a period, not exceeding 6 months, during which the warrant is to remain in force. This is consistent with the period for which most warrants issued to ASIO may remain in force.

372. However, the Minister may revoke the identified person warrant before this period expires, which is consistent with the existing warrant provisions.

Issue of further warrants not prevented

373. Subsection 27C(5) clarifies that subsection 27C(4) (Duration of warrants) does not prevent further warrants being issued.

Warrant may be subject to restrictions or conditions

374. Subsection 27C(6) provides that an identified person warrant is subject to any restrictions or conditions specified in the warrant.

Section 27D – Authority under identified person warrant—search of premises and persons

375. Where an identified person warrant gives conditional approval for ASIO to access records or other things in or on premises in relation to a person (the identified person), section 27D permits ASIO to request that the Minister or the Director-General authorise ASIO to do one or more of the things listed in subsection 27D(2) in relation to one or more specified premises.

Things that may be authorised under warrant

376. The specific things that may be authorised are similar to those that may be authorised under an existing search warrant under section 25, as amended by this Schedule.

377. Subsection 27J(1) (general rules) provides that if the request is to the Minister, it must be made by the Director-General, and if the request is to the Director-General, it may be made by an ASIO employee or an ASIO affiliate.

Test for authorisation

378. Subsection 27D(3) requires the Minister or Director-General be satisfied, on reasonable grounds, that doing the thing or things under the warrant, as specified in the authorisation in relation to the subject premises, will substantially assist the collection of intelligence relevant to the 'prejudicial activities' of the identified person (defined in section 22).

379. By comparison, the Minister may only issue a search warrant under section 25 of the ASIO Act if he or she is satisfied that there are reasonable grounds for believing that access by ASIO to records or other things on the subject premises will substantially assist the collection of intelligence in respect of a matter that is important in relation to security.

380. By requiring the Minister or Director-General to be satisfied that doing the specified thing or things will substantially assist the collection of intelligence relevant to the 'prejudicial activities' of the identified person, rather than in respect of broader matters in relation to security, subsection 27D(3) imposes a more stringent test for the issuing of an authorisation.

381. This more stringent test is consistent with the purpose of the identified person warrant regime, which is to allow ASIO to investigate particular persons with greater efficiency without reducing the thresholds or accountability mechanisms.

382. The list of things that may be authorised under subsection 27D(2) is based on the things that may be specified in a search warrant issued under section 25, as amended by this Bill. However, the Minister or Director-General may only authorise ASIO to do the things specified under paragraphs 27D(2)(c), (d), (e) and (h) in relation to the prejudicial activities of the identified person. By comparison, the Minister may authorise ASIO to do the equivalent things under a search warrant issued under section 25 of the ASIO Act where they would be relevant to the security matter specified in the warrant. Limiting the scope of the things that the Minister or Director-General may authorise ASIO to do under an identified person warrant to things that are relevant to the 'prejudicial activities' of the identified person is consistent with the purpose of the identified person warrant regime, which is to allow ASIO to investigate particular persons with greater efficiency without weakening thresholds or reducing accountability.

Additional rules applying to authorisations

383. The additional rules applying to authorisations given under section 27D, set out in subsections 27D(4) and (5), reflect the rules currently contained in subsection 25(4C) and section 25AA. Similarly, the restriction contained in subsection 27D(6) relating to strip searches and searches of a person's body cavities reflect the restrictions currently contained in subsection 25(4B).

384. Similar to existing search warrants issued under section 25, the Minister or Director-General can authorise using a computer on the subject premises if there is reasonable cause to believe that data relevant to the prejudicial activities may be accessible by using a computer or other electronic equipment or a data storage device on the premises being searched. As such, subsection 27D(7) contains a prohibition on material interference with the lawful use of the computer by other persons. This amendment is consistent with subsections 25(6) and 25A(5), as modified by this Bill.

385. As previously noted, subparagraph 27C(4) provides that an identified person warrant must specify a period, not exceeding 6 months, during which the warrant is to remain in force. However, paragraph 27J(5)(a) (general rules) provides that an authorisation under section 27D must not specify a period – during which the authorisation is in force – that exceeds 90 days. This 90-day limit is consistent with the maximum period during which a search warrant issued under section 25 may be in force.

Section 27E – Authority under identified person warrant—computer access

386. Where an identified person warrant gives conditional approval for ASIO to access data held in computers in relation to a person (the identified person), section 27E permits

ASIO to request that the Minister or the Director-General authorise ASIO to do one or more of the things listed in subsection 27E(2) in relation to a 'target computer'.

387. The specified things that may be authorised are similar to those things that may be authorised under a computer access warrant under section 25A, as amended by this Bill.

388. Subsection 27E(3) defines 'target computer' in identical terms to subsection 25A(3), as amended by this Bill.

389. Subsection 27E(4) requires the Minister or Director-General be satisfied, on reasonable grounds, that doing the thing or things under the warrant, as specified in the authorisation in relation to the target computer, will substantially assist the collection of intelligence relevant to the 'prejudicial activities' of the identified person (defined in section 22).

390. By comparison, the Minister may only issue a computer access warrant under section 25A of the ASIO Act if he or she is 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 respect of a matter that is important in relation to security.

391. By requiring the Minister or Director-General to be satisfied that doing the specified thing or things will substantially assist the collection of intelligence relevant to the 'prejudicial activities' of the identified person, rather than in respect of a potentially broader matter that is important in relation to security, subsection 27E(4) imposes a more stringent test for the giving of an authorisation.

392. This more stringent test is consistent with the purpose of the identified person warrant regime, which is to allow ASIO to investigate particular persons with greater efficiency without weakening thresholds or reducing accountability.

393. Subsection 27J(1) (general rules) provides that if the request is to the Minister, it must be made by the Director-General, and if the request is to the Director-General, it may be made by an ASIO employee or an ASIO affiliate.

Things that may be authorised

394. The list of things that may be authorised under subsection 27E(2) is based on the things that may be specified under computer access warrant issued under section 25A, as amended by this Bill.

395. However, the Minister or Director-General may only authorise ASIO to do the things specified under subsection 27E(2) if satisfied that on reasonable grounds the doing of the things in relation to the target computer will substantially assist the collection of intelligence relevant to the prejudicial activities of the identified person.

396. By comparison, the Minister may authorise ASIO to do the equivalent things under a computer access warrant issued under section 25A of the ASIO Act for the purpose of obtaining access to data that is relevant to the security matter specified in the warrant.

397. Limiting the scope of the things that the Minister or Director-General may authorise ASIO to do under an identified person warrant, to the things that are for the purpose of

obtaining access to data that is relevant to the 'prejudicial activities' of the identified person, is consistent with the purpose of the identified person warrant regime, which is to allow ASIO to investigate particular persons with greater efficiency without weakening thresholds or reducing accountability.

Certain acts not authorised

398. Subsection 27E(5) contains a limitation on ASIO's power to do things under an identified person warrant that have been authorised under subsection 27E(2). This limitation is consistent with the modified limitation contained in subsection 25A(5).

Section 27F – Authority under identified person warrant—surveillance devices

399. Where an identified person warrant gives conditional approval for ASIO to use one or more kinds of surveillance devices in relation to a person (the identified person), section 27F permits ASIO to request that the Minister or the Director-General authorise ASIO to do one or more of the things listed in subsection 27F(2).

400. The specific things that may be authorised are similar to those that may be authorised under existing sections 26 to 26C, as amended by this Bill.

401. Subsection 27F(3) provides that the Minister or Director-General may only give an authorisation under section 27F where satisfied, on reasonable grounds, that doing the thing or things under the warrant, as specified in the authorisation, will substantially assist the collection of intelligence relevant to the 'prejudicial activities' of the identified person (defined in Section 22).

402. By comparison, current paragraph 26(3)(a), as amended by this Bill, requires the Minister to satisfy a two-part test before issuing a surveillance devices warrant in relation to a particular person. Firstly, the Minister must be satisfied 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, activities prejudicial to security. Secondly, the Minister must be satisfied that the use by ASIO of a surveillance device in relation to that person will, or is likely to, assist ASIO in carrying out its function of obtaining intelligence relevant to security.

403. By requiring the Minister or Director-General to be satisfied that doing the specified thing or things will substantially assist the collection of intelligence relevant to the 'prejudicial activities' of the identified person, rather than the potentially broader ground of assisting ASIO in carrying out its function of obtaining intelligence relevant to security, subsection 27F(3) imposes a more stringent test for the giving of an authorisation.

404. This more stringent test is consistent with the purpose of the identified person warrant regime, which is to allow ASIO to investigate particular persons with greater efficiency without weakening thresholds or reducing accountability.

405. Subsection 27J(1) (general rules) provides that if the request is to the Minister, it must be made by the Director-General, and if the request is to the Director-General, it may be made by an ASIO employee or an ASIO affiliate.

Things that may be authorised under warrant

406. The list of things that may be authorised under subsections 27F(2), (4) and (5) is based on the things that are authorised in a surveillance devices warrant issued in relation to a particular person under new section 26B.

407. The identified person warrant regime does not contain a comparable power to subparagraphs 26(2)(a)(ii) and (iii) of the ASIO Act, as amended by this Bill, which would allow the Minister to issue a warrant in relation to particular premises or an object or class of objects. This is consistent with the limited purpose of the identified person warrant regime, which is to allow ASIO to investigate identified persons.

408. The requirement for the Minister or Director-General to separately authorise each of the things listed in subsection 27F(2), represents an additional safeguard in the identified person warrant regime, compared to a surveillance device warrant issued by the Minister in relation to a particular person, which authorises each of the things listed in subsection 26B(1).

Section 27G – Authority under identified person warrant—inspection of postal articles

409. Where an identified person warrant gives conditional approval for ASIO to access postal articles while the articles are in the course of the post in relation to a person (the identified person), section 27G permits ASIO to request that the Minister or the Director-General authorise ASIO to do one or more of the things listed in subsection 27G(3) in relation to a postal articles of the kind listed in subsection 27G(2).

410. The specified things that may be authorised are similar to those that may be authorised under existing section 27, as amended by this Bill.

411. Subsection 27J(1) (general rules) provides that if the request is to the Minister, it must be made by the Director-General, and if the request is to the Director-General, it may be made by an ASIO employee or an ASIO affiliate.

Test for authorisation

412. Subsection 27G(4) requires the Minister or Director-General to be satisfied, on reasonable grounds, that doing the thing or things under the warrant, as specified in the authorisation will substantially assist the collection of intelligence relevant to the 'prejudicial activities' of the identified person (defined in Section 22).

413. By comparison, subsection 27(2) requires the Minister to satisfy a two-part test before issuing an inspection of postal articles warrant in relation to a person. Firstly, the Minister must be satisfied 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, activities prejudicial to security. Secondly, the Minister must be satisfied that access by ASIO to postal articles posted by or on behalf of, addressed to or intended to be received by, that person while the articles are in the course of the post will, or is likely to, assist ASIO in carrying out its function of obtaining intelligence relevant to security.

414. By requiring the Minister or Director-General to be satisfied that doing the specified thing or things will substantially assist the collection of intelligence relevant to the 'prejudicial activities' of the identified person, rather than the potentially broader ground of

assisting, or being likely to assist, ASIO in carrying out its function of obtaining intelligence relevant to security, subsection 27G(4) imposes a more stringent test for the giving of an authorisation. This more stringent test is consistent with the purpose of the identified person warrant regime, which is to allow ASIO to investigate particular persons with greater efficiency without weakening thresholds or reducing accountability.

Rules relating to the Australian Postal Corporation

415. Subsections 27G(5), (6) and (7) set out rules relating to the Australian Postal Corporation. These rules are modelled on the existing rules in subsections 27(6), (6A) and (7).

416. Subsection 27G(8) sets out the relationship between authorisations made under section 27G, between Part VIIA of the *Crimes Act 1914* and between the *Australian Postal Corporation Act 1989*. This provision is modelled on existing subsection 27(8).

Section 27H – Authority under identified person warrant—inspection of delivery articles

417. Where an identified person warrant gives conditional approval for ASIO to access 'articles' while the articles are being delivered by a 'delivery service provider' in relation to a person (the identified person), section 27H permits ASIO to request that the Minister or the Director-General authorise ASIO to do one or more of the things listed in subsection 27H(3) in relation to articles of the kind listed in subsection 27H(2) ('article' and 'delivery service provider' are defined in subsection 27H(5)).

418. The specified things that may be authorised are similar to those that may be authorised under existing section 27AA, as amended by this Schedule.

419. Subsection 27J(1) (general rules) provides that if the request is to the Minister, it must be made by the Director-General, and if the request is to the Director-General, it may be made by an ASIO employee or an ASIO affiliate.

Things that may be authorised under warrant

420. The kinds of articles listed in subsection 27H(2), and the list of things that may be authorised under subsection 27H(3), reflect the current language used in paragraph 27AA(4)(b) and subsection 27AA(5) which set out the things that the Minister may authorise under a section 27AA inspection of delivery service articles warrant.

Test for authorisation

421. Subsection 27H(4) requires the Minister or Director-General be satisfied, on reasonable grounds, that doing the thing or things under the warrant, as specified in the authorisation will substantially assist the collection of intelligence relevant to the 'prejudicial activities' of the identified person (defined in Section 22).

422. By comparison, subsection 27AA(2) of the ASIO Act requires the Minister to satisfy a two-part test contained in either subsection 27AA(3) or 27AA(6) before issuing an inspection of articles warrant in relation to a person.

423. Under subsection 27AA(3), the Minister must first be satisfied 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, activities prejudicial to security. Secondly, the Minister must be satisfied that access by ASIO to articles sent by or on behalf of, addressed to or intended to be received by, the subject while the articles are being delivered by a delivery service provider, will, or is likely to, assist ASIO in carrying out its function of obtaining intelligence relevant to security.

424. Under subsection 27AA(6), the Minister must first be satisfied that some or all of the articles that are being, or are likely to be, sent by a delivery service provider to an address are, or will be intended to be, received by a person (whether of known identity or not) engaged in, or reasonably suspected by the Director‑General of being engaged in, or of being likely to engage in, activities prejudicial to security. Second, the Minister must be satisfied that access by ASIO to articles sent to, or intended to be received by, the subject while the articles are being delivered by a delivery service provider will, or is likely to, assist ASIO in carrying out its function of obtaining intelligence relevant to security.

425. By requiring the Minister or Director-General to be satisfied that doing the specified thing or things will substantially assist the collection of intelligence relevant to the 'prejudicial activities' of the identified person, rather than the potentially broader grounds of assisting or being likely to assist ASIO in carrying out its function of obtaining intelligence relevant to security, subsection 27H(4) imposes a more stringent test for the giving of an authorisation. This more stringent test is consistent with the purpose of the identified person warrant regime, which is to allow ASIO to investigate particular persons with greater efficiency without weakening thresholds or reducing accountability.

Section 27J – Authority under identified person warrants—general rules

426. Section 27J sets out the general rules that apply to requests for authorisations and when authorisations cease to be in force under an identified person warrant.

Requests for authorisations

427. Subsection 27J(1) provides that if the request is to the Minister, it must be made by the Director-General, and if the request is to the Director-General, it may be made by an ASIO employee or an ASIO affiliate.

428. Subsection 27J(2) is an avoidance of doubt provision that provides that a request for an authorisation under an identified person warrant must specify the necessary facts and grounds which justify the authorisation being sought.

Requirements for authorisations

429. Subsection 27J(3) provides the general requirements for an authorisation under an identified person warrant. Specifically, the authorisation must identify the identified person, specify the subject premises, target computer, things authorised to be done, restrictions or conditions (if any) and the period the warrant is in force, must authorise the use of any force that is necessary and reasonable and where authorising entry to premises, specify the time of entry (day or night).

430. Subsection 27J(4) is an important safeguard which clarifies that a restriction or condition in an authorisation (for example, a condition on an authorisation under section 27D regarding the search of a premises or person) must not be inconsistent with a restriction or conditions specified in an identified person warrant under which an authorisation is given. The intention is that a condition or restriction contained in an authorisation may not override a restriction or condition contained in the identified person warrant under which the authorisation is given.

431. Subsection 27J(5) sets out the maximum period that an authorisation under an identified person warrant may be specified to be in force. An authorisation must not end after the period during which an identified person warrant, under which the authorisation is issued, is in force. An additional limitation to this requirement applies to authorisations issued under section 27D (search of premises and persons) which must not be more than 90 days. This 90-day limit is consistent with the maximum period during which a search warrant issued under section 25 of the ASIO Act may be in force.

When authorisations cease to be in force

432. Subsection 27J(6) clarifies the earliest time that an authorisation under an identified person warrant will cease to be in force.

Other matters

433. Subsection 27J(7) clarifies that the authority conferred by an identified person warrant also includes the authority conferred by the authorisation that is issued under an identified person warrant.

434. Subsection 27J(8) is an avoidance of doubt provision to ensure that multiple authorisations may be issued under an identified person warrant. It is likely that more than one authorisation will be issued under an identified person warrant with respect to each type of warrant power (for example, multiple authorisations involving searches, computer access and surveillance devices could be issued under a single identified person warrant).

435. Subsection 27J(9) makes it clear that a determination made under section 27J is not a legislative instrument. This provision is merely declaratory in nature. Determinations of this type are administrative in character because they are merely the application of a legal power in a particular case, they do not determine or alter the content of the law itself.

Item 42 – Before section 28

436. This item separates Division 2 into subdivisions and inserts the title of the eighth subdivision, 'Subdivision H – General provisions relating to warrants'.

Item 43 – Paragraph 29(1)(a)

437. This item removes the references to, '26B, 26C'.

Item 44 – After section 29

438. This item inserts new section 29A which provides Ministerial discretion to vary warrants issued under Division 2 of Part III on request by the Director-General, other than emergency warrants issued under section 29.

439. Section 29A provides that a warrant cannot be varied to extend the total period for which it is in force, beyond 90 days for search warrants, and beyond a total period of 6 months for all other warrants issued by the Minister under Division 2 of Part III.

440. Paragraph 29A(4)(b) has been included to cover surveillance device warrants in circumstances where a warrant was originally sought in relation to premises or objects and then an application is made for variation to apply the warrant to a person. In these circumstance, it is appropriate that the Director-General's request to vary that type of warrant should specify, where appropriate, the grounds on which the person is engaged in, or reasonably suspected by the Director-General of being engaged in, or of being likely to engage in, activities 'prejudicial to security', as the original test required under section 26 (issue of surveillance device warrants) would not have otherwise been met. To avoid doubt, the words 'where appropriate' are only to apply in circumstances where ASIO is seeking to vary an existing surveillance device warrant to apply to a particular person, where it did not previously. This safeguard at paragraph 29A(4)(b) will ensure that the threshold (test) at paragraph 26(3)(a) is met at some point in the warrant variation process. Further, this power will only be used for variations of a relatively minor nature. Where there have been significant changes to the circumstances which applied when the original warrant was issued, a new warrant will be sought.

Item 45 – Section 30

441. This item repeals and replaces section 30 which requires the Director-General, if satisfied that the grounds on which a warrant issued under Division 2 of Part III have ceased to exist – as soon as practicable – the Director-General is to inform the Minister and take such steps as are necessary to ensure that action under the warrant is discontinued.

442. Subsection 30(2) clarifies that, for the purpose of paragraph 30(1)(b), an 'action under a warrant' includes action under an authorisation given under the new identified person warrants, but does not include the recovery of a surveillance device or any enhancement equipment in relation to the device.

443. Subsection 30(3) applies only in relation to surveillance device warrants and ensures the preservation of a warrant that has been issued in respect of a number of matters, for the remainder of the matters, where the facts and grounds of those remaining matters still exist. As a surveillance device warrant can be issued in relation to multiple matters (for example, a particular person, particular premises and/or an objection or a class of object) subsection 30(3) ensure that requirements set out in subsection (1) are limited to only those matters where the grounds on which the warrant was issued have ceased to exist. It is only the matter, in respect of which the facts and grounds have ceased to exist, that is to be removed from the warrant. As such, where the grounds in relation to the remaining matters continue to exist, ASIO is not required to inform the Minister or take such steps as listed under section 30.

Item 46 – After section 32

444. This item inserts a new section 33 which sets out the relationship between this Division and other laws, specifically the TIA Act and other laws in relation to the use of surveillance devices.

Computer access – relationship with the Telecommunications (Interception and Access) Act 1979

445. New subsection 33(1) provides that nothing in sections 25A, 27A or 27E, or a warrant or authorisation under those sections, authorises the interception of a communication passing over a telecommunications system operated by a carrier or carriage service provider, within the meaning of the TIA Act. This restriction is intended to operate in respect of ASIO's powers relating to computers and communications in transit contained in those sections.

446. This amendment provides additional safeguards and accountability mechanisms as a consequence of the changes to sections 25A and the related sections 27A and 27E, including for example, a computer access warrant being able to authorise the use of a communication in transit and adding, copying, deleting or altering data in the communication in transit. The new subsection 33(1) provides that those sections, and warrants and authorisations under those sections, cannot authorise the interception of a communication for the purposes of the TIA Act. Instead, in the event that ASIO seeks to intercept communications, it will need to apply for a warrant under the TIA Act (unless otherwise exempted under the TIA Act). ASIO can still continue to access stored communications under a computer access warrant.

Listening devices – relationship with the Telecommunications (Interception and Access) Act 1979

447. New subsection 33(2) preserves existing subsections 26(8) and 27A(5) and extends to cover section 27F. It provides that nothing in sections 26B, 27A and 27F, or a warrant or authorisation under those sections, applies in relation to the use of a listening device for a purpose that would constitute the interception of a communication passing over a telecommunications system operated by a carriage service provider under the TIA Act. In those circumstances, ASIO would be required to obtain a warrant under Part 2-2 of the TIA.

Surveillance devices – interaction with other laws

448. New subsection 33(3) makes it clear that a person acting on behalf of the Organisation does not act unlawfully by installing, using or maintaining a surveillance device, with or without a warrant as provided for in Division 2, where those activities are lawfully done under the ASIO Act.

Item 47 – At the end of Division 2 of Part III

449. This item adds a new evidentiary certificates regime at section 34AA. The regime seeks to protect the identity of ASIO officers, sources and sensitive capabilities connected with the execution of a warrant.

450. The regime is to work in a similar fashion to the existing schemes under the *Telecommunications (Interception and Access) Act 1979* and *Surveillance Devices Act 2004*

and is to complement the framework under the *National Security Information (Criminal and Civil Proceedings) Act 2004*.

451. The regime will allow the Director-General of Security (or a Deputy Director-General) to issue an evidentiary certificate with respect to acts or things done by, on behalf of, or in relation to ASIO in connection with a warrant issued under sections 25A (computer access) or 26 (surveillance devices), or an authorisation given under section 27F (surveillance devices) or in accordance with the relevant authorising provisions allowing use of surveillance devices without warrants (sections 26C, 26D, and 26E).

452. The regime will also allow the Director-General (or a Deputy Director-General) to issue an evidentiary certificate with respect to acts or things done by, on behalf of, or in relation to ASIO in connection with a warrant issued under sections 27A (foreign intelligence warrant), 27C (identified person warrant) or 29 (emergency warrant), but only if but only if those acts or things are authorised under section 25E (computer access) or 25F (surveillance devices) under the warrant, and only with respect to those acts or things.

453. The regime is framed to ensure that an evidentiary certificate will only cover the manner in which the evidence was obtained (using the above powers) and not the evidence itself. As such, the court will retain its ability to test the weight and veracity of evidence put before it.

454. For operational security reasons, the proposed regime does not provide a conclusive list of the facts that the Director-General or a Deputy Director-General may issue in a written certificate. The regime is not intended to provide a means for the prosecution to provide proof of any ultimate fact, or any fact so closely connected with an ultimate fact so as to be indistinguishable from it, or facts that go to elements of the offence, without recourse for the course or the defendant to challenge the certificate and the facts it covers.

455. Subsection 34AA(2) of the regime clarifies that the certificates are to be prima facie evidence of the matters stated in the certificate (that is, certificates issued under the regime will be persuasive before a court, as distinct from a conclusive certificate that cannot be challenged by a court or a defendant).

Part 2 – Consequential amendments

Telecommunications (Interception and Access) Act 1979

Item 48 – After paragraph 108(2)(c)

456. This item inserts a new paragraph 108(2)(ca) to TIA Act. This is a consequential amendment to provide an exception for ASIO to access a stored communication, under an authorisation given under the new identified person warrant, in accordance with new section 27E of the ASIO Act (authority under identified person warrant—computer access). This exception is consistent with the existing exception under paragraph 108(2)(c) of the TIA for ASIO to access a stored communication under a computer access warrant issued under section 25A of the ASIO Act.

Item 49 – At the end of paragraph 108(2)(f)

457. This item inserts a new subparagraph 108(2)(f)(iv) to the TIA Act. This is a consequential amendment to provide an exception for ASIO to access a stored communication in order to install, connect or maintain equipment used, or to be used, for accessing a stored communication, under an authorisation under the new identified person warrant, in accordance with new section 27E of the ASIO Act (Authority under identified person warrant – computer access). This exception is consistent with the existing exception under subparagraph 108(2)(f)(iii) of the TIA Act for ASIO to access a stored communication in order to install, connect or maintain equipment used, or to be used, for accessing a stored communication, under a computer access warrant issued under section 25A of the ASIO Act.

Part 3 – Application, transitional and savings provisions

Item 50 – Application, transitional and savings provisions

458. Paragraph 1 of this item provides that amendments made by this Schedule do not apply to warrants requested before, or issued before, the commencement of this Schedule.

459. Paragraph 2 provides that if a person was approved to exercise the authority under a warrant for the purposes of subsection 24(1) of the ASIO Act prior to commencement of this Schedule, the person will be taken to be a person approved under subsection 24(2) of that Act as amended by this Schedule after the commencement of this Schedule.

460. Paragraph 3 provides that if a person was an authorising officer for the purposes of subsection 24(1) of the ASIO Act prior to commencement of this Schedule, the person will be taken to be a person appointed under subsection 24(3) of that Act as amended by this Schedule after its commencement.

461. Paragraph 4 provides that section 34AA of the ASIO Act, relating to evidential certificates, applies to warrants issued and authorisations given after, and proceedings commenced after, the commencement of this Schedule.

Schedule 3—Protection for special intelligence operations

Overview of measures

462. Schedule 3 amends Part III of the *Australian Security Intelligence Organisation Act 1979* (ASIO Act) by inserting a new Division 4, which establishes a statutory framework for the conduct of special intelligence operations (SIOs) by ASIO. The purpose of the SIO scheme is to ensure that the Organisation can continue to collect intelligence by ensuring its capacity to gain close access to sensitive information via covert means.

463. New Division 4 implements a recommendation of the Parliamentary Joint Committee on Intelligence and Security (PJCIS) *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation* of May 2013 (PJCIS Report). The PJCIS recommended that an SIO scheme be established, similar to the controlled operations regime in Part IAB of the *Crimes Act 1914* (Crimes Act) in relation to the covert activities of law enforcement agencies. While the SIO scheme is based broadly on the controlled operations scheme in the Crimes Act, appropriate modifications have been made to reflect the differences between a law enforcement operation to investigate a serious criminal offence in order to gather admissible evidence, and a covert intelligence-gathering operation conducted for national security purposes.

464. As the PJCIS recognised, a legislative framework for the conduct of SIOs is necessary to ensure that ASIO officers, employees and agents will have appropriate legal protections when conducting covert operations for the purpose of carrying out functions in under the ASIO Act. ASIO's ability to collect useful and relevant intelligence on the most serious threats to the security of Australia and Australians is significantly dependent on its capacity to covertly gain and maintain access to highly sensitive information. This activity can involve engaging and associating with those who may be involved in criminal activity, and therefore has the potential to expose ASIO employees or affiliates to criminal or civil liability in the course of their work.

465. In particular, a number of offences relating to the protection of the security of the Commonwealth are directed to conduct that is ancillary to the actual carrying out of a security threat. For example, some offences in Division 102 of the Criminal Code 1995 (Criminal Code) relate to a person's engagement with a terrorist organisation (such as membership, direction, recruitment, training, funding, providing support and association). While such offences are necessary to protect Australia's security interests by isolating terrorist organisations from the community, they are technically capable of capturing the activities of persons who associate covertly with targets for the purpose of authorised intelligence collection activities. Hence, there is a theoretical possibility that such conduct could be the subject of a criminal prosecution.

466. For example, it is an offence under subsection 102.5(2) of the Criminal Code for a person to intentionally provide training to, or receive training from, a listed terrorist organisation. Therefore, if an ASIO employee or an ASIO affiliate is tasked to collect covert intelligence in relation to a listed terrorist organisation or its members, they may be exposed to criminal liability under subsection 102.5(2) if, in the course of collecting the relevant intelligence, they receive training from that organisation (for instance, by attending a training session). Other offences may also arise in the course of obtaining information in relation to a

security threat, such as dealing with proceeds of crime, or complicity in another person's attempt to commit an offence.

467. At present, some significant covert operations either do not commence or are ceased due to the risk that participants could be exposed to criminal or civil liability. Given the significant benefit to Australia's security that is derived from the collection of intelligence via covert operations, it is appropriate to address this issue by removing the possibility that a person could be exposed to conviction for a criminal offence, or civil liability, in respect of his or her conduct in the course of, and as part of, an authorised SIO. While, in the absence of a statutory immunity, the commencement or continuation of a prosecution is dependent on the exercise of prosecutorial discretion, a limited immunity is considered preferable as a matter of policy because it removes the possibility that conduct in accordance with an authorised SIO could be investigated or referred for prosecution. A limited immunity, in the form of the SIO regime under new Division 4, is considered preferable to the potential alternative of conferring upon SIO participants a wholesale immunity from criminal liability. Limiting the immunity to specifically authorised conduct in particular operations will ensure that it is enlivened only where a case has been established for its application.

468. The limited immunity conferred by the new Division 4 is subject to rigorous safeguards. In particular, its application is limited to a person's conduct that is undertaken as part of an authorised SIO, which the person is authorised to undertake by the relevant SIO authority. The Division further establishes an application-based scheme for SIOs, with authorities granted by the Director-General of Security (Director-General) or a Deputy Director-General of Security (Deputy Director General) only on the basis of strict issuing criteria. In addition, conduct permitted to be authorised under an SIO cannot include that which would require authorisation under a warrant issued under the ASIO Act, or a warrant or authorisation under the Telecommunications (Interception and Access) Act 1979 (TIA Act).

469. The operation of Division 4 is also subject to specific reporting requirements to the Minister and to the Inspector-General of Intelligence and Security (IGIS) and to Ministers and the Parliament via the Organisation's annual report. It is further subject to the extensive independent oversight mechanisms that apply to the Organisation's activities. These include the oversight role of the IGIS and the PJCIS.

Item 1 – Section 4

470. Item 1 amends section 4 of the ASIO Act to provide for the definition of terms used in the SIO scheme established by Division 4. Item 1 inserts definitions of the terms 'authorising officer', 'engage in conduct', 'participant', 'special intelligence conduct', 'special intelligence function', 'special intelligence operation' and 'special intelligence operation authority'.

Authorising officer

471. An authorising officer for the purpose of Division 4 of Part III means the Director-General or a Deputy Director-General.

472. An authorising officer is empowered by sections 35C, 35F and 35G to grant, vary or cancel an SIO authority (also a defined term in section 4). The role and function of an authorising officer is non-delegable.

Engage in conduct

473. This phrase has the same meaning as in subsection 4.1(2) of the Criminal Code, being to do an act or to omit to perform an act.

474. This phrase is relevant principally to a person's engagement in special intelligence conduct (also a defined term in section 4) as authorised under a special intelligence authority (also a defined term in section 4). Immunity from liability in section 35K applies to special intelligence conduct, provided that the conditions specified in subsection 35K(1) are satisfied. It is also relevant to offences for contravening safeguards relating to questioning warrants and questioning and detention warrants in section 34ZF of the ASIO Act (see item 2 below).

Participant

475. A participant in an SIO is defined as a person who is authorised under Division 4 of Part III to engage in special intelligence conduct for the purposes of the SIO.

476. This term ensures that both the SIO, and an individual person's conduct, must be authorised specifically by an SIO authority.

Special intelligence conduct

477. Special intelligence conduct means conduct for or in relation to which a person would, but for the immunity provision in section 35K, be subject to civil or criminal liability under a law of the Commonwealth, a State or a Territory.

478. This term is applied in the definition of an SIO authority in section 4, with the result that such an authority must specifically authorise both the conduct to be engaged in as part of an SIO, and the persons ('participants' as defined in section 4) who are permitted to engage in that conduct. This term ensures that the scope of authority is particularised and limited appropriately in an SIO authority.

Special intelligence function

479. A special intelligence function means one or more of the following functions of the Organisation under section 17 of the ASIO Act:

- obtaining, correlating and evaluating intelligence relevant to security (as that term is defined in section 4): paragraph 17(1)(a) or
- for purposes relevant to security, communicating such intelligence to such persons, and in such manner, as are appropriate to those purposes: paragraph 17(1)(b) or
- obtaining within Australia foreign intelligence, and communicating such intelligence in accordance with applicable statutory requirements: paragraph 17(1)(e), or

- co-operating with and assisting bodies referred to in section 19A in accordance with that section: paragraph 17(1)(f). These bodies are specified members of the Australian Intelligence Community, a law enforcement agency, or a Commonwealth or State authority prescribed by regulations.

480. The special intelligence functions are limited to the Organisation's functions under section 17 of the ASIO Act, except for its advisory functions under paragraphs 17(1)(c), (ca) and (d)). This means that a special intelligence function does not include, for example, advising Ministers and other persons or Commonwealth authorities on matters relating to security or protective security, or furnishing security assessments to a State. It is intended that any relevant information obtained from an SIO may be used for the performance of the Organisation's advisory functions in section 17, but it is not necessary for an SIO to be authorised specifically for those functions. It is also considered appropriate that ASIO employees or ASIO affiliates (as these terms are defined in section 4 of the ASIO Act by reason of Schedule 1 to this Bill) or other persons who perform the Organisation's advisory functions under section 17 are subject to laws of general application.

Special intelligence operation

481. A special intelligence operation (SIO) is the key defined term in section 4 for the purposes of the new Division 4 of Part III. An SIO is an operation in relation to which an SIO authority has been granted, that is carried out for a purpose relevant to the performance of one or more special intelligence functions and that may involve an ASIO employee or ASIO affiliate in special intelligence conduct.

482. This term is significant because the immunity from liability in section 35K applies exclusively to conduct that is engaged in as part of an SIO that is authorised and carried out in accordance with the requirements of Division 4 of Part III.

Special intelligence operation authority

483. A special intelligence operation authority (an SIO authority) means an authority to conduct an SIO granted under section 35C. Only an authorising officer (as defined in section 4) may grant an SIO authority following an application of an ASIO employee made under section 35B.

Item 2 – Subsection 34ZF(8)

484. Item 2 repeals subsection 34ZF(8) as a consequential amendment to item 1 of this Schedule. Subsection 34ZF(8) defines the term 'engage in conduct' for the purpose of section 34ZF of the ASIO Act (offences for contravening safeguards applying to warrants issued under Division 3 of Part III). This definition is no longer necessary because the term is now included in the general definitional provisions in section 4.

Item 3 – At the end of Part III

485. Item 3 inserts a new Division 4 in Part III (functions and powers of the Organisation), which establishes the SIO regime. Division 4 contains new sections 35A-35R.

New section 35A – Relationship to other laws and matters

486. Courts have a general discretion to exclude evidence that was obtained through unlawful conduct. New section 35A provides statutory guidance in the exercise of this discretion in relation to intelligence obtained as part of an SIO that is required to be used as evidence. This is necessary because participants in an SIO may be authorised to engage in conduct that constitutes a criminal offence for the sole purpose of executing an SIO in accordance with the relevant SIO authority. Section 35A will ensure that such evidence is not excluded automatically.

487. Subsection 35A(1) expressly preserves general judicial discretion in relation to the admission or exclusion of evidence, or to stay criminal proceedings, subject to two modifications. The first is in subsection 35A(2), which provides that a court may not exclude evidence solely because it was obtained as a result of a person's engagement in a criminal activity, if the person was a participant in an SIO, and the relevant conduct was within the scope of the SIO authority. Subsection 35A(2) applies exclusively to evidence obtained as a result of conduct that is authorised under an SIO. It does not extend to evidence obtained as a result of conduct which exceeds the scope of authority under an SIO authority, or conduct which pre-dated the grant of the authority.

488. The second modification to the general position in subsection 35A(1) is that an authorising officer may, under section 35R, issue an evidentiary certificate in respect of any factual matters relevant to the granting of an SIO. Such a certificate is taken as prima facie evidence of the matters stated in the certificate.

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

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

New section 35B – Applications for authorities to conduct special intelligence operations

491. New section 35B provides for an application-based authorisation scheme in relation to SIOs. This ensures that the immunity from criminal or civil liability is limited only to those operations which are the subject of an authority granted in accordance with Division 4.

SIO Application may be made to an authorising officer – subsection 35B(1)

492. Subsection 35B(1) provides that an ASIO employee may apply to an authorising officer (being the Director-General or a Deputy Director-General) for an authority to conduct an SIO on behalf of the Organisation.

493. The authorisation process for an SIO is internal to the Organisation, which appropriately reflects the fact that the conduct of SIOs is an internal, operational matter, on which the Director-General or a Deputy Director-General is best placed to make decisions given their detailed awareness of the security environment, and their practical expertise in relation to the conduct of intelligence operations. The internal authorisation process established by Division 4 is further necessary to facilitate operational efficiency and protect the security of covert intelligence operations. In addition to the scrutiny of an application by the authorising officer (who holds an appropriately senior position within the Organisation), accountability and oversight arrangements are given effect via reporting requirements in new section 35Q and subsection 94(1C) (detailed below). In short, these provisions establish, respectively, the Organisation's reporting requirements to the Minister and the IGIS on the exercise of powers under Division 4, and a reporting requirement to the Parliament as part of the Organisation's annual report.

494. These requirements are additional to the general jurisdiction of IGIS to examine all of the Organisation's activities, including those in relation to SIOs, under section 8 of the *Inspector-General of Intelligence and Security Act 1986* (IGIS Act), and the mandate of the PJCIS to conduct inquiries into such activities on a reference from the Attorney-General, or on a resolution of either House of the Parliament under section 29 of the *Intelligence Services Act 2001* (IS Act).

Form requirements in relation to SIO applications – subsections 35B(2) and (4)

495. Subsection 35B(2) sets out the form an SIO application is required to take. Paragraph 35B(2)(a) provides that an application must be in writing and signed by the applicant.

496. Paragraph 35B(2)(b) provides an alternative to the form requirement in paragraph 35B(2)(a) in circumstances of urgency. It is available if an applicant has reason to believe that the delay caused by making a written application may be prejudicial to security. In this event, the application may be made orally in person, by telephone, or other means of communication. In the event that an application is made under paragraph 35B(2)(b), subsection 35B(4) further requires the applicant, as soon as practicable after making the application, to make a written record of it and to give this record to the authorising officer.

497. The requirements of paragraph 35B(2)(b) and subsection 35B(4) provide for necessary flexibility in the application process to accommodate circumstances of urgency, with appropriate safeguards to ensure that applications made via non-written means are limited to instances of operational need, and that appropriate records are made of them.

No limit on subsequent SIO applications – subsection 35B(3)

498. Subsection 35B(3) clarifies that nothing in Division 4 prevents an application for an SIO authority being made in respect of an SIO that has been the subject of a previous application. The note to this provision further clarifies that, while an SIO authority can be varied, a variation cannot extend its term of operation beyond the statutory maximum of 12 months. This requirement is established by section 35F (detailed below).

499. It is appropriate that no statutory limitations are placed on the number of subsequent applications that may be made for an SIO authority. Any subsequent application will be considered anew. In all cases the authorising officer must be satisfied that the relevant issuing criteria in section 35C are made out in respect of the particular application placed before him or her under section 35B.

New section 35C – Granting of special intelligence operation authorities

500. New section 35C sets out the issuing criteria and other procedural requirements for the granting of an SIO authority by an authorising officer (being either the Director-General or a Deputy Director-General).

Issuing criteria – subsections 35C(1) and (2)

501. New subsection 35C(1) provides that an authorising officer may grant an authority to conduct an SIO, if an application is made pursuant to section 35B and the authorising officer is satisfied, on reasonable grounds, of the matters set out in subsection 35C(2). These matters are:

- the SIO will assist the organisation in the performance of one or more special intelligence functions, and the circumstances are such as to justify the conduct of an SIO: paragraphs 35C(2)(a) and (b)
- any unlawful conduct involved in conducting the SIO will be limited to the maximum extent consistent with conducting an effective SIO: paragraph 35C(2)(c)
- the SIO will not be conducted in such a way that a person is likely to be induced to commit an offence against a law of the Commonwealth, or a State or Territory, that the person would not otherwise have intended to commit: paragraph 35C(2)(d), and
- the conduct involved in an SIO will not cause death or serious injury to any person, or involve the commission of a sexual offence against any person, or result in significant loss of property or serious damage to property: paragraph 35C(2)(e).

502. These issuing criteria are targeted to ensure that SIOs are only able to be conducted in circumstances in which they are necessary and appropriate (see paragraphs 35C(2)(a) and (2)(b)). The criteria further limit any unlawful conduct to that which is needed to conduct an effective SIO as per the requirements of paragraph (2)(c), and which is proportionate to that end as per the exclusion in paragraphs 35C(2)(d) and (e) of conduct in the nature of 'entrapment' or which constitutes a serious offence against a person or in relation to property.

Other procedural requirements – subsections 35C(3)-(7)

503. Subsection 35C(3) provides that an SIO may be granted unconditionally or subject to conditions. There is no statutory requirement in relation to the relevant conditions that may be applied to an order, reflecting that this is a matter for the discretion of the authorising officer, acting within the scope of his or her authority under subsections (1) and (2).

504. Subsection 35C(4) provides that an SIO authority may be granted in writing and signed by the authorising officer. If the authorising officer has reason to believe that the delay caused by giving a written authority may be prejudicial to security, he or she may grant the authority orally in person, or by telephone or other means of communication. In the event that an SIO is granted by means other than in writing and signed, subsection 35C(5) requires the authorising officer, within seven days, to issue a written record of the authority that complies with the contents requirements set out in section 35D. These requirements are consistent with those in subsection 35B(2) in relation to applications, and are directed to the same purpose of ensuring appropriate operational flexibility and efficiency in circumstances of urgency, while providing for appropriate safeguards in relation to non-written applications and authorities (including record-keeping requirements).

505. Subsection 35C(6) confirms that no provision in Division 4 prevents an SIO authority being granted in respect of a special intelligence operation that has been the subject of a previous SIO authority. The note to the provision further refers to a related requirement in section 35F, that a variation to an SIO may not cause its period of effect to exceed the statutory maximum of 12 months. This is consistent with the corresponding provisions in subsection 35B(3) in relation to an application for an SIO authority.

506. Subsection 35C(7) provides that the written authority for an SIO, or a written record of an authority issued on an urgent basis, is not a legislative instrument. This declaration is in line with section 7(1)(b) of the Legislative Instruments Act 2003 (LIA), which provides for the making of a declaration, via an express statutory provision, that a particular matter or thing is not a legislative instrument for the purposes of that Act.

507. An exemption from the LIA is necessary to preserve the covert nature of SIOs. Legislative instruments are required by section 24 of the LIA to be registered on the Federal Register of Legislative Instruments (FRLI). The registration of an authority on the FRLI would disclose publicly the existence and operational details of an SIO and would therefore prevent the Organisation from collecting the intelligence information sought, and disclose inappropriately security classified information. Registration may also endanger the safety of participants identified in the authority by revealing publicly their identities.
Subsection 35C(7) is based on a similar provision in subsection 15GI(4) of the Crimes Act in respect of controlled operations, reflecting that an exemption was considered acceptable to the Parliament in 2009-2010 when the relevant legislation, the *Crimes Legislation Amendment (Serious and Organised Crime) Bill 2009* (Act of 2010) was passed.

New section 35D – Contents of special intelligence operation authorities

Details that must be included in a written authority or record of authority: subsection 35D(1)

508. New subsection 35D(1) sets out the details that must be included in a written SIO authority, which must also be included in a written record of an SIO authority that is issued

verbally or otherwise pursuant to paragraph 35C(4)(b) and subsection (5). An authority must include the following information:

(a) how the SIO will assist the Organisation in the performance of special intelligence functions

(b) the persons authorised to engage in special intelligence conduct for the purposes of the SIO

(c) a general description of the nature of the special intelligence conduct the persons referred to in paragraph 35D(1)(b) may engage in

(d) the period of effect of the SIO authority, within a maximum period of 12 months

(e) any conditions to which the SIO is subject, and

(f) the date and time when the SIO authority is granted.

509. The matters specified in paragraphs 35D(1)(a)-(f) are intended to ensure that the nature and scope of the authority conferred by an SIO authority is particularised adequately and documented. This will promote clarity and certainty in the operation of the SIO scheme.

510. In addition, the maximum duration for an SIO authority of 12 months in paragraph 35D(1)(d) accommodates the possibility that there may be a legitimate operational need for an SIO to run for a reasonably substantial period of time in order to gather the intelligence sought, without the disruption and possible risk to participants associated with a shorter duration, for example, in the nature of weeks or days. A shorter duration than the maximum term of 12 months may be authorised if the authorising officer is satisfied that it is appropriate, having regard to the issuing criteria in section 35C.

511. The maximum period of 12 months further strikes an appropriate balance between operational necessity and appropriate accountability and oversight in relation to operations of a longer duration. It requires the making of a new application for an authority if there is considered to remain an operational need to conduct an SIO at the conclusion of the statutory maximum period. An application for a new SIO authority in these circumstances will be considered afresh by the authorising officer, in accordance with the requirements of sections 35B, 35C and 35D. There are no limitations in Division 4 on the number of new authorities that may be granted in respect of an SIO, or on the making of applications for an SIO that have been made previously (whether or not an authority is granted).

Means of identifying individuals in an authority or a record of authority: subsection 35D(2)

512. A person referred to in paragraph 35D(1)(b) may be identified in a number of ways, including by name, class, assumed name, code name or code number. New subsection 35D(2) further provides that a person who is authorised to participate in an SIO is sufficiently identified by an assumed name, code name or code number, provided that the authorising officer can match the assumed name, code name or code number to the person's identity. This is designed to ensure that appropriate confidentiality is maintained in relation to a participant's identity, while enabling such persons to be identified for the purpose of authorising their involvement in an SIO, including particularising the scope of their authority.

New section 35E – Commencement and duration of special intelligence operation authorities

513. New section 35E provides for the commencement and duration of SIO authorities. New subsection 35E(1) provides that an SIO authority comes into force at the time the SIO authority is granted under section 35C. In the case of an urgent authority granted under paragraph 35C(4)(b), commencement is the time at which the authorising officer communicates to the applicant that the authority is granted, and not the issuing of a written record of that decision under subsection 35C(5).

514. New subsection 35E(2) provides that an SIO authority has effect for the period specified in accordance with paragraph 35D(1)(d) (being a period not exceeding 12 months) unless it is cancelled before the end of the period of effect, or the period of effect is extended in accordance with section 35F (which permits variation of the period of effect up to a cumulative maximum of 12 months).

New section 35F – Variation of special intelligence operation authorities

515. New section 35F makes provision for the variation of an SIO authority. Subsection 35F(1) provides that an authorising officer may vary an authority at any time while it is in effect. He or she may do so on either the application of an ASIO employee, or on his or her own initiative.

516. For the avoidance of doubt, the reference in subsection 35F(1) to 'an authorising officer' enables, but does not mandate, a different authorising officer to determine a variation application to the authorising officer who granted the relevant SIO authority under section 35C. This will enable appropriate flexibility in the operation of the SIO scheme and ensure the availability of authorising officers to consider a variation application.

Application for a variation – subsections 35F(2)-(3)

517. Subsection 35F(2) provides that an application for a variation may be made in writing. Alternatively, if the applicant has reason to believe that the delay caused by making a written application may be prejudicial to security, the application may be made orally in person, by telephone or by other means of communication. If an application is made on an urgent basis, subsection 35F(3) requires the applicant, as soon as practicable after making the application, to make a written record of the application and to provide a copy to the authorising officer.

518. The issuing criteria for an authority in paragraphs 35C(2)(b)-(e) and subsection (3) are not replicated in relation to variation applications under section 35F, because these provisions continue to apply, of their own force, to the relevant SIO authority that is sought to be varied. A purported variation of an SIO authority that is inconsistent with the requirements of section 35C would be incapable of answering the description of an SIO authority as defined in section 4, and would therefore be outside an authorising officer's authority under section 35C.

Limits on variation – subsection 35F(4)

519. Subsection 35F(4) provides that the authorising officer considering the variation application must not make a variation unless he or she: (a) is satisfied, on reasonable grounds,

that the SIO conducted in accordance with the SIO as varied, will assist the Organisation in the performance of one or more special intelligence functions and (b) considers it appropriate to make a variation.

520. The reference in paragraph 35F(4)(a) to 'one or more special intelligence functions' makes clear that a variation need not pertain to the same special intelligence function or functions in respect of which the SIO was granted under section 35C. This is necessary to accommodate the possibility that a variation may be sought specifically to extend or substitute the relevant special intelligence function or functions to which the SIO relates.

521. Consistent with the issuing process for SIO authorities, an internal approval process for variations appropriately reflects that the conduct of SIOs is an internal and operational matter. This ensures operational efficiency and protects the security of the investigation. Variations are subject to the oversight and accountability arrangements applicable to SIOs generally. The reporting requirements in new section 35Q (mandating 'per use' reporting to the Minister and the IGIS in respect of each six-monthly period for which an SIO authority is in effect) include variations that are sought or granted within the relevant period of operation. The IGIS's general powers of oversight under the IGIS Act also cover variations of SIOs.

Limitations on variations of the period of effect of an SIO authority – subsection 35F(6)

522. Subsection 35F(6) further provides that, if a variation extends a period of effect of an SIO authority, the total period of effect must not be longer than the maximum period of 12 months. This ensures that the time limitation in paragraph 35D(1)(d) cannot be extended by way of a variation of the period of effect.

Manner of variation – subsections 35F(6)-(7)

523. Subsection 35F(5) provides for the making of a variation in writing, or on a purely verbal basis (in person or by telephone) or other means of communication in urgent circumstances. That is, if the authorising officer has reason to believe that the delay caused by giving a written variation may be prejudicial to security.

524. Subsection 35F(7) further provides that if an SIO authority is varied on an urgent basis, the authorising officer must, within seven days, issue a written record of the variation, which is signed by him or her. These provisions are consistent with the requirements for the granting of an SIO authority in subsections 35C(4) and (5).

525. For the avoidance of doubt, a variation of an SIO authority is not a legislative instrument by reason of paragraph 7(1)(a) of the LIA (item 24 of the table in section 7, which excludes instruments prescribed by regulation). Item 33 of Part 1 of Schedule 1 to the Legislative Instruments Regulations 2004 excludes an instrument that varies or revokes an instrument that is not a legislative instrument.

Authority may be varied more than once – subsection 35F(8)

526. Subsection 35F(8) provides that an SIO authority may be varied more than once under section 35F. This provision is included for the avoidance of doubt. In all instances, a variation application (whether initial or subsequent) must be made in accordance with the requirements of subsections 35F(1)-(7).

New section 35G – Cancellation of special intelligence operation authorities

527. New section 35G provides for the cancellation of an SIO authority. An authorising officer may cancel an authority under subsection 35G(1) at any time and for any reason. Subsection 35G(2) requires a cancellation to be made in writing, and to specify when it takes effect. This provision enables appropriate operational discretion to cancel an operation, and ensures that records are made of all cancellation decisions.

New section 35H – Effect of special intelligence operational authorities

528. Section 35H describes the effect of an SIO authority. Subsection 35H(1) provides that an SIO authority has the effect of authorising each participant who is identified in the relevant SIO authority to engage in the conduct specified in the authority in respect of that participant. The authority to engage in special intelligence conduct cannot be delegated to any other person. Section 35H is material to the application of the protection from criminal or civil liability in section 35K, which is strictly limited to conduct authorised under an SIO authority.

529. Subsection 35H(2) further provides that the duration of an authorisation in relation to a person identified in an SIO authority is for the period of effect of the SIO authority, unless one of the exceptions in paragraphs 35H(2)(a)-(c) applies. These are that the SIO authority provides for a shorter period of authorisation in relation to a person, or that the SIO authority is varied under section 35F to provide that the person is no longer authorised, or that the SIO authority is cancelled under section 35G before the end of the period of effect.

New section 35J – Defect in a special intelligence operation authority

530. New section 35J provides that applications and authorities are not invalidated by defects, unless the defect affects the application, authority or variation in a material particular.

531. This provision is designed to ensure that minor matters relating to form or process do not invalidate an application, authority or variation. The material nature (or otherwise) of a particular affected by a defect is a matter to be determined in the circumstances of the individual application or authority in question. A defect affecting a material particular is intended to include one that vitiates the basis on which an application was made, or an authority granted, or a variation requested or granted.

New section 35K – Immunity from liability for special intelligence conduct during special intelligence operations

532. New section 35K protects from criminal or civil liability a participant in an authorised SIO who engages in special intelligence conduct. It does not deem lawful special intelligence conduct which would otherwise be unlawful. Rather, it provides that a participant in an SIO who engages in conduct that satisfies the requirements of subsection 35K(1) is not subject to any criminal or civil liability in relation to that conduct.

533. As noted above, the immunity conferred by section 35K is necessary and appropriate for the effective operation of SIOs. This includes by providing an assurance to participants that they are not legally liable in respect of special intelligence conduct, and by preventing

the potential that sensitive operational information or the safety of participants may be compromised because legal proceedings are initiated in relation to special intelligence conduct that would result in, or risk, the disclosure of an SIO.

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

Conditions for the application of the immunity – subsections 35K(1) and (2)

535. Subsection 35K(1) sets out the following conditions which must be satisfied for the immunity to apply:

(a) the participant engages in the conduct in the course of, and for the purposes of, the SIO

(b) the participant engages in the conduct in accordance with the SIO authority

(c) the participant is identified in the SIO authority as a person authorised to engage in special intelligence conduct for the purpose of the SIO

(d) the conduct does not involve the participant intentionally inducing another person to commit an offence against the Commonwealth, a State or Territory that the person would not otherwise have intended to commit

(e) the conduct does not involve the participant engaging in any conduct that causes the death of or serious injury to a person, or involves the commission of a sexual offence against any person, or causes significant loss of, or serious damage to, property, and

(f) the requirements (if any) specified in a determination under subsection 35K(2) have been met.

536. Subsection 35K(2) provides that the Minister may, by legislative instrument, determine requirements for the purpose of paragraph 35K(1)(f).

Safeguards applying to the immunity conferred by section 35K

537. A number of safeguards apply to the immunity conferred by section 35K. These safeguards, which are set out presently, ensure that its application is duly limited and is subject to independent oversight, and that there remains scope for the payment of compensation to aggrieved individuals in appropriate cases.

<u>Conditions in subsections 35K(1) and (2)</u>

538. The conditions in subsection (1) ensure that the immunity in section 35K applies only to conduct that is in the course of and as part of a SIO, and is accordance with the relevant SIO authority. This includes a requirement that the participant must be authorised under the relevant SIO authority to engage in the particular conduct. In addition, the immunity is qualified by the exclusion of conduct in the nature of entrapment and serious offences against persons or property. These exclusions replicate those in the issuing criteria in paragraphs 35C(2)(d) and (e), and accordingly are declaratory of the limits in the scope of authority able to be conferred by an SIO authority under section 35C. The exclusion of such

offences from Division 4 reflects a policy judgment that such offences are not necessary or proportionate to the effective performance by the Organisation of its special intelligence functions, or the effective operation of the SIO scheme. This ensures that the immunity in section 35K is proportionate to the security intelligence-related ends to which the SIO scheme is directed.

539. Subsection (2) enables the Minister to impose any additional conditions for the application of the immunity in subsection 35K(1), if he or she considers it appropriate to do so. This means that a participant or participants in a particular SIO, or participants in SIOs generally, may be held to an even higher standard of conduct than that which is required under paragraphs 35K(1)(a)-(e). As section 35K does not make provision for legislative instruments issued under subsection 35K(2) to modify the conditions in paragraphs 35K(2)(a)-(e), subsection 35K(2) cannot be relied upon to modify the existing statutory conditions in any way.

Oversight by the Inspector-General of Intelligence and Security

540. The application of Division 4, including section 35K, is subject to the IGIS's statutory powers of inquiry under the IGIS Act. This includes the discretion of the IGIS to recommend that the Organisation pay compensation to a person in appropriate cases, which could potentially include persons who are unable to commence civil proceedings against the Organisation by reason of section 35K, in respect of special intelligence conduct. Similarly, the immunity conferred by section 35K does not preclude the Organisation from paying compensation to an individual.

541. As such, the oversight role and function of the IGIS is an effective and important means of ensuring that consideration is given to the payment of compensation to individuals in appropriate cases concerning actions taken under Division 4, while preventing any prejudice to national security that could arise if participants in an SIO were subject to civil liability in respect of their conduct as part of the SIO.

Prospective application of immunity

542. The immunity conferred by section 35K is, like the entirety of Division 4, of prospective application. It applies only to the conduct of an SIO participant that is carried out after the commencement of Division 4, provided that the relevant special intelligence conduct accords with the terms of an SIO authority sought and granted in accordance with the provisions of Division 4, once those provisions have commenced.

543. In addition, Division 4 does not authorise the retrospective conferral of an immunity from criminal or civil liability upon a participant in a covert intelligence operation which was in effect prior to the commencement of the Division. This is so even if the relevant covert operation is later the subject of an SIO application and authority under the new Division once it has commenced. In these circumstances, a person's conduct as part of a pre-Division 4 operation is subject to the general principles of criminal responsibility or civil liability which applied at the time he or she engaged in the relevant conduct.

New section 35L – Requirements for warrants, etc. not affected

544. New section 35L provides that Division 4 does not authorise the doing of an act that would otherwise require authorisation by a warrant issued under the ASIO Act or Part 2-2 of

the TIA Act or an authorisation under Part 4-1 of the TIA Act. This provision is included for the avoidance of doubt. It gives express effect to the policy intention that the SIO regime cannot be engaged as a substitute for these warrant or authorisation-based requirements.

New section 35M – Effect of being unaware of variation or cancellation of special intelligence operation authority

545. New section 35M makes provision for circumstances in which an SIO authority is varied or cancelled, but a participant is unaware of the variation or cancellation, and he or she is not reckless about the existence of a variation or cancellation. Section 35M provides that Division 4 continues to apply to that participant. This ensures that a participant will remain protected from criminal or civil liability provided that he or she continues to act in accordance with the terms of the authority as in effect immediately prior to its variation or cancellation, and he or she is not reckless as to the existence of the variation or cancellation.

546. New subsection 35M(3) provides guidance on the meaning of 'reckless' for the purpose of section 35M, which is based on the meaning of this term in section 5.4 of the Criminal Code. A person is taken to have been reckless about the existence of a variation or cancellation if he or she is aware of a substantial risk that the variation or cancellation has happened, and having regard to the circumstances known to the person, it is unjustifiable to take the risk that the authority has not been varied or cancelled. For example, by acting in accordance with its terms prior to variation or cancellation.

547. Section 35M takes account of the fact that decisions relating to an authority can be made without the knowledge of all participants, and that it may be difficult or impossible to contact some participants immediately while an SIO is in progress. A similar provision is included in relation to the controlled operations scheme in section 15HD of the Crimes Act. The requirement that a person must not have been reckless in relation to the existence of a cancellation provides an appropriate safeguard. It imports both a subjective and an objective test in relation to a person's state of mind in relation to the existence of a variation or cancellation.

New section 35N – Protection from criminal responsibility for certain ancillary conduct

548. New section 35N provides protection from criminal liability for a person who is connected with an SIO, but who is not necessarily an authorised participant in the SIO, if that person has a belief that the activities in which they are engaging are ancillary to the authorised conduct of a participant in an SIO.

549. In particular, subsection 35N(2) establishes a limited immunity in respect of persons who engage in conduct (referred to as 'ancillary conduct') that constitutes an 'ancillary offence' to the conduct of an SIO participant that would otherwise have constituted an offence (the 'related conduct'). For the immunity to apply, the person must believe, at the time of engaging in the ancillary conduct, that the related conduct of the SIO participant was being engaged in, or would be engaged in, as part of an authorised SIO.

550. Subsection (3) defines an 'ancillary offence' for the purpose of section 35N as an offence against the law of the Commonwealth, a State or a Territory consisting of:

(a) conspiring to commit the offence constituted by the related conduct, or

(b) aiding, abetting, counselling or procuring, inciting or being in any way knowingly concerned in, the commission of the offence constituted by the related conduct.

551. This provision is necessary because the immunity from liability in section 35K is limited to participants in an SIO who engage in authorised conduct that technically constitutes an offence. For example, section 35K does not immunise non-participants in an SIO from criminal responsibility under Division 11 of Part 2.4 of the Criminal Code, if such persons engage in conduct ancillary to the special intelligence conduct of an SIO participant. It might be argued that the authorising officer under Division 4, or other ASIO employees supporting the administration of an SIO, had counselled, procured, aided or abetted the commission of what would otherwise have been an offence by an SIO participant. The SIO participant's conduct would be immune from criminal liability pursuant to section 35K, but the non-participant may be liable to prosecution.

552. It is not appropriate, as a matter of policy, that a person be held legally liable for ancillary conduct in this context or that such ancillary conduct is exposed to possible investigation or prosecution. This would create an arbitrary distinction in the treatment of participants in an SIO, and persons who are required as part of their official duties to assist in or support an SIO (or other persons who have complied voluntarily with a request to provide such assistance or support). Section 35N provides an equal assurance to persons who lawfully support an authorised SIO.

New section 35P – Unauthorised disclosure of information

553. New section 35P creates two offences in relation to the unauthorised disclosure of information relating to an SIO. These offences are necessary to protect persons participating in an SIO and to ensure the integrity of operations, by creating a deterrent to unauthorised disclosures, which may place at risk the safety of participants or the effective conduct of the operation.

554. The offences apply to disclosures by any person, including participants in an SIO, other persons to whom information about an SIO has been communicated in an official capacity, and persons who are the recipients of an unauthorised disclosure of information, should they engage in any subsequent disclosure.

555. The term 'disclose' is intended to take its ordinary meaning for the purpose of section 35P. It is intended to include the making available of information to others by any means. It is not intended to require, as a rule, proof that the information was received by another person, or proof that another person read, heard or viewed the information. Nor is the term intended to require proof that a person provided or intended to provide information to a particular person or group of persons.

Offence of unauthorised disclosure of information relating to an SIO – new subsection 35P(1)

556. New subsection 35P(1) creates an offence applying to the conduct of a person in the form of a disclosure of information, and a circumstance that the information relates to an SIO. The fault element of intention applies to the physical element of a person's conduct in disclosing information, by reason of subsection 5.6(1) of the Criminal Code. The fault

element of recklessness applies to the physical element of the circumstance that the information relates to an SIO, by reason of subsection 5.6(2) of the Criminal Code. The offence carries a maximum penalty of five years' imprisonment.

Aggravated offence – new subsection 35P(2)

557. New subsection 35P(2) creates an aggravated form of the offence in subsection 1. The relevant aggravating elements, which are set out in paragraph (c), are that:

(i) the person intended, in making the disclosure, to endanger the health or safety of any person, or prejudice the effective conduct of an SIO, or

(ii) the disclosure of the information will endanger the health or safety of any person or prejudice the effective conduct of an SIO.

558. The fault element applying to the physical element in paragraph 35P(2)(c)(i) is that of intention, pursuant to the express statement in the provision. The fault element applying to the physical element in paragraph 35P(2)(c)(ii) is that of recklessness, by reason of subsection 5.6(2) of the Criminal Code. The aggravated offence is subject to a maximum penalty of 10 years' imprisonment.

Offence-specific defence – new subsection 35P(3)

559. The new offences in subsections 35P(1) and (2) are subject to an offence-specific defence in subsection 35P(3), which provides for a number of lawful disclosures in paragraphs 35P(3)(a)-(d). These include disclosures pertaining to the operation of Division 4 or legal proceedings relating to Division 4, other legal obligations of disclosure, and the performance by the Organisation of its statutory functions.

560. Consistent with subsection 13.3(3) of the Criminal Code, the defendant bears an evidential burden in relation to the offence-specific defence in subsection 35P(3). This means that he or she must adduce or point to evidence suggesting a reasonable possibility that one or more of the matters set out in paragraphs 35P(3)(a)-(d) exist. The prosecution is then required to negate this matter to the legal standard (beyond reasonable doubt).

561. It is appropriate to frame the matters in subsection 35P(3) as an offence-specific defence (with the result that an evidential burden is imposed on the defendant) rather than including these matters as an element of the offences in subsections 35P(1) and (2). For example, a requirement that the disclosure was not made pursuant to any of the matters set out in paragraphs 35P(3)(a)-(d), with the result that the prosecution bears the legal and evidential burden.

562. This is because evidence suggesting a reasonable possibility of the authorised nature of the disclosure is readily available to a defendant, who would have had such authority, or perceived authority, in contemplation at the time he or she disclosed the relevant information. The inclusion of subsection 35P(3) as an element of the offences in subsections 35P(1) and (2) would be inappropriate is it would impose a disproportionate burden on the prosecution. It would be necessary for the prosecution to disprove, as a matter of course, all of the matters set out in paragraphs 35P(3)(a)-(d) even if there is no evidence suggesting they are in issue.

Penalties

563. The penalties applying to these offences implement a gradation consistent with established principles of Commonwealth criminal law policy, as documented in the *Guide to Framing Commonwealth Offences, Infringement Notices and Enforcement Powers*. The Guide provides that a heavier maximum penalty is appropriate where the consequences of an offence are particularly dangerous or damaging.

564. The offence in subsection 35P(2), applying to the disclosure of information with an intent to cause harm (or where harm will result from such a disclosure), appropriately attracts a heavier penalty than the offence in subsection 35P(1), which targets conduct that places at risk such information. The penalty of 10 years' imprisonment applying to the aggravated offence in subsection 35P(2) maintains parity with the penalty applying to the offence of unauthorised communication of information in subsection 18(2) (as that penalty is amended by Schedule 6).

565. The maximum penalty of five years' imprisonment applying to the offence in subsection (1) reflects an appropriate gradation with the new unauthorised dealing offences in sections 18A and 18B (inserted by Schedule 6) which carry a maximum penalty of three years' imprisonment, and parity with section 34ZS of the ASIO Act regarding the unauthorised disclosure of information relating to a questioning or questioning and detention warrant. The unauthorised disclosure of information pertaining to an SIO is considered to be more culpable than the unauthorised dealing with information pertaining to the Organisation's statutory functions. For example, the unauthorised disclosure of information pertaining to an SIO, by its very nature, carries a greater risk of harm, both in jeopardising the safety of participants and in potentially limiting the Organisation's intelligence-gathering capability by compromising the integrity of the operation.

566. Subsection (4) provides that section 15.4 of the Criminal Code (extended geographical jurisdiction—category D) applies to the offences in section 35P. This means that the offences apply to any person, in respect of conduct engaged in any country, whether or not the conduct is an offence under the laws of the relevant local jurisdiction (if outside Australia). This form of extended geographical jurisdiction is necessary to ensure that the offences apply to SIO participants or persons who have knowledge of an SIO who are not Australian citizens and who engage in unauthorised disclosures outside Australia. Given the potential of information obtained under an SIO to place at risk Australia's national security and intelligence gathering capabilities, in addition to potentially endangering SIO participants, it is appropriate that the offences have the widest possible geographical application to target such wrongdoing. Prosecutions of non-Australians in relation to conduct outside Australia is subject to the safeguard in section 16.1 of the Criminal Code, which requires the Attorney-General to consent to the commencement of such prosecutions.

567. Subsection 35P(5) provides that subsection 35P(4) does not, by implication, affect the interpretation of any other provision in the ASIO Act. This provision is necessary because some offences in the ASIO Act were enacted prior to the commencement of the extended geographical jurisdiction provisions of Part 2.7 of the Criminal Code on 24 May 2001. As such, the geographical jurisdiction of any pre-2001 offence provisions which do not provide for the application of Part 2.7 of the Criminal Code is assessed in accordance with ordinary principles of statutory interpretation. Subsection 35P(5) makes clear that the inclusion of subsection 35P(4) in relation to new section 35P is not intended to have any impact on the

interpretation of the geographical jurisdiction applying to any offence provision in the ASIO Act enacted prior to 24 May 2001.

New section 35Q – Reports by the Director-General

568. New section 35Q establishes reporting requirements in relation to the exercise of powers under Division 4. Subsection 35Q(1) provides that the Director-General must give the Minister, and the IGIS, a written report in respect of each six-month period in which an SIO is in effect. Where the duration of an SIO authority exceeds six months, the subsequent report must address the remainder of the period for which the SIO authority has effect. Where an SIO authority is for a period of less than six months, the report must address the relevant period in which the authorisation is in effect. New subsection 35Q(2) provides that a report must address the extent to which the SIO has, during the relevant reporting period, assisted the Organisation in the performance of its special intelligence functions.

569. This reporting requirement ensures Ministerial visibility and oversight of the operation of Division 4 of Part III. It also ensures that the IGIS is provided with notification on the use of these powers, in order to inform his or her oversight powers in relation to the Organisation under section 8 of the IGIS Act. The IGIS may also exercise the information-gathering powers under the IGIS Act in respect of operations under Division 4. This includes the power to compel the production of documents or the provision of information, and the power to compel a person to give evidence under oath or affirmation.

570. New subsection 35Q(3) provides that a report issued under subsection 35Q(1) is not a legislative instrument. This provision is of declaratory rather than substantive effect, given that a report under section 35Q does not satisfy the definition of a legislative instrument in section 5 of the LIA. It is included as an aid to interpretation.

New section 35R – Evidence relating to special intelligence operations

571. New subsection 35R(1) provides that an authorising officer may issue a written certificate setting out such facts as the authorising officer considers relevant with respect to the granting of an SIO authority. Subsection 35R(2) provides that, in any proceedings, a certificate issued under subsection 35R(1) is prima facie evidence of the matters stated in the certificate. This means that a certificate issued under section 35R creates a rebuttable presumption as to the existence of the factual basis on which the authorising officer was satisfied the relevant issuing criteria for an SIO authority were met.

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

Item 4 – After subsection 94(2)

573. Item 4 inserts a new subsection 94(2A), which establishes reporting requirements in relation to the Organisation's exercise of powers under new Division 4 of Part III. New subsection 94(1C) provides that the Organisation's annual report must include a statement of the total number of applications made under section 35B for SIO authorities, and the total number of authorities granted under section 35C during the reporting period. The information reported under subsection 94(1C) is subject to the Minister's power under subsection 94(4) to delete information if considered necessary to avoid prejudice to security, defence, international affairs or individual privacy.

574. This mechanism ensures appropriate Parliamentary and public notification of the exercise of powers under new Division 4 of Part III while maintaining security interests by ensuring the covert nature of SIOs. In particular, it is appropriate that Parliamentary reporting is undertaken on a cumulative, annual basis rather than on a 'per use' basis. This, in combination with subsection 94(4), is necessary to minimise the risk that individual SIOs are able to be identified.

Schedule 4—ASIO co-operation and information sharing

Overview of measures

575. Schedule 4 amends the *Australian Security Intelligence Organisation Act 1979* (ASIO Act) to enable breaches of section 92 of the ASIO Act, which contains offences relevant to the non-disclosure of identity obligations, to be referred to law enforcement agencies for investigation. This amendment implements the Government's response to Recommendation 34 of the Parliamentary Joint Committee on Intelligence and Security's (PJCIS) *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation*. The Schedule also clarifies ASIO's ability to co-operate with the private sector both in Australia and overseas and implements the Government's response to Recommendation 33 of the Report of the PJCIS.

Australian Security Intelligence Organisation Act 1979

Item 1 – Paragraph 18(3)(b)

576. Section 18 of the ASIO Act limits the communication of intelligence, information or matters possessed, in the knowledge of or acquired as a result of a person having been an ASIO officer.

577. Subsection 18(3) provides that the Director-General of Security (Director-General) or a person authorised by the Director-General, may communicate information that has come into the possession of ASIO in the course of performing its functions under section 17, to a Minister or staff members of Commonwealth or State authorities (identified in subsection 18(4)), if it relates to the commission, or intended commission, of a 'serious crime', or where the Director-General or a person authorised by the Director-General, is satisfied that the national interest requires the communication, and provided the information relates to the performance of the functions, responsibilities or duties of the person to whom the information is being communicated (identified in subsection 18(4)). A 'serious crime' is defined in section 4 of the ASIO Act as an offence punishable by imprisonment exceeding 12 months.

578. Section 4 of the ASIO Act defines 'authority of the Commonwealth' and, other than for Part IV, 'authority of a State'. Section 4 also defines 'State' as including the Australian Capital Territory and the Northern Territory.

579. This item amends paragraph 18(3)(b) by substituting 'either' with 'any of the following subparagraphs apply'. In conjunction with items 2 and 3, this item provides that a person referred to in subsection 18(1) may communicate information to a person referred to in subsection 18(4) if the information has come into ASIO's possession in the course of performing its functions under section 17 and the information relates, or appears to relate to the commission or intended commission of an offence against section 92.

580. The penalty for the offence of unauthorised communication of information by a person pursuant to subsection 18(2) of the ASIO Act is amended in Schedule 6.

Item 2 – Subparagraph 18(3)(b)(i)

581. This item makes a technical amendment to subparagraph 18(3)(b)(i) by omitting the words 'crime; or' and substituting 'crime;'.

Item 3 – After subparagraph 18(3)(b)(i)

582. This item inserts new subparagraph 18(3)(b)(ia) to provide that a person referred to in subsection 18(1) may communicate information to a person referred to in subsection 18(4) if the information has come into ASIO's possession in the course of performing its functions under section 17 and the information relates, or appears to relate to the commission or intended commission of an offence against section 92.

583. Section 92 is amended in Schedule 1 to make it an offence to publish the identity of a current or former ASIO employee or ASIO affiliate, without the written consent of the Minister or Director-General.

584. The combination of the penalty for the offence in section 92 and the requirement in subsection 18(3) that communication of information to law enforcement authorities must be in relation to a 'serious crime' has resulted in ASIO being precluded from communicating information about the commission or intended commission of an offence under section 92, to relevant authorities, including law enforcement authorities. The amendment in this item will overcome this limitation and allow a person to communicate information about possible breaches of section 92 (where that information is not otherwise relevant to security).

585. Consistent with the communication of information under section 18, the communication of any breach of section 92 would only be made by the Director-General or a person acting within the limits of authority conferred on the person by the Director-General.

586. It is also consistent with subsections 18(3) and (4) enabling communication of information to a Minister or staff member of an authority of the Commonwealth or State, if the information relates or appears to relate to their functions or duties.

Item 4 – At the end of paragraph 19(1)(a)

587. Section 19 provides that ASIO may co-operate with other authorities in connection with the performance of the Organisation's functions, so far as is necessary for, or conducive to, the performance of its functions.

588. This item makes a technical amendment adding 'and' at the end of paragraph 19(1)(a), to clarify that ASIO may co-operate with those authorities referred to in paragraphs 19(1)(a) to (c).

Item 5 – At the end of subsection 19(1)

589. There is uncertainty as to whether section 19 could be read to exclude ASIO's ability to co-operate with private sector organisations or other persons or bodies not currently described within section 19 of the ASIO Act.

590. This item adds '; and (d) any other person or body whether within or outside Australia' to include this category of person or body. This amendment clarifies that under

section 19, ASIO may co-operate with any person or body within or outside Australia, in addition to:

(a) authorities of the Commonwealth, and

(b) departments, Police Forces and authorities of the States, and

(c) authorities of other countries approved by the Minister as being capable of assisting the Organisation in the performance of its functions.

591. The effect of this amendment is to clarify that ASIO can co-operate with private sector organisations (both within and outside of Australia).

592. It is necessary for, or conductive to, the performance of ASIO's existing functions to co-operate with private sector organisations. ASIO's ability to co-operate with the private sector is particularly important, given that the private sector owns and operates a large amount of Australia's critical infrastructure, which is vulnerable to security threats such as terrorism. For example, ASIO's Business Liaison Unit (BLU), provides an interface between Australian businesses and the Australian Intelligence Community in order to raises awareness of national security issues. The BLU engages directly with businesses on a one-on-one basis to help build strong relationships between ASIO and the private sector. This engagement seeks to enable Australian business security managers to recognise and respond to national security related threats, develop and implement appropriate risk management strategies and provide informed briefings to executives and staff.

593. Section 19 operates in conjunction with sections 17 and 18 which set out ASIO's functions and enable ASIO to communicate intelligence and information outside of the Organisation. Where ASIO seeks to co-operate with a private sector organisation outside Australia, this may be subject to arrangements made or directions given by the Minister as provided for under subsection 19(1). Any arrangements made or directions given by the Minister with respect to ASIO's co-operation with the private sector may also be subject to written guidelines under section 8A of the ASIO Act.

594. In addition to the safeguards on private sector co-operation contained in the ASIO Act, the Inspector-General of Intelligence and Security has oversight of the functions of ASIO including to ensure ASIO acts legally and with propriety and complies with ministerial directions and Guidelines.

Item 6 – At the end of section 92

595. This item inserts a note at the end of section 92 providing a cross reference to subsection 18(3) which provides that ASIO may communicate information to a Minister or a staff member of an authority of the Commonwealth or of a State, about offences under section 92, to appropriate authorities.

Item 7 – Application—communication of intelligence etc

596. This item is a transitional provision clarifying that the amendments made to section 18 apply in relation to communication of information made on or after the commencement of this item, whether the information has come into the possession of ASIO before or after the commencement of this item.

Schedule 5—Activities and functions of Intelligence Services Act 2001 agencies

Overview of measures

597. Schedule 5 amends the Intelligence Services Act 2001 (IS Act) to enable the Australian Secret Intelligence Service (ASIS) to undertake a new function of co-operating with ASIO in relation to the production of intelligence on Australian persons in limited circumstances without Ministerial authorisation, enhances the protective security capacity of ASIS and creates a new ground of Ministerial authorisation enabling ASIS to protect its operational security and allows ASIS to train certain individuals in use of weapons and self-defence techniques. The measures in the Schedule will also extend immunity for IS Act agencies for actions undertaken in relation to an overseas activity of the agency, provide a limited exception for use of a weapon or self-defence technique in a controlled environment and clarify the authority of the Defence Imagery and Geospatial Organisation (DIGO).

Item 1 – Section 3

Definitions

598. Item 1 includes the new definition of the 'operational security of ASIS'. This definition should be read in conjunction with the new Ministerial authorisation ground in new subparagraph 9(1A)(a)(iiia). Operational security means the protection of the integrity of ASIS operations from the risk of being undermined by foreign and non-State adversaries such as terrorist organisations or the reliance on inaccurate or false information. Protecting the integrity of ASIS's operations is part of ASIS's counter-intelligence function.

Item 2 – Before section 6

Division 1 – Functions of the agencies

599. Item 2 separates Part 2 into divisions and inserts the title of the first division, 'Functions of the agencies'.

Item 3 – After paragraph 6(1)(da)

Functions of ASIS

600. Item 3 is consequential to new section 13B and inserts new paragraph 6(1)(db) into subsection 6(1) to cover activities undertaken in relation to ASIO. It amends section 6 to provide ASIS with a specific function to enable it to undertake activities under the new section 13B in relation to ASIO without the need to obtain a Ministerial authorisation under section 9 of the IS Act. This new function should be read in conjunction with the new Division 3.

Items 4 and 5 – Paragraph 6B(e)(ii)

Functions of DIGO

601. Item 4 updates the description of DIGO's functions at paragraph 6B(3)(ii) in relation to providing assistance to Commonwealth authorities, State authorities and bodies approved

in writing by the Minister by removing the words, 'such imagery or products' and substituting, 'imagery and other geospatial products'.

602. Item 5 inserts new subparagraph 6B(e)(iia) to enable it to provide assistance in relation to the production and use of imagery and other geospatial technologies.

Item 6 – After subparagraph 9(1A)(a)(iii)

Ministerial authorisation

603. Item 6 implements the Government's response to Recommendation 38 of the Parliamentary Joint Committee on Intelligence and Security's (PJCIS) *Report on Potential Reforms of Australia's National Security Legislation* by inserting a new Ministerial authorisation ground. It should be read in conjunction with the new definition of operational security at Item 1.

604. This new Ministerial authorisation ground will enable an IS Act agency to produce intelligence on an Australian person whose activities pose a risk, or are likely to pose a risk, to the operational security of ASIS. The production of this intelligence 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.

605. The manner in which the activity is conducted, the circumstances of the activity or the relationships involved could provide the basis for the Minister to be satisfied that the ground has been met.

606. This ground is intended to address activities that pose a risk, or are likely to pose a risk, to the operational security of ASIS but are not, or are not likely to be, a threat to 'security' (for example, espionage or sabotage or interference by foreign governments) as defined in the ASIO Act.

607. While the intelligence produced must be relevant to the operational security of ASIS, ASD and DIGO may also seek a Ministerial authorisation from the Defence Minister to produce intelligence to assist ASIS.

608. The existing safeguards in the IS Act would apply to this new Ministerial authorisation ground. This includes the requirements for all authorisations to be made available for inspection by the Inspector-General of Intelligence and Security (IGIS). This will ensure that the IGIS will have oversight of ASIS's activities consistent with the IGIS's existing oversight role.

609. Before issuing an authorisation under this new ground, the Minister responsible for the IS Act must be satisfied of the factors in subsection 9(1). In accordance with paragraph 9(1A)(b), where the Australian person is also, or is also likely to be, involved in an activity or activities that are, or likely to be a threat to security, the Minister responsible for the IS Act will still be required to obtain the agreement of the Attorney-General before issuing an authorisation.

Item 7 – Subsection 9(1B) (note)

610. Item 7 inserts the new words, 'and operational security of ASIS' after the word, 'crime' in the note at the end of subsection 9(1B).

Item 8 – Before section 13

Division 2 – Co-operation

611. Item 8 separates Part 2 into divisions and inserts the title of the second division, 'Co-operation', consequential to amendments made by item 2.

Item 9 – Subsection 13(1A)

Co-operation with other authorities in connection with performance of agency's own functions

612. Item 9 amends existing subsection 13(1A) by replacing all the words after, 'planning or'. The amendment implements Recommendation 40 of the PJCIS Report, which recommended that the IS Act be amended to enable ASIS to provide training in self-defence techniques and the use of weapons to persons co-operating with ASIS.

613. The intention is to require the Foreign Minister to consult with the Prime Minister and the Attorney-General before approving an authority of another country that ASIS can provide training in weapons and self-defence techniques to an officer of that authority.

614. This amendment should be read in conjunction with the new subclause 1(1A) in Schedule 2 of the IS Act (item 14).

615. Any approval given by the Foreign Minister will be kept by ASIS and will be available on request by the IGIS. This is consistent with IGIS's existing oversight role of section 13 approvals.

Item 10 – Application – subsection 13(1A)

616. Item 10 provides that the amendment to subsection 13(1A) will not apply retrospectively. Any existing approval under subsection 13(1A) to co-operate with an authority of another country, at the date of the commencement of the amendment to subsection 13(1A), is not taken to also be an approval for ASIS to plan or undertake training in weapons or self-defence techniques with that authority. ASIS would be required to seek separate approval for such co-operation under the new subsection 13(1A).

Item 11 – After section 13A

Division 3 – Activities undertaken in relation to ASIO

617. Item 11 separates Part 2 into divisions and inserts the title of the third division, 'Activities undertaken in relation to ASIO', consequential to amendments made by items 2 and 8.

618. The new third division implements the Government's response to Recommendation 39 of the PJCIS report, which recommended that where ASIO and an IS Act agency, such as ASIS, is engaged in a co-operative intelligence operation, consistent protections for Australian persons should apply for the authorisation of ASIO and the IS Act agencies' activities.

Subsection 13B(1) – When an activity may be undertaken in relation to ASIO

619. Item 11 inserts a new section 13B into the IS Act. This will allow ASIS, subject to the new section 13D, to undertake an activity or a series of activities 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 where the Director-General of Security (Director-General) or a senior ASIO position holder authorised by the Director-General, has notified ASIS in writing that it requires the production of intelligence on the Australian person or class of Australian person.

620. Division 3 will only apply to ASIS activities outside Australia and only when ASIS is undertaking activities to support ASIO in the performance of ASIO's functions.

621. A notice issued by ASIO under this provision notifies ASIS of a requirement to produce intelligence on an Australian person, or a class of Australian person. The notice may identify a number of Australian persons.

Subsection 13B(2) – Conditions

622. Item 11 inserts the new subsection 13B(2) to provide that the undertaking of an activity or series of activities under subsection 13B(1) is subject to any conditions specified in the notice issued under paragraph 13B(1)(d).

623. Notices will not be required to include conditions but if any conditions are included ASIS must comply with them. The ability for the notice to include conditions will assist in ensuring that any intelligence produced by ASIS under this provision meets ASIO's requirements.

Subsection 13B(3) – When notice from ASIO not required – particular activity

624. Item 11 inserts a new subsection 13B(3) to provide that a notice under new subsection 13B(1) will not be required where an ASIS staff member reasonably believes that it is not practicable in the circumstances (like an emergency) for ASIO to notify ASIS in accordance with paragraph 13B(1)(d) before the staff member undertakes the activity.

625. In considering whether it is not practicable in the circumstances for ASIO to notify ASIS, the ASIS staff member will consider the time required for ASIS to seek, and for ASIO to issue, a notice. It will not be practicable in circumstances where it is not possible to contact ASIO to obtain a notice or there is insufficient time to obtain a notice from ASIO and the ASIS staff member believes that there is an immediate need to undertake the activity or that the opportunity to undertake the activity would be lost if there were to be a delay while a notice was obtained. If it is possible to undertake the activity following a delay, the arrangements under the new subsection 13B(1) should be applied. Before undertaking each activity in relation to a particular Australian person without notice from ASIO, the ASIS staff

member must reasonably believe it is not practicable in the circumstances for ASIO to notify ASIS.

626. This amendment addresses the realities of operating in high threat environments overseas. In high threat environments, ASIS staff members put themselves at great personal risk. Requiring them to obtain a written notice from ASIO before producing intelligence that unexpectedly arises may add to this risk and the opportunity to produce valuable intelligence that is relevant to Australia's security may also be lost (for example, intelligence about an imminent terrorist attack).

Subsection 13B(4) – Notification of IGIS

627. Item 11 inserts the new subsection 13B(4). If ASIS undertakes an activity in reliance on the new subsection 13B(3), ASIS must, as soon as practicable, notify the IGIS, in writing, of the activity. This will ensure that the IGIS will have oversight of ASIS's activities under this new provision, including ASIS's compliance with relevant laws and Ministerial guidelines and directions, consistent with the IGIS's existing oversight role.

628. ASIS will also be required to notify ASIO. This will make ASIO aware that ASIS has produced intelligence on an Australian person in support of ASIO's functions without a notice and enable ASIO to decide if it should issue a notice under subsection 13B(1) to enable ASIS to continue to produce intelligence on the Australian person.

Subsection 13B(5) – Effect of this section

629. Item 11 inserts new subsection 13B(5). This amendment makes clear that despite the direction of the Minister which is required under subsection 8(1) of the IS Act that an authorisation be obtained from the Minister under section 9 to produce intelligence on an Australian person, where section 13B applies an authorisation under section 9 will not be required.

630. This new provision should be read in conjunction with the new section 13D, which provides that ASIS will still be required to obtain a Ministerial authorisation under section 9 of the IS Act before undertaking a particularly intrusive activity overseas as defined in section 13D.

631. In undertaking an activity or series of activities under this new Division, the limitations in subsection 6(4) and sections 11, 12 and 13 of the IS Act that apply to ASIS's functions will continue to apply. Importantly in accordance with section 11 of the IS Act, ASIS's activities under this new Division are to be performed only in the interests of Australia's national security, Australia's foreign relations or Australia's economic well-being, and only to the extent that those matters are affected by the capabilities, intentions or activities of people or organisations outside Australia.

Subsection 13B(6) – Incidental production of intelligence

632. Item 11 inserts the new subsection 13B(6). This provision will ensure that an activity or a series of activities does not cease to be undertaken in accordance with section 13B, or for the specific purpose of supporting ASIO in the performance of its functions, only because ASIS also incidentally receives intelligence relevant to ASIS's functions and 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) of the IS Act.

633. The nature of intelligence collection means that while ASIS may undertake an activity to produce intelligence on an Australian person for one purpose it may also incidentally receive other intelligence related to another Australian person. This provision makes it clear that ASIS can receive this other incidental intelligence as part of an activity or series of activities under section 13B where it relates to the involvement or likely involvement in one or more of the activities set out in paragraph 9(1A)(a).

634. Incidental intelligence that concerns an Australian person will be communicated in accordance the new section 13F and the rules made under section 15 of the IS Act. If this incidental intelligence is unrelated to ASIO's requirements, before ASIS is able to produce further intelligence on that Australian person a Ministerial authorisation under section 9 will be required.

635. Clarification is not required for incidental intelligence on a person who is not Australian because the arrangements under section 13B are not needed to produce such intelligence.

Subsection 13B(7) – Authorised staff members

636. Item 11 inserts the new subsection 13B(7). This new provision will ensure that only ASIS staff members or classes of ASIS staff members who have been authorised by the Director-General of ASIS can produce intelligence on an Australian person in accordance with the new subsection 13B(3) where it is not practicable in the circumstances for ASIO to notify ASIS (for example, where there is an imminent terrorist threat).

Subsection 13B(8) – Instruments not legislative instruments

637. Subsection 13B(8) makes it clear that a notice or authorisation made under subsection 13B is not a legislative instrument. This provision is merely declaratory in nature. Notices or authorisations of this type are administrative in character because they are merely the application of a legal power in a particular case – they do not determine or alter the content of the law itself.

Section 13C – Authorised persons for activities undertaken in relation to ASIO

638. Item 11 inserts new section 13C. This provision will allow the Director-General to authorise a senior position-holder, or class of senior position holders, to notify ASIS under paragraph 13B(1)(d) of a requirement for intelligence production on an Australian person or class of Australian persons. Senior position-holder is defined in section 4 of the ASIO Act.

639. Subsection 13C(2) makes it clear that an authorisation made under subsection 13C(1) is not a legislative instrument. This provision is merely declaratory in nature. Authorisations of this type are administrative in character because they are merely the application of a legal power in a particular case, they do not determine or alter the content of the law itself.

Section 13D – Certain action not permitted

640. Item 11 inserts section 13D which will make it clear that the new Division 3 does not allow any act that ASIO could not do in at least one State or Territory, without it being authorised by a warrant issued under Division 2 of Part III of the *Australian Security Intelligence Organisation Act 1979* (ASIO Act) or under Part 22 of the *Telecommunications (Interception and Access) Act 1979* (TIA Act).

641. ASIS will still be required to obtain a Ministerial authorisation under section 9 of the IS Act before undertaking particularly intrusive activities overseas (for example, the use of tracking devices, listening devices and the interception of telecommunications).

Section 13E – Director-General to be satisfied of certain matters

642. Item 11 inserts section 13E into the IS Act to require the Director-General of ASIS to be satisfied there are satisfactory arrangements in place to ensure that activities will be undertaken under section 13B only for the specific purpose of supporting ASIO in the performance of its functions and there are satisfactory arrangements in place to ensure that the nature and consequences of acts done under section 13B will be reasonable, having regard to the purposes for which they are carried out.

643. This provides additional safeguards around ASIS's activities. It will ensure that activities done under section 13B are solely for the purpose of supporting ASIO in the performance of its functions and the nature and consequences of acts done are reasonable, having regard to the purposes for which they are carried out.

Section 13F – Other matters relating to activities undertaken in relation to ASIO

644. Item 11inserts the new section 13F into the IS Act.

ASIO to be consulted before communicating intelligence

645. Subsection 13F(1) provides that ASIS is prohibited from communicating any intelligence produced under the new section 13B to agencies other than ASIO, unless ASIO has been consulted.

Intelligence to be communicated to ASIO

646. Subsection 13F(2) makes it clear that if, in undertaking an activity or series of activities under section 13B, ASIS produces intelligence, ASIS must cause the intelligence to be communicated to ASIO as soon as practicable after the production.

647. The rules made under section 15 of the IS Act will also apply to the communication of any intelligence information that concerns an Australian person. These rules protect the privacy of Australians.

Notices to be made available to the Inspector-General of Intelligence and Security

648. Subsection 13F(3) provides that, if ASIO issues a notice under paragraph 13B(1)(d), the Director-General of ASIS must ensure that a copy of the notice is kept by ASIS and is available for inspection on request by the IGIS. This is consistent with the IGIS's existing

role and facilitates the IGIS's continued oversight of the agencies' activities and their compliance with relevant laws and Ministerial guidelines and directions.

Reports about activities to be given to the responsible Minister

649. Subsection 13F(4) provides that, as soon as practicable after each year ending on 30 June, the Director General of ASIS must give to the responsible Minister in relation to ASIS a written report in respect of activities undertaken by ASIS under section 13B during the year.

650. This will ensure that the Minister responsible for ASIS continues to have appropriate oversight of the activities undertaken by ASIS under this Division.

Section 13G – Guidelines relating to activities undertaken in relation to ASIO

651. Item 11 inserts the new section 13G into the IS Act to enable the responsible Minister in relation to ASIO and the responsible Minister in relation to ASIS to jointly make written guidelines relating to the undertaking of activities under section 13B.

652. Ministers will not be required to make guidelines but if any guidelines are made the agencies must comply with them. This is consistent with existing provisions in the IS Act that enable Ministers to provide guidelines or directions relevant to their agencies.

653. Any guidelines issued under subsection 13G(1) are not a legislative instrument. This provision is declaratory and is intended to assist readers in the interpretation of this provision.

Item 12 – Division 4—Other

Division 4 – Other

654. Item 12 separates Part 2 into divisions and inserts the title of the fourth division, 'Other' consequential to amendments made by items 2, 8 and 11.

Item 13 – Subsection 14(2)

655. Item 13 amends subsection 14(2) of the IS Act. This amendment will extend the limited protection from liability from Australian laws to persons who assist the IS Act agencies outside Australia.

656. This will ensure that persons who assist the IS Act agencies outside Australia are provided with the same limited protection from Australian law as those persons who assist IS Act agencies i Australia where that act is preparatory to, in support of, or otherwise directly connected with the proper performance of the IS Act agencies' functions.

657. 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 IS Act agency.

Item 14 – After subclause 1(1) of Schedule 2

658. Item 14 inserts the new subclause 1(1A) into the IS Act.

659. This amendment implements Recommendation 40 of the PJCIS Report, which recommended that the IS Act be amended to enable ASIS to provide training in self-defence techniques and the use of weapons to persons co-operating with ASIS. 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.

660. The training of individual officers will also be approved by the Minister under the new subclause (3A).

661. The purpose of the training is to enable the person to protect him or herself, protect an ASIS staff member or agent or a person co-operating with ASIS in accordance with section 13.

Item 15 – Subparagraph 1(2)(a)(ii) of Schedule 2

662. Item 15 provides that the use of a weapon or self-defence techniques is not prevented by subsection 6(4) of the IS Act, if it is in training in accordance with the new subclause (1A).

663. This will ensure that the new subclause 1(1A) is limited to ASIS providing training in self-defence techniques and the use of weapons.

Item 16 – After subclause 1(2) of Schedule 2

664. Item 16 clarifies that ASIS staff members and agents are able to use weapons or self-defence techniques in controlled environments, 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 where the use is in the proper performance of a function of ASIS.

665. The guidelines issued by the Director-General under subclause 1(6), and given to the IGIS, will set out the limited circumstances in which this amendment will operate.

666. This provision is not intended to limit the other situations in which ASIS staff member or agents can use, or train in the use of, weapons or self-defence techniques for defensive purposes in accordance with Schedule 2 of the IS Act.

Item 17 – After subclause 1(3) of Schedule 2

667. Item 17 should be read in conjunction with the new subclause 1(1A). This will allow the Minister, by written notice given to the Director-General of ASIS, to approve the provision of a weapon, or training in the use of a weapon or self-defence techniques to individual officers from the small number of Australian agencies that have a lawful right under Australian law to carry weapons (like the Australian Defence Force) or individual officers authority of other countries that have been approved under the new subsection 13(1A). This will ensure that the Minister responsible for ASIS continues to approve the provision of weapons and training by ASIS.

Item 18 – Subclause 1(4) of Schedule 2

668. Item 18 should be read in conjunction with new subclause 1(3A). Consistent with current clause 1(3) of Schedule 2, this will require that a ministerial approval under clause 1(3A) must specify the purposes for which the weapon or training is provided, any conditions that must be complied with in relation to the provision of the weapon or training and if the approval is for the provision of a weapon or training in the use of a weapon - the kind or class of weapon involved.

Item 19 – Subclause 1(5) of Schedule 2

669. Item 19 should also be read in conjunction with the new subclause 1(3A) of Schedule 2. Consistent with the existing clause 1(3), this provisions will require that any approval given by the Foreign Minister under the subclause 1(3A) will be given to the IGIS, who will oversight the operation of these provisions.

Item 20 – Clause 2 of Schedule 2

670. This amendment will ensure people who are approved under subclause 1(3A) of Schedule 2 will not be required under, or by reason of, a State or Territory law to obtain or have a licence or permission for doing any act or thing in accordance with subclause 1(1A) or register any weapon provided in accordance with the new subclause 1(1A). This is consistent with the existing clause 2 of Schedule 2. A requirement to obtain State or Territory licences could prejudice ASIS activities as it would involve disclosure of those activities and the identities of persons undertaking the training. This information is protected from disclosure by sections 39 and 41 of the IS Act.

Schedule 6—Protection of information

Outline of measures

671. Schedule 6 amends the secrecy offences in Division 1 of Part III of the *Australian Security Intelligence Organisation Act 1979* (ASIO Act) and Part 6 of the *Intelligence Services Act 2001* (IS Act). In particular, the Schedule amends the offences in subsection 18(2) of the ASIO Act and sections 39, 39A and 40 of the IS Act. These offences apply to persons who have accessed certain information of ASIO or an IS Act agency while acting in a specified official capacity (for example, as an employee of the relevant agency) and who communicate this information without authorisation.

672. The measures in Schedule 6 make four key amendments to the ASIO Act and IS Act:

(a) an increase in the maximum penalty applying to the offences of unauthorised communication of certain information in subsections 18(2) of the ASIO Act and sections 39, 39A and 40 of the IS Act to 10 years' imprisonment (from two years' imprisonment)

(b) an extension of the unauthorised communication offences in sections 39, 39A and 40 of the IS Act to additional agencies within the Australian Intelligence Community (AIC), namely the Office of National Assessments (ONA) and the Defence Intelligence Organisation (DIO) (new sections 40A and 40B)

(c) the inclusion of new offences in respect of intentional unauthorised dealings with certain records of an intelligence agency, where those dealings stop short of the unauthorised communication of information to a third party, for example, the intentional unauthorised removal, retention, copying or transcription of a record. These new offences apply to all AIC agencies and carry a maximum penalty of three years' imprisonment (new section 18A of the ASIO Act and sections 40C, 40E, 40G, 40J and 40L of the IS Act), and

(d) the inclusion of new offences in respect of the intentional unauthorised recording of certain information or matter. These offences carry a maximum penalty of three years' imprisonment (new section 18B of the ASIO Act and sections 40D, 40F, 40H, 40K and 40M of the IS Act).

673. These amendments will ensure that the secrecy offences in the ASIO Act and the IS Act target, denounce and punish appropriately the wrongdoing inherent in the intentional unauthorised communication of, or dealing with, the official records or information of AIC agencies.

674. In particular, the amendments will rectify two major limitations identified in the coverage of the existing offences in subsection 18(2) of the ASIO Act and subsections 39-40 of the IS Act. The first limitation is that the present maximum penalty applying to these offences (being two years' imprisonment) is disproportionate to the significant, adverse consequences that the unauthorised disclosure of highly classified information can have on a country's reputation, intelligence-sharing relationships and intelligence-gathering capabilities. A higher maximum penalty is needed to reflect the gravity of the wrongdoing inherent in such conduct in the contemporary security environment.

675. The second limitation is that the existing secrecy offences in the ASIO Act and the IS Act focus on the unauthorised communication of information and do not address the wrongdoing associated with any other form of intentional unauthorised dealing with information or records. For example, the existing offences do not have any application to the unauthorised copying, transcription, removal or retention of a record, or the unauthorised making of a new record from sensitive information obtained by a current or a former employee of an intelligence agency. Such conduct is meritorious of a specific criminal sanction in order to reflect the substantial risk it presents to the security of such information, and a legitimate expectation on the part of the Government that persons to whom sensitive materials are entrusted are held to a high standard of conduct in relation to their use, handling and disclosure.

676. Schedule 6 to this Bill is divided into two parts. Part 1 contains the amended and new offences and supporting provisions in the ASIO Act and the IS Act. Part 2 contains consequential amendments to other Acts.

Part 1 – Main amendments (ASIO Act and IS Act)

Australian Security Intelligence Organisation Act 1979

Item 1 – Subsection 18(2) (penalty)

677. Item 1 increases the maximum penalty applying to the offence for unauthorised communication of information in subsection 18(2) of the ASIO Act from two years' imprisonment to 10 years' imprisonment.

678. This measure will ensure that the penalty applying to subsection 18(2) is proportionate to the gravity of the wrongdoing targeted by the offence. As the existing maximum penalty of two years' imprisonment was included in the ASIO Act as originally enacted in 1979, revision is appropriate to ensure its adequacy in the contemporary security environment.

679. Recent domestic and international incidents involving the unauthorised communication of security intelligence-related information illustrate that the existing maximum penalty of two years' imprisonment does not accurately reflect the risk of serious harm to intelligence and security interests that is occasioned by such behaviour. Such risks include jeopardising extant intelligence-gathering operations (including the lives or safety of informants and undercover operatives) or investigations or prosecutions reliant upon intelligence information. The intentional unauthorised communication of intelligence information also risks compromising Australia's intelligence-gathering capabilities by undermining relationships of trust and confidence with foreign intelligence partners and human sources.

680. In addition, the existing maximum penalty of two years' imprisonment limits the effectiveness of the offence as a general deterrent to the intentional unauthorised communication of intelligence information by persons who have accessed that information in an official capacity, for the limited purpose of performing their official duties – for example, a person who accesses such information in their capacity as an affiliate or employee of the Organisation as defined in section 4 of the ASIO Act, or as an official or employee of another Commonwealth agency, for the purpose of performing their duties that official capacity.

Given the potentially devastating consequences 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.

681. A maximum penalty of 10 years' imprisonment gives effect to the policy objective of recognising and communicating the gravity of the wrongdoing inherent in the unauthorised communication of intelligence information, and establishing a strong deterrent to such conduct. In particular, the penalty reflects an appropriate gradation with that applying to the espionage offences in Division 91 of the *Criminal Code 1995* (Criminal Code), which is 25 years' imprisonment.

682. The higher penalty applying to espionage offences in the Criminal Code reflects that these offences contain additional elements to those in subsection 18(2) of the ASIO Act. Namely, the espionage offences require proof of a person's intent to cause certain harm to Commonwealth interests, and proof that the person's conduct resulted in, or was likely to result in, the communication of information to another country or a foreign organisation.

683. In contrast, the conduct constituting an offence under subsection 18(2) of the ASIO Act is less culpable than that constituting the offence of espionage because it does not require a person to form a specific intention that a particular unauthorised communication should cause harm, and nor does it require proof that a foreign government or organisation was the recipient, or likely recipient, of an unauthorised communication. Rather, the wrongdoing inherent in an offence against subsection 18(2) of the ASIO Act is the unauthorised communication of information which is, by definition, of a sensitive nature and carries a high risk of harming national security interests. That is, information which is acquired or prepared by or for the Organisation in connection with the performance of its statutory functions, or information which relates to the performance by the Organisation of its functions.

684. The offence in subsection 18(2) remains subject to multiple statutory safeguards in the ASIO Act, which ensure that its application is limited appropriately. In particular, the commencement of a prosecution requires the consent of the Attorney-General under subsection 18(5) (which is relocated to new section 18C by items 3 and 4 of this Schedule). This consent requirement ensures that all potential prosecutions are scrutinised by both the Commonwealth Director of Public Prosecutions (CDPP) in accordance with the Prosecution Policy of the Commonwealth, and the Attorney-General who can make a determination of the appropriateness (or otherwise) of a prosecution having regard to broader public policy considerations than the CDPP is permitted to take into account under the prosecution policy.

685. This provision is consistent with the general principle of Commonwealth criminal law policy that the Attorney-General, as first law officer, may be required to consent to the prosecution of an offence that could potentially affect Australia's national security or international relations, where there are matters of policy to be weighed up that are best left to elected representatives to decide. The prosecutorial consent requirement further ameliorates the potentially strict application of subsection 18(2) in individual cases.

686. In addition, Division 1 of Part III of the ASIO Act contains a number of lawful communication provisions, to which the offences in subsection 18(2) do not apply. This includes, in paragraphs 18(2)(a)-(c), communications made to the Director-General of

Security or another affiliate or employee of the Organisation in the course of a person's official duties, or communications made with the specific authority or approval of the Director-General or another person authorised by the Director-General. Provision is also made in subsections 18(3)-(4B) and sections 19 and 19A for the communication of information to other agencies or Ministers, in specified circumstances, including:

- the communication of information relevant to the commission or intended commission of a serious crime or communications that are in the national interest: subsections 18(3) and (4)
- the communication of information relevant to the performance of the functions of another Australian intelligence agency: subsection 18(4A) and paragraphs 19A(1)(a)-(c)
- the collection, use and disclosure of personal information in emergencies and disasters in accordance with Part VIA of the *Privacy Act 1988*: subsection 18(4B)
- the communication of information relevant to the security of another country, provided that disclosure is made to an officer of an authority of that country which is approved by the Attorney-General: subsection 19(2), and
- the communication of information to a law enforcement agency, or another Commonwealth or State authority prescribed by regulations, for the purpose of co-operating with or assisting the relevant authority in the performance of its functions, on the request of the head of that agency or authority: subsection 19A(4).

687. The offence provision in subsection 18(2) is further subject to provisions in the legislation of oversight and accountability bodies, which confer an immunity from criminal or civil liability upon persons who produce documents or provide information to the relevant body in accordance with an obligation to do so. For example, subsection 18(9) of the *Inspector-General of Intelligence and Security Act 1986* (IGIS Act) provides that a person is not liable to penalty under any law of the Commonwealth or of a Territory by reason only of the person having given information, produced a document, or answered a question when required to do so in accordance with a written notice issued by the Inspector-General of Intelligence and Security (IGIS) under subsection 18(1) of the IGIS Act.

688. The offence provision in subsection 18(2) of the ASIO Act is further subject to the public interest disclosure regime set out in the *Public Interest Disclosure Act 2013* (PID Act). Section 10 of the PID Act may operate to confer an immunity on an ASIO affiliate or employee from any civil, criminal or administrative liability if the relevant information was communicated in accordance with the PID Act as it applies to the Organisation. In particular, the PID Act allows for the disclosure of information to internal authorised officers or the IGIS.

Item 2 – After subsection 18(2)

689. Item 2 inserts new subsection 18(2A), which provides for an exception to the offence in subsection 18(2). It provides 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.

690. This exception is limited expressly to information or matters which are communicated or made available publicly on an authorised basis. Hence, it does not apply to an unauthorised public communication or disclosure of a record in the nature of a 'leak'.

691. The inclusion of the word 'already' in the provision further limits the exception to a communication or disclosure which is made, in accordance with an authorisation, prior to the person's engagement in the conduct constituting the offence under subsection 18(2). The exception has no application to persons who engage in an unauthorised communication of information, and that information is subsequently made lawfully available. This is consistent with the intention that the offence gives effect to an expectation that persons who are entrusted with sensitive information of the Organisation, or pertaining to its functions, in an official capacity must use and disclose it strictly accordance with the scope of their authority.

692. The note to subsection 18(2A) confirms the application of subsection 13.3(3) of the Criminal Code to the exception. Subsection 13.3(3) provides that a defendant who wishes to rely on any exception provided for by a law creating an offence bears an evidential burden in relation to that matter. This means that a defendant must adduce or point to evidence suggesting a reasonable possibility that the relevant information or matter had been communicated or otherwise made available publicly, on an authorised basis, prior to his or her engagement in the conduct constituting the offence under subsection 18(2). The prosecution must then negate this matter to the legal standard (beyond reasonable doubt).

693. It is legitimate to cast the matters set out in subsection 18(2A) as an exception to the offence in subsection 18(2) rather than including them as elements of the offence. This is because evidence suggesting a reasonable possibility of a prior, authorised public disclosure of the relevant information or matter is readily available to a defendant, since such evidence is necessarily a matter of public record. This might include, for example, evidence suggesting a reasonable possibility that a record had been tabled in Parliament or that information was disclosed by the Government in the course of Parliamentary proceedings, or that information was disclosed by the Minister at a media conference.

694. In addition, it would be counter-productive to include, as an element of the offence, a circumstance that the information or matter was not already disclosed or made available publicly with the authority of the Commonwealth. Such an element would impose an unacceptably onerous burden on the prosecution to prove in every case, beyond reasonable doubt, that there was no prior authorised communication of the relevant information, even where there was no evidence that this was an issue.

695. Given the onerous nature of a requirement on the prosecution to prove, in all cases, that a particular piece of information was not previously communicated publicly, the inclusion of the matters in subsection 18(2A) as elements of the offence in subsection 18(2) could enable otherwise culpable conduct to go unpunished.

Item 3 – Subsection 18(5)

696. Item 3 makes a technical amendment by repealing section 18(5) as a consequential amendment to the insertion of new section 18C by item 4 of this Schedule. As noted above, subsection 18(5) provides that a prosecution for an offence under subsection 18(2) may only be commenced with the prior consent of the Attorney-General. This provision is retained in new section 18C, which applies to offences against section 18(2) and new sections 18A and 18B. New sections 18A, 18B and 18C are inserted by item 4 of this Schedule.

Item 4 – After section 18

697. Item 4 inserts new sections 18A and 18B in Part III of the ASIO Act. These provisions are new offences in respect of intentional unauthorised dealings with records and information acquired or prepared by or on behalf of the Organisation in connection with its functions, or which relate to the performance by the Organisation of its functions.

698. In particular, new section 18A creates an offence in respect of the intentional unauthorised handling of a record of the Organisation by a current or former ASIO affiliate, an ASIO employee (as those terms are defined in section 4 of the Act by reason of Schedule 1) or a person who has previously entered into any contract, agreement or arrangement with the Organisation.

699. New section 18B creates an offence in respect of the intentional unauthorised making of records of information pertaining to the Organisation's performance of its statutory functions. It extends to the same persons as in new section 18A. New section 18C sets out rules in relation to the geographical jurisdiction of the offences in subsection 18(2) and sections 18A and 18B and the commencement of prosecutions for these offences.

700. These new offences will ensure that specific criminal offences are available in relation to all forms of unauthorised dealing with security intelligence-related records and information.

Section 18A – Unauthorised dealing with records

Offence of unauthorised dealing with records – subsection 18A(1)

701. Subsection 18A(1) creates a new offence for the intentional unauthorised dealing with certain records acquired or prepared by the Organisation in connection with its functions, or which relate to the performance by the Organisation of its functions.

Physical element 1 – application of offence to an 'entrusted person': paragraph 18A(1)(a)

702. New paragraph 18A(1)(a) provides that the offence applies to a person who is, or who has been, an 'entrusted person'. This term is defined in subsection 18A(5) as a person who is an ASIO employee, an ASIO affiliate (as these terms are defined in section 4) or any other person who has entered into a contract, agreement or arrangement with ASIO, otherwise than as an ASIO affiliate.

703. The reference in paragraph 18A(1)(a) to a person who 'has been an entrusted person' makes clear that the offence is not limited to a person who is an entrusted person at the time he or she engages in the relevant conduct set out in paragraph 18A(1) (d), or at the time of investigation, arrest, charge or prosecution under subsection 18A(1). Rather, as set out in paragraph 18A(1)(b), he or she must have been an entrusted person at the time at which he or she obtained the record. As such, the offence is intended recognise that obligations of confidentiality in relation to records can apply beyond the duration of a person's status as an 'entrusted person'.

Physical element 2 – person must have obtained a record in his or her capacity as an 'entrusted person': paragraph 18A(1)(b)

704. Paragraph 18A(1)(b) requires that an entrusted person must have obtained a record in his or her capacity as an entrusted person. The term 'record' is defined in subsection 18A(5), (detailed below). Paragraph 18A(1)(b) does not require a record to remain in the possession of the person at the time he or she is investigated in relation to, arrested for, or charged with, an offence under subsection 18B(1).

705. As the physical element in paragraph 18A(1)(b) is a circumstance, the standard fault element of recklessness applies by reason of subsection 5.6(2) of the Criminal Code. This means that the prosecution must establish that a person was aware of a substantial risk that the record came into his or her possession by reason of his or her status as an entrusted person, and nonetheless and unjustifiably in the circumstances known to him or her, took the risk of engaging in the relevant form of conduct set out in paragraph 18A(1)(d).

706. The fault element of recklessness as to a circumstance may also be satisfied by proof of a person's knowledge, pursuant to subsection 5.4(4) of the Criminal Code. Hence, the prosecution may alternatively prove that a person was aware that the record came into his or her possession by reason of his or her status under paragraph 18A(1)(b).

Physical element 3 – the relevant record is a record of the Organisation, or pertains to the Organisation's performance of its functions: paragraph 18A(1)(c)

707. Paragraph 18A(1)(c) requires that the record was acquired or prepared by or on behalf of the Organisation in connection with its functions or relates to the performance by the Organisation of its functions. This includes records acquired by the Organisation which are created by an external organisation, department or body. It also includes any records prepared or created by a person in the course of their current or former employment by the Organisation, or under an agreement, contract or arrangement with the Organisation.

708. For the avoidance of doubt, the term 'acquired' is intended to cover records that have come into the possession of the Organisation by any means. This includes records that have come into the Organisation's possession upon its request, and those which have come into the Organisation's possession without any action on its part – for example, the Organisation's receipt of any records pursuant to a standing information-sharing arrangement with another agency or entity. This is consistent with the use of the term 'acquired by' elsewhere in the Commonwealth statute book, and the ordinary meaning of the term 'acquire' in respect of a record or thing, being to come into a person's possession.

709. As the physical element in new paragraph 18A(1)(c) is a circumstance, the fault element of recklessness applies by reason of subsection 5.6(2) of the Criminal Code. The prosecution must prove that the person was aware of a substantial risk that the record satisfied the requirements of either subparagraph 18A(1)(c)(i) or (ii), and nonetheless and unjustifiably in the circumstances known to him or her, took the risk of engaging in the relevant form of conduct set out in paragraph 18A(1)(a). In accordance with subsection 5.4(4) of the Criminal Code, the prosecution may alternatively prove that the person knew of this circumstance.

Physical element 4 – the person engages in one of the prohibited forms of conduct: paragraph 18A(d)

710. Paragraph 18A(1)(d) sets out the physical element of conduct in relation to a record. The offence applies if a person engages in one of the forms of conduct in relation to a record set out in subparagraphs 18A(1)(d)(i)-(v) (relevant conduct). The term 'record' is defined in new subsection (5) (detailed below). As the physical element in paragraph 18A(1)(d) is conduct, the standard fault element of intention applies by reason of subsection 5.6(1) of the Criminal Code. This means that the prosecution must prove that a person meant to engage in a form of conduct specified in subparagraphs 18A(1)(d)(i)-(v).

711. The prescribed forms of conduct in subparagraphs 18A(1)(d)(i)-(v) are not defined terms in the ASIO Act, and are intended to take their ordinary meanings. Some key aspects of the intended application of these terms to pargraphs18A(1)(d)(i)-(v) are set out below as an aid to interpretation.

(i) Copying the record

712. This phrase is intended to include the copying of a record by any means, such as photocopying, photographing, scanning or otherwise duplicating a physical record. It is also intended to include the duplication by any means of an electronic record, such as by copying a file saved to a computer from one location to another on that computer, or to another computer or storage device. The copying of an electronic record could also include duplicating a saved file to re-format it, placing it into a different electronic database, file directory or electronic location, or attaching it to an email or including it in the body of an email.

(ii) Transcribing the record

713. This phrase is intended to include the writing out or printing in any characters of, or transliterating, the contents of a record, whether in part or in full. It is intended to include, for example, a person who views a record comprising written, printed or visual material (or who listens to a record comprising a sound recording) and seeks to recreate that record or parts of it by writing down or otherwise recording some or all of its contents.

(iii) Retaining the record

714. This phrase is intended to include conduct by which a person keeps in his or her possession or physical control, or continues to use, a record or part of a record. Retention is intended to include, but is not limited to, a person's conduct in continuing to possess or use a record after being requested or instructed to remove it from his or her possession or to cease using it, such as a request or instruction to return a record, dispose of it, or provide it to another person. Retention need not be contingent on an instruction or direction in relation to a person's continued possession or use of a record. Retention may also occur where a person becomes aware that he or she has removed a record, mistakenly or not, and does not return the record.

(iv) Removing the record

715. This phrase is intended to include the removal of a record from any location (physical or electronic) by any means. This includes, for example, moving a record from a place or position within a premises (such as from a secure location to a non-secure location) and removing a record from a premises. It is intended to include the removal of a physical

document from a file, or an electronic document or object from a computer, electronic system or database. For example, the removal of an electronic document could include a person's action in removing a file attached to an email message received by their official work email address, attaching it to a new email message, and sending that message to another email address such as a personal email address.

(v) Dealing with the record in any other manner

716. This phrase is intended cover any other form of conduct in relation to a record that is not capable of being characterised as being within subparagraphs 18A(1)(d)(i)-(iv). It is intended to include, for example, a person who accesses a record. It is also intended to include a person who discloses a record in a manner that does not amount to a communication for the purpose of the offence in subsection 18(2) of the ASIO Act. Subparagraph 18A(1)(d)(v) is necessary to ensure that otherwise culpable conduct does not go unpunished on the basis of a technical construction of the forms of conduct prescribed in subparagraphs 18A(1)(d)(i)-(iv), notwithstanding that the person was not authorised to deal with the relevant record in that way, and thereby placed at risk security intelligence-related information.

Physical element 5 – the relevant conduct was not authorised: paragraph 18A(1)(e)

717. Paragraph 18A(1)(e) requires that the relevant conduct in paragraph 18A(1)(d) must not have been engaged in pursuant to a form of authorisation specified in subparagraphs 18A(e)(i)-(iv).

718. As the physical element in paragraph 18A(1)(e) is a circumstance, the standard fault element of recklessness applies by reason of subsection 5.6(2) of the Criminal Code. The prosecution must prove that a person was aware of a substantial risk that the relevant conduct was not authorised in accordance with any of the matters specified in subparagraphs 18A(1)(e)(i)-(iv), and that he or she nonetheless, and unjustifiably in the circumstances known to him or her, took that risk by engaging in the relevant form of conduct specified in paragraph 18A(1)(d). The fault element of recklessness as to a circumstance may also be satisfied by proof of a person's knowledge, pursuant to subsection 5.4(4) of the Criminal Code. Hence, the prosecution may alternatively prove that a person was aware that the conduct was not authorised in accordance with any of the matters specified in subparagraphs 18A(e)(i)-(iv).

(i) Conduct in the course of the duties of an ASIO employee

719. Subparagraph 18A(1)(e)(i) provides that the relevant conduct was not engaged in, in the case of an ASIO employee, in the course of his or her duties. The phrase 'in the course of the person's duties' is intended to include only the duties of the specific position assigned to the employee at the time he or she engaged in the conduct under paragraph 18A(1)(d). This may include duties set out in a formal duty statement in relation to a person's position, as well as formal duties of general application to all employees of the Organisation. The latter may include requirements or obligations set out in the Organisation's internal personnel-related policy or procedural documents. Conduct in the course of an ASIO employee's duties may also include that which is undertaken on the express direction of an employee's manager or superior (provided that such direction is not manifestly unlawful, or otherwise manifestly exceeds the authority of the relevant manager or superior).

Subparagraph 18A(1)(e)(i) is also intended to include conduct which is commonly understood by an employee and his or her manager or superior to be part of the employee's duties.

720. For the avoidance of doubt, subparagraph 18A(1)(e)(i) is not intended to include any duties of an ASIO employee undertaken in a previous position within the Organisation. For example, if a person transfers from a position in one organisational unit within the Organisation into a position in another organisational unit, the person's duties would be determined by reference to those of his or her position in the organisational unit at the time he or she is alleged to have engaged in a form of conduct prescribed under paragraph 18A(1)(d). A person's duties in a former position would not be material.

721. Similarly, subparagraph 18A(1)(e)(i) is not intended to include any duties of a person that were specific to a particular matter within his or her responsibility, if that matter was not within the person's responsibility at time at which the relevant conduct under paragraph 18A(1)(d) is alleged to have occurred. For example, subparagraph 18A(1)(e)(i) would not apply if a person holding a position within the Organisation had duties requiring him to deal with certain records in relation to a specific matter, and the person continued to deal with those records after the matter was concluded, or he or she was removed from that matter, while still holding the same position.

(ii) Conduct of an ASIO affiliate in accordance with a contract, agreement or other arrangement

722. Subparagraph 18A(1)(e)(ii) applies in relation to the conduct of an ASIO affiliate, in accordance with the relevant contract, agreement or other arrangement under which the person is performing functions or services for the Organisation. A contract may include, for example, contractors or consultants engaged by the Organisation who access and deal with a record in accordance with their retainer to provide services for the Organisation. An agreement may include an instrument in the nature of a memorandum of understanding with a foreign liaison partner, recording the conditions on which access to records is provided (such as limitations on use, handling and disclosure).

723. The term 'arrangement', which is also included in the unauthorised communication offence in subsection 18(2), is intended to be a generic term that covers a person's relationship with the Organisation through which he or she is authorised to deal with records of the Organisation, generally for specified purposes and on specified conditions. It may include, for example, a person who is employed by a company which has a contract or agreement with ASIO. For instance, a consultant to the Organisation, where the relevant contractual relationship is between the consultancy firm that employs the person and the Organisation.

724. The inclusion of an 'arrangement' in subparagraph 18A(1)(e)(ii) is designed to ensure that otherwise culpable conduct does not go unpunished on the basis of a technical determination of the legal nature of the relevant relationship, if it is unclear whether an individual has a contractual or some other form of agreement-based relationship with the Organisation. For example, the inclusion of the term 'arrangement' will ensure that no suggestion or argument can be made that a particular type of relationship with the Organisation was outside the scope of the offence because it did not satisfy the legal elements of a contract or agreement.

(iii) Conduct in accordance with a contract, agreement or arrangement with the Organisation (other than as an ASIO affiliate)

725. Subparagraph 18A(1)(e)(iii) applies to persons who do not satisfy the definition of an ASIO affiliate in section 4 of the ASIO Act. It requires the prosecution to prove that the person was not authorised by a contract, agreement or arrangement with the Organisation to engage in a form of conduct listed in paragraph 18A(1)(d).

726. For example, subparagraph 18A(1)(e)(iii) may apply to officers of other Commonwealth agencies who have received a security briefing in order to receive classified information from, prepared by, or pertaining to, the Organisation, and who deal with a record of such information in accordance with the conditions set out in that briefing, for the purpose of performing their duties as Commonwealth officers (as distinct from performing the functions of, or providing services for, the Organisation). Subparagraph 18A(1)(e)(iii) may also apply to a person who is employed by a private company that has need of sensitive information from, or pertaining to, ASIO but does not perform services or functions for ASIO. Subparagraph 18A(1)(e)(iii) may be satisfied if that person deals with a record other than in accordance with their duties to their employer.

727. Accordingly, subparagraph 18A(1)(e)(iii) ensures that culpable conduct does not go unpunished by subsection 18A(1) due to the technical construction of the term 'ASIO affiliate'. It ensures that persons who access records of, or pertaining to the functions of, the Organisation on conditions as to their use, are within the scope of the offence should they contravene those conditions.

(iv) and (v) Conduct in accordance with the authority or approval of the Director-General or another authorised person

728. Subparagraph 18A(1)(e)(iv) applies to a person who was, at the time the relevant conduct was engaged in, acting within the limits of authority conferred upon him or her by the Director-General of Security (Director-General). Subparagraph 18A(1)(e)(v) applies to a person who was, at the time the relevant conduct was engaged in, acting with the approval of the Director-General or another person who had the authority of the Director-General to give such an approval.

729. For example, the Director-General may authorise a person to exercise certain powers, such as communicating intelligence, under a specific warrant issued by the Attorney-General under the ASIO Act. If a person who is so authorised engages in a form of conduct listed in paragraph 18A(1)(d), in the course of exercising a power under the warrant, this conduct will not contravene subparagraph 18A(1)(e)(iv).

730. The reference to the Director-General's ability to authorise or approve relies on authorities or powers otherwise found in the ASIO Act. For example, subsection 18(1) permits the Director-General to confer authority on a person to communicate intelligence.

Maximum penalty: subsection 18A(1)

731. The offence in new subsection 18A(1) is subject to a maximum penalty of imprisonment for three years. This gives effect to a policy intention that the conduct constituting the offence is less culpable than the conduct constituting an offence against

subsection 18(2) (which is increased to 10 years' imprisonment by item 1 of this Schedule). This gradation of penalties reflects that the wrongdoing targeted by subsection 18A(1) is the placing of security intelligence-related information at risk of unauthorised communication, while the wrongdoing targeted by subsection 18(2) is the unauthorised communication of such information.

732. The maximum penalty of three years' imprisonment is an appropriate deterrent to the conduct constituting an offence against subsection 18A(1), by communicating clearly an expectation that persons who are entrusted with access to records of the Organisation in the course of their official duties are held to a high standard in relation to the handing and use of those records. This penalty is further consistent with the established principle of Commonwealth criminal law policy, documented in the *Guide to Framing Commonwealth Offences, Infringement Notices and Enforcement Powers,* that a heavier penalty is appropriate where the consequences of the offence are particularly dangerous or damaging. Criminal conduct which carries a significant risk of jeopardising Australia's national security, by placing at risk the confidentiality of intelligence-related information, is one such instance of particularly dangerous or damaging conduct.

733. Accordingly, it is appropriate that the offence in subsection 18A(1) is subject to a higher maximum penalty than other statutory secrecy offences that do not specifically target conduct which creates a significant risk that security intelligence information may be compromised. For example, a number of other secrecy offences, such as that in section 70 of the *Crimes Act 1914,* are subject to a maximum penalty of two years' imprisonment.

Exception – record lawfully available: subsection 18A(2)

734. Subsection 18A(2) provides for an exception to the offence in subsection 18A(1), in respect of a record that has already been communicated or made available to the public with the authority of the Commonwealth.

735. This exception is limited expressly to records that have been communicated or made available publicly on an authorised basis. Hence, it does not apply to an unauthorised public communication or disclosure of a record in the nature of a 'leak'. The inclusion of the word 'already' in the provision further limits the exception to a communication or disclosure which is made, in accordance with an authorisation, prior to the person's engagement in the conduct constituting the offence under subsection 18A(1). The exception does not apply to persons who deal with a record on an unauthorised basis, and the relevant record is subsequently communicated or made publicly available on a lawful basis. This is consistent with the intention that the new offence gives effect to an expectation that persons who are entrusted with the records of the Organisation in an official capacity must handle them strictly in accordance with the scope of their authority.

736. The note to subsection 18A(2) confirms the application of subsection 13.3(3) of the Criminal Code to the exception. Subsection 13.3(3) provides that a defendant who wishes to rely on any exception provided for by a law creating an offence bears an evidential burden in relation to that matter. This means that a defendant must adduce or point to evidence suggesting a reasonable possibility that the relevant record had been communicated or otherwise made available publicly, on an authorised basis, prior to his or her engagement in the conduct constituting the offence under subsection 18A(1). The prosecution must then negate this matter to the legal standard (beyond reasonable doubt).

737. It is legitimate to cast the matters set out in subsection 18A(2) as an exemption to the offence in subsection 18A(1) rather than including them as elements of the offence. This is because evidence suggesting a reasonable possibility of a prior, authorised public disclosure of the relevant record is readily available to a defendant, since such evidence is necessarily a matter of public record. This might include, for example, evidence suggesting a reasonable possibility that a record had been tabled in Parliament, was adduced in evidence in a legal proceeding heard in open court, was published on an Australian Government website, or was provided to a third party by a person acting within the scope of his or her authority to do so.

738. In addition, it would be counter-productive to include, as an element of the offence in subsection 18A(1), a circumstance that the record was not already disclosed or made available publicly with the authority of the Commonwealth. Such an element would impose an unacceptably onerous burden on the prosecution to prove in every case, beyond reasonable doubt, that there was no prior authorised communication of the relevant information, even where there was no evidence that this was an issue. Given the onerous nature of a requirement on the prosecution to prove, in all cases, that a particular record was not previously communicated or made available publicly, the inclusion of the matters in subsection 18A(2) as elements of the offence in subsection 18A(1) could enable otherwise culpable conduct to go unpunished.

Alternative verdict: subsections 18A(3) and 18A(4)

739. New subsections 18A(3) and (4) are alternative verdict provisions, which provide that a person who is prosecuted for an offence against subsection 18A(1) may be convicted of an offence against subsection 18B(1). This is provided that the trier of fact is not satisfied that the person is guilty of an offence against subsection 18A(1), but is satisfied the person is guilty of an offence against section 18B, and the person has been accorded procedural fairness in relation to section 18B.

740. These provisions are intended to cover, for example, the scenario in which a person is prosecuted for offence under section 18A(1) in respect of transcribing a record contrary to subparagraph 18(1)(d)(ii) and paragraph 18(1)(e). However the jury considers that the evidence, in fact, supports a finding that the person made a contemporaneous note of his or her recollections of that record (rather than a transcription proper) and hence made a new record of information contained in the record, contrary to subsection 18B(1). In these circumstances, provided that the trial judge is satisfied the person has been accorded procedural fairness in relation to subsection 18B(1), it would be open to the jury to return a verdict of guilty in relation to subsection 18B(1).

741. An alternative verdict provision is appropriate given that both subsections 18A(1) and 18B(1) carry an identical maximum penalty, and their elements are similar because they are directed to closely related forms of wrongdoing. Subsections 18A(3) and (4) provide for an efficient and procedurally fair means of dealing with persons who engage in unauthorised conduct in relation to a record, which a trier of fact considers would satisfy the elements of subsection 18B(1) rather than subsection 18A(1) as prosecuted.

Definitions for the purpose of section 18A: subsection 18A(5)

Entrusted person

742. The term 'entrusted person' covers three categories of persons who are subject to the offence in subsection 18A(1). These persons are: ASIO employees, ASIO affiliates, and persons who have entered into a contract, agreement or arrangement with ASIO otherwise than as ASIO affiliates. The terms 'ASIO employee' and 'ASIO affiliate' are defined in section 4 of the ASIO Act (via amendments in Schedule 1).

743. For the avoidance of doubt, there is a distinction between a person who is an ASIO affiliate, and a person who has entered into a contract, agreement or arrangement with ASIO other than as an ASIO affiliate. The definition of an ASIO affiliate in section 4 of the ASIO Act (as inserted by Schedule 1) applies to a person who has entered into a contract, agreement or arrangement with the Organisation, for the purpose of performing functions or services for the Organisation. This may include, for example, a contractor or consultant to the Organisation.

744. The term 'entrusted person' includes persons who have entered into a contract, agreement or arrangement with ASIO other than as an ASIO affiliate, to ensure that the offence in subsection 18A(1) applies to persons whose contract, agreement or arrangement is not for the performance of functions or services for the Organisation. This may include, for example, persons (such as officers of other Commonwealth agencies) who have received a security briefing to receive classified information from, prepared by, or pertaining to, the Organisation. Security briefings may be used as a pre-requisite to a person's receipt of records or information from, prepared by or pertaining to the Organisation. Such briefings can require a person to agree to certain terms on which the records or information are to be provided. These include conditions on the person's use, handling and disclosure of such records or information.

745. Coverage of each of these three categories of person is necessary to ensure that the offence in subsection 18A(1) applies to all persons who are given access to information or records acquired by or prepared for the Organisation in connection with its functions, or which relate to the performance by the Organisation of its functions. This coverage ensures that a person's culpable conduct does not go unpunished on the basis of a technical construction of the precise type of his or her relationship with the Organisation under which he or she was provided with access to information or records subject to certain conditions (including limitations on the use, disclosure or other forms of dealing with information or records).

Record

746. A record is defined to mean a document or any other object by which words, images, sounds or signals are recorded or stored or from which information can be obtained. It includes part of a record (being part of a document or object).

747. As the note to the definitional provision makes clear, the definition of the term 'document' in section 2B of the *Acts Interpretation Act 1901* (Acts Interpretation Act) is incorporated in the definition of 'record' in subsection 18A(5) of the ASIO Act. This ensures the term 'document' is given an appropriately broad meaning in relation to the offence in

subsection 18A(1). In particular, a document includes both physical documents and information that is stored or recorded by means of a computer.

Signals

748. The term 'signals', as it is used in the definition of 'record' in subsection 18(5), includes electromagnetic emissions (which, in turn, is taken to include light emissions). This definition replicates that in section 22 of the ASIO Act for the purpose of Division 2 of Part III (special powers). The inclusive nature of the definition reflects an intention that the term be given an expansive interpretation.

Section 18B – Unauthorised recording of information or matter

749. The offence in new subsection 18B(1) cover the intentional unauthorised making of records of information or matters in connection with, or relating to, the Organisation's performance of its statutory functions. It supplements the offence in subsection 18A(1) (unauthorised dealing with records) by ensuring that such conduct is covered by the offences in Part III of the ASIO Act.

750. The absence of an offence in the nature of that in subsection 18B(1) in the ASIO Act creates an unacceptable risk that culpable conduct may go unpunished. In particular, there may be instances in which the intentional unauthorised making of a record may not be covered by the offence in subsection 18A(1), if the information or matter in question is not referrable to a specific record of the Organisation. Similarly the unauthorised communication offence in subsection 18(2) would not be open unless the relevant information or matter was communicated to a third party. Accordingly, in the absence of section 18B, there would be an arbitrary distinction between culpable and non-culpable conduct on the basis of a technical matter of form, notwithstanding that the person engaged in unauthorised conduct which placed at risk sensitive information. That is, the availability of a criminal sanction would depend on a distinction between whether a person's unauthorised conduct was in relation to his or her dealing with a 'record', or 'information' or a 'matter'.

Physical element 1 – application of offence to an 'entrusted person': paragraph 18B(1)(a)

751. Paragraph 18B(1)(a) provides that the offence applies to a person who is, or has been, an 'entrusted person'. The term 'entrusted person' is defined in subsection 18B(5) as having the same meaning in section 18A, being an ASIO employee, an ASIO affiliate or a person who has entered into a contract, agreement or arrangement with ASIO, other than as an ASIO affiliate.

Physical element 2 – information or matter has come to the knowledge of the person in the person's capacity as an entrusted person: paragraph 18B(1)(b)

752. Paragraph 18B(1)(b) requires the relevant information or matter to have come into the knowledge or possession of the person by reason of his or her status as an entrusted person. Consistent with the elements of the offence in subsection 18A(1), paragraph 18B(1)(b) does not require that a person must remain an entrusted person at the time of making a record of the information or matter under paragraph 18B(1)(d), or at the time of investigation, arrest, charge or prosecution in relation to an offence against subsection 18B(1). Rather, the material time is when the information or matter came into his or her possession.

753. As the physical element in paragraph 18B(1)(b) is a circumstance, the standard fault element of recklessness applies by reason of subsection 5.6(2) of the Criminal Code. This means that the prosecution must establish that a person was aware of a substantial risk that the information or matter came into his or her knowledge or possession by reason of his or her status as an entrusted person, and nonetheless and unjustifiably in the circumstances known to him or her, took the risk of engaging in the relevant form of conduct set out in paragraph 18B(1)(d).

754. The fault element of recklessness as to a circumstance may also be satisfied by proof of a person's knowledge, pursuant to subsection 5.4(4) of the Criminal Code. Hence, the prosecution may alternatively prove that a person was aware that the record came into his or her possession by reason of his or her status as an entrusted person.

Physical element 3 – connection of the information or matter to ASIO: paragraph 18B(1)(c)

755. Paragraph 18B(1)(c) requires the information or matter to have been acquired by or prepared by, or on behalf of, the Organisation in connection with its functions, or relates to the performance by the Organisation of its functions.

756. This includes any information or matter acquired by the Organisation which is provided by an external organisation, department or body. It also includes any information or matter generated by a person in the course of their current or former employment by the Organisation, or under an agreement, contract or arrangement with the Organisation.

757. As with the offence in subsection 18A(1), for the avoidance of doubt, the term 'acquired' in paragraph 18B(1)(c) is intended to cover information or matter that has come into the possession of the Organisation by any means. This includes information or matter that has come into the Organisation's possession upon its request, and that which has come into the Organisation's possession without any action on its part. For example, the Organisation's receipt of any information pursuant to a standing information-sharing arrangement with another agency or entity. This is consistent with the use of the term 'acquired by' elsewhere in the Commonwealth statute book, and the ordinary meaning of the term 'acquire' in respect of information or matter, being to come into a person's possession.

758. As the physical element in new paragraph 18B(1)(c) is a circumstance, the fault element of recklessness applies by reason of subsection 5.6(2) of the Criminal Code. The prosecution must prove that the person was aware of a substantial risk that the information or matter satisfied the requirements of paragraph 18B(1)(c), and nonetheless and unjustifiably in the circumstances known to him or her, took the risk of engaging in the relevant form of conduct set out in paragraph 18B(1)(a). In accordance with subsection 5.4(4) of the Criminal Code, the prosecution may alternatively prove that the person knew of this circumstance.

Physical element 4 – making a record of ASIO information or matter: paragraph 18B(1)(d)

759. Paragraph 18B(1)(d) applies to a person who makes a record of information or a matter. The making of a record is intended to cover the conduct of persons who make a new record, as defined in subsection 18B(5) for the purpose of the offence in subsection 18B(1). This may include, for example, the conduct of a person who hears a conversation or sees a written report in the course of his or her official engagement with the Organisation, and later writes down a note of the contents of the conversation or report based on his or her

recollection. The term 'record' for the purpose of subsection 18B(1) is identical to the definition of this term in subsection 18A(5) in relation to the offence in subsection 18A(1).

760. As the physical element in paragraph 18(1)(d) is that of conduct, the fault element of intention applies by reason of subsection 5.6(1) of the Criminal Code. This means that the prosecution must establish that a person meant to make a record of information of a matter as per subsection 5.2(1) of the Criminal Code.

Physical element 5 – the making of the record was not authorised: paragraph 18B(1)(e)

761. Paragraph 18B(1)(e) requires that the record must not have been made in accordance with a form of authorisation specified in subparagraphs 18B(1)(i)-(iv). These forms of authorisation are identical to those in relation to paragraph 18A(1)(e). Similar to section 18A, it is not intended that section 18B create a new power for the Director-General to authorise or approve conduct. The ability of the conduct to be authorised or approved for the purpose of section 18B must arise from a provision other than sections 18A or 18B.

762. As the physical element in paragraph 18B(1)(e) is a circumstance, the standard fault element of recklessness applies by reason of subsection 5.6(2) of the Criminal Code. The prosecution must prove that a person was aware of a substantial risk that the relevant conduct was not authorised in accordance with any of the matters specified in subparagraphs 18B(1)(e)(i)-(iv), and that he or she nonetheless, and unjustifiably in the circumstances known to him or her, took that risk by making the record of the information or matter. The fault element of recklessness as to a circumstance may also be satisfied by proof of a person's knowledge, pursuant to subsection 5.4(4) of the Criminal Code. Hence, the prosecution may alternatively prove that a person was aware that the conduct was not authorised in accordance with any of the matters specified in subparagraphs 18B(1)(e)(i)-(iv).

Maximum penalty: subsection 18B(1)

763. The offence in subsection 18B(1) carries a maximum penalty of three years' imprisonment. This maintains parity with the penalty applying to subsection 18A(1).

Exception – information or matter lawfully available: subsection 18B(2)

764. Subsection 18(2) provides for an exemption in respect of information or matters that have already been communicated or made available to the public with the authority of the Commonwealth. A defendant bears an evidential burden in respect of this matter, pursuant to subsection 13.3(3) of the Criminal Code.

765. This provision is identical to the exemptions to the offences in subsections 18(2) and 18A(1) inserted by this Schedule, and is supported by the same policy justification as applies to those exemptions.

Alternative verdict: subsections 18B(3) and (4)

766. Subsections 18B(3) and (4) insert identical alternative verdict provisions to those in subsections 18A(3) and (4). A person who is prosecuted for an offence against subsection 18B(1) may be convicted of an offence under subsection 18A(1). This is provided that the trier of fact is not satisfied the person is guilty of an offence against subsection 18B(1), but is satisfied to the legal standard that the person is guilty of an offence

against subsection 18A(1), and the person has been accorded procedural fairness in relation to the finding of guilt.

767. The alternative verdict provisions in subsections 18B(3) and (4) are intended to cover, for example, the circumstances in which a jury is not satisfied that a person who is prosecuted for an offence against subsection 18B(1) has made a record of information without authorisation, but is satisfied that the evidence supports a finding that the person has copied, transcribed, removed or otherwise dealt with a record without authorisation, contrary to paragraphs 18A(1)(d) and (e). Provided that the trial judge is satisfied the person has been accorded procedural fairness in relation to an offence against subsection 18A(1), subsections 18B(3) and (4) will ensure it is open to the jury to convict the person of an offence against subsection 18A(1).

768. Consistent with subsections 18A(3) and (4), the alternative verdict provisions in subsections 18B(3) and (4) will provide an efficient and procedurally fair means of dealing with persons who engage in unauthorised conduct in relation to a record, which trier of fact considers would satisfy the elements of subsection 18A(1) rather than subsection 18B(1) as prosecuted. Such a provision is appropriate given that both subsections 18A(1) and 18B(1) carry an identical maximum penalty, and their elements are similar, reflecting that they target closely related forms of wrongdoing.

Definitions: subsection 18B(5)

769. Subsection 18B(5) defines the terms 'entrusted person' and 'record' as having the same meaning as in section 18A.

Section 18C – Offences against subsection 18(2) and sections 18A or 18B – general rules

Extended geographical jurisdiction: subsections 18C(1)-(2)

770. New subsection 18C(1) provides that the offences in subsection 18(2) and sections 18A and 18B are subject to Category D extended geographical jurisdiction under section 15.4 of the Criminal Code. This means that the offences apply whether or not the relevant conduct occurs in Australia, and whether or not the person alleged to have committed the offence is an Australian citizen, and whether or not there is an equivalent offence in the law of the local jurisdiction in which the conduct constituting the offence is said to have occurred.

771. 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.

Accordingly, Category D geographical jurisdiction will ensure that such persons are culpable, in addition to ASIO employees or affiliates who are based overseas.

772. The commencement of a prosecution of a person other than an Australian citizen, in relation to conduct occurring wholly in a foreign country, is subject to the Attorney-General's consent under section 16.1 of the Criminal Code. This operates as a safeguard to ensure that such prosecutions are not commenced in inappropriate circumstances, having regard to public policy considerations in relation to matters of international relations and national security.

773. Subsection 18C(2) confirms the intention that the application of extended geographical jurisdiction under section 15.4 of the Code to the offences in subsection 18(2) and sections 18A and 18B does not modify or otherwise affect the geographical jurisdiction applying to any other offence provision in the ASIO Act. This provision is necessary because the existing offences in the ASIO Act were enacted prior to the commencement of the geographical jurisdiction provisions in Part 2.7 of Criminal Code on 24 May 2001, which are of prospective application. (That is, Part 2.7 of the Criminal Code applies to offences created from its commencement, unless a Commonwealth law provides that a specific category of geographical jurisdiction under Part 2.7 applies to a particular offence.) Accordingly, subsection 18C(2) makes clear that the application of Category D extended geographical jurisdiction to the offences listed in subsection 18C(1) does not evince any intention to displace the pre-2001 position in relation to the geographical jurisdiction of any other offence provision in the ASIO Act. The geographical jurisdiction of the pre-2001 offences continues to be determined on the interpretation of each offence provision according to general principles of statutory interpretation. Subsection 18C(2) makes clear that new subsection 18C(1) is not intended to have any effect on this position in relation to pre-2001 offences.

Institution of prosecution: subsections 18C(3)-(5)

774. Subsections 18C(3)-(5) require the Attorney-General to consent to a prosecution of an offence under subsection 18(2) and sections 18A and 18B. A prosecutorial consent requirement operates as an additional safeguard in the enforcement of the offences.

775. Subsection 18C(4) confirms that a person may be arrested in relation to, charged with, and remanded in custody or released on bail in relation to a charge of, an offence under subsection 18A(1) in the absence of the Attorney-General's consent to the commencement of a prosecution under subsection 18(4). Subsection 18C (5) further confirms that an accused person may be discharged if proceedings are not commenced within a reasonable time.

Item 5 – Section 22 (definition of *signals*)

776. Item 5 makes a technical amendment to the definition of 'signals' in section 22 of the ASIO Act, which defines this term for the purpose of special powers in Division 2 of Part III. This amendment is consequential to the definition of 'signals' as it is used in Division 1 of Part III for the purpose of the secrecy offences in subsection 18(2) and sections 18A and 18B (pursuant to the relevant amending items in this Schedule). It is also consequential to the insertion of a definition of 'signals' in Part 6 of the IS Act (pursuant to the relevant amending items in Part 2 of this Schedule).

777. The definition of the term 'signals' in section 22 includes light emissions and electromagnetic emissions. As light emissions are a form of electromagnetic emissions, the inclusive reference to both terms is not necessary. Item 5 therefore repeals the reference to light emissions. This amendment does not affect the substantive coverage of the definition, including in relation to its coverage of light emissions.

Intelligence Services Act 2001

778. Schedule 6 further amends the secrecy offence provisions in Part 6 of the IS Act to include offences corresponding to those in subsection 18(2) and sections 18A and 18B of the ASIO Act, in respect of all AIC agencies.

Items 6 and 7– Section 3

779. Items 6 and 7 amend section 3 of the IS Act to include definitions of two terms used in the new and amended offences in the IS Act.

780. Item 6 defines the term 'record' for the purpose of each of the new and amended offences. 'Record' is defined in identical terms to the definition in subsections 18A(5) and 18B(5) of the ASIO Act. It means a document or any other object by which words, images, sounds or signals are recorded or stored, or from which information can be obtained. The term includes part of a record. As the note to the definition makes clear, the term 'document' as it is used in the definition of a 'record' is defined by reference to the definition of 'document' in section 2B of the Acts Interpretation Act.

781. Item 7 defines the term 'signals' as it is used in the definition of 'record'. The term 'signals' is defined in identical terms to subsections 18A(5), 18B(5) and section 22 of the ASIO Act. The inclusive nature of this definition makes clear the intention that it is to be given an expansive interpretation. For the avoidance of doubt, the term 'electromagnetic emissions' as it is used in the inclusive definition of 'signals' inserted by item 2B of the Acts Interpretation Act is intended to include light signals which are, by their nature, a form of electromagnetic emission.

Item 8 – Before section 39

782. Item 8 inserts a new Division 1 of Part 6 of the IS Act, in which the amended and new secrecy offences are contained (sections 39-40M.) The amended and new offences in sections 39-40M are inserted by items 9-22 of this Schedule.

Items 9-22 – New and amended secrecy offences in the IS Act: sections 39-40M

783. Items 9-22 amend or insert new secrecy offences in Part 6 of the IS Act. These are divided into three broad categories, being offences in relation to:

- the unauthorised communication of certain information
- the unauthorised dealing with records, and
- the unauthorised recording of information or matters.

784. The offences in ss 39-40M apply each category of offence to each agency subject to the IS Act. These agencies are ASIS, the AGO, the ASD, DIO and ONA.

785. The AGO and ASD are renamed by the amending items in Schedule 7. These agencies are presently referred to in the IS Act, including in the secrecy offences in sections 39A and 40, as the Defence Imagery and Geospatial Organisation (DIGO) and the Defence Signals Directorate (DSD) respectively.

Offences in relation to the unauthorised communication of certain information:

- Items 9-11 – amendments to section 39 offence – ASIS
- Items 12-14 –amendments to section 39A offence – AGO
- Items 15-17–amendments to section 40 offence – ASD, and
- Item 18 – new offences – section 40A (ONA), section 40B (DIO).

786. Items 9-18 are directed to offences in respect of the unauthorised communication of certain information. Items 9-17 amend the existing unauthorised communication offences in sections 39, 39A and 40 (applying to ASIS and the agencies presently referred to as DIGO and DSD).

787. Item 18 inserts two new unauthorised communication offences, in sections 40A and 40B, applying to ONA and DIO respectively.

Items 9-17 – Amendments to existing unauthorised communication offences: sections 39, 39A and 40 (ASIS, AGO and ASD)

788. Items 9-17 amend the existing unauthorised communication offences in sections 39, 39A and 40 by making three amendments to each of these sections as follows.

Items 9, 12 and 15 – physical elements 1 and 2– communication of information or matter relating to the agency's functions: paragraph (1)(a) of sections 39, 39A and 40

789. Paragraph (1)(a) in each of sections 39, 39A and 40 require that a person must not communicate any information or matter that was prepared by or on behalf of the relevant agency (ASIS, AGO, ASD or DIO) in connection with its functions, or relates to the performance by that agency of its functions except as provided in the section.

790. Items 9, 12 and 15 amend paragraph (1)(a) of each of sections 39, 39A and 40 to additionally include any information or matter that was received by the relevant agency.

791. The term 'acquired' is intended to cover information that has come into the possession of the relevant agency by any means. This includes information or matter that has come into the agency's possession upon its request, and that which has come into the agency's possession without any action on that agency's part. For example, an agency's receipt of any information or matter pursuant to standing information-sharing arrangements with another entity. This is consistent with the usage of the term 'acquired by' elsewhere in the Commonwealth statute book, and the ordinary meaning of the term 'acquire' in respect of any information or matter, being to come into a person's possession.

792. There are two physical elements in paragraph (1)(a), with the result that discrete fault elements apply to each physical element. The first physical element is that a person must communicate any information or matter. As this physical element is that of conduct,

subsection 5.6(1) of the Criminal Code provides that the attendant fault element is that of intention, which means the prosecution must prove to the legal standard that the person meant to communicate the information or matter.

793. The second physical element in paragraph (1)(a) is the circumstance that the information or matter was prepared or acquired by or on behalf of the agency, in connection with its functions, or that the information or matter relates to the performance by the agency of its functions. As this element is a circumstance, subsection 5.6(2) of the Criminal Code provides that the relevant fault element is that of recklessness, meaning that the prosecution must prove that the defendant was aware of a substantial risk that the relevant circumstance existed but nonetheless and unjustifiably in the circumstances took the risk of making the communication in the absence of authorisation. Alternatively, subsection 5.4(4) of the Criminal Code provides that recklessness may be satisfied by proof of a person's knowledge of the relevant circumstance.

Items 10, 13 and 16 – maximum penalty applying to subsections 39(1), 39A(1) and 40(1)

794. Items 10, 13 and 16 increase the maximum penalty applying to the offences in sections 39(1), 39A(1) and 40(1) to 10 years' imprisonment (presently two years' imprisonment, 120 penalty units, or both). The increase in maximum penalty is aligned with that in relation to the corresponding unauthorised communication of information offence in subsection 18(2) of the ASIO Act.

795. For the reasons set out above in relation to subsection 18(2) of the ASIO Act, this increase in maximum penalty is necessary to reflect the gravity of the wrongdoing inherent in the unauthorised communication of intelligence-related information, including the significant risk of harm to Australia's national security that such conduct presents.

Items 11, 14 and 17 – exception – information or matter lawfully available: subsection (2) of sections 39, 39A and 40

796. Items 11, 14 and 17 repeal the existing subsection (2) of sections 39, 39A and 40 (containing a prosecutorial consent requirement from the Attorney-General in relation to these offences) and substitute this with an exception to the offences in subsection (1) of each section. The repeal of the existing provisions in subsection (2) is necessary because the prosecutorial consent requirement is relocated to a single provision, applying to all offences in the new Division 1 of Part 6 of the IS Act, in new section 41A (inserted by amending item 21 of this Schedule).

797. The new subsection (2) in each of sections 39, 39A and 40 provides that the offences in subsection (1) of each section do not apply to information or matter that has already been communicated or made available to the public with the authority of the Commonwealth.

798. As this provision is an exception to an offence, subsection 13.3(3) of the Criminal Code applies, with the result that the defendant bears the evidential burden in relation to this matter. This is confirmed by the note to subsection (2). The imposition of the evidential burden on the defendant means that he or she must adduce or point to evidence suggesting a reasonable possibility that the information or matter was not already communicated or made publicly available with the authority of the Commonwealth. The prosecution must then negate this to the legal standard (beyond reasonable doubt).

799. The exception in subsection (2) is in identical terms to the exceptions applying to subsection 18(2) and sections 18A and 18B of the ASIO Act. Accordingly, it is intended to take the same meaning in all provisions, as detailed in the commentary on the ASIO Act provisions above. In particular, the exception does not apply to the unauthorised public communication or disclosure of information or matter, such as that in the nature of a 'leak'. Similarly, the exception does not exculpate a person who makes an unauthorised communication of information or matter which is subsequently made public with the authority of the Commonwealth. This reflects the policy intent of the offence to ensure that persons who are entrusted with sensitive information are held to an appropriately high standard of conduct in relation to its use, handling and disclosure.

Item 18 – New unauthorised communication offences in sections 40A and 40B (ONA and DIO)

800. Item 18 inserts identical offences to those in sections 39, 39A and 40 (as amended by items 9-17 of this Schedule) in respect of the unauthorised communication of information or matters prepared or acquired by or on behalf of ONA or DIO in connection with either agency's functions, or information which relates the performance by either agency of its functions. New section 40A contains the offence in respect of ONA and new section 40B contains the offence in respect of DIO.

801. Both sections 40A and 40B contain identical elements, offence-specific defences and penalties to those in sections 39, 39A and 40 (as amended by this Schedule to the Bill). These provisions are, in turn, consistent with the unauthorised communication offence in subsection 18(2) of the ASIO Act (as amended by this Schedule).

802. Accordingly, the policy justification applying to the offences in sections 40A and 40B is identical to that outlined above in relation to sections 39-40 of the IS Act and subsection 18(2) of the ASIO Act. It is considered appropriate that persons who place at risk information pertaining to the functions of intelligence agencies are liable to a criminal sanction that specifically targets this wrongdoing, given the significant risk to national security that such conduct presents.

Physical elements 1 and 2 – communication of information or matter relating to the agency's functions: paragraph (1)(a)

803. The physical elements in paragraph (1)(a) of sections 40A and 40B are identical to those in paragraph (1)(a) of sections 39, 39A and 40 as set out above in relation to amending items 9, 12 and 15 of this Schedule.

804. In particular, the prosecution must prove that the person intentionally communicated any information or matter (by reason of subsection 5.6(1) of the Criminal Code). The prosecution must also prove that the information or matter was acquired or prepared by, or on behalf of, the relevant agency in connection with its functions, or related to the performance by the agency of its functions. The prosecution must prove that the person was reckless as to this circumstance (by reason of subsection 5.6(2) of the Criminal Code.)

805. The term 'acquired' as it is used in paragraph (1)(a) of sections 40A and 40B is intended to take the same meaning as per paragraph (1)(a) of sections 39, 39A and 40, as set out under the commentary on amending items 9, 12 and 15 of this Schedule to the Bill.

Physical element 3 – reason by which the information or matter came into the person's knowledge or possession: paragraph (1)(b)

806. Paragraph (1)(b) of each of sections 40A and 40B requires the prosecution to prove that the information or matter came into the person's knowledge or possession by reason of one of the matters set out in subparagraphs (b)(i)-(iii). These are that the person is or was a staff member of the relevant agency, that the person has entered into any contract, agreement or arrangement with the agency or that the person has been an employee or agent of a person who has entered into a contract, agreement or arrangement with the relevant agency.

807. The terms 'contract', 'agreement' and 'arrangement' are intended to take an identical meaning to that in subsection 18(2) and section 18A and 18B of the ASIO Act, as set out in the above commentary on the relevant amending items in this Schedule to the Bill.

808. As paragraph (1)(b) is a circumstance, the prosecution must prove that the person was reckless in relation to one of the matters in subparagraphs (b)(i)-(iii), by reason of subsection 5.6(2) of the Criminal Code. This means that the prosecution must prove that the person was aware of a substantial risk that one of the circumstances in subparagraphs (b)(i)-(iii) existed, and nonetheless and unjustifiably in the circumstances made the unauthorised communication.

Physical element 4 – unauthorised nature of communication: paragraph (1)(c)

809. Paragraph (1)(c) of each of subsections 40A and 40B requires the prosecution to prove that the relevant communication was not made under any of the forms of authority set out in subparagraphs (i)-(iv).

810. As the physical element in paragraph (1)(c) is a circumstance, the standard fault element of recklessness applies by reason of subsection 5.6(2) of the Criminal Code. The prosecution must prove that a person was aware of a substantial risk that the relevant conduct was not authorised in accordance with any of the matters specified in subparagraphs (c)(i)-(iv), and that he or she nonetheless, and unjustifiably in the circumstances known to him or her, took that risk by engaging in the relevant form of conduct specified in paragraph (1)(a). The fault element of recklessness as to a circumstance may also be satisfied by proof of a person's knowledge, pursuant to subsection 5.4(4) of the Criminal Code. Hence, the prosecution may alternatively prove that a person was aware that the conduct was not authorised in accordance with any of the matters specified in subparagraphs (c)(i)-(iv).

(i) Communication to the relevant agency head or another agency staff member, in the course of the person's duties as a staff member of the agency

811. Subparagraph (c)(i) of each of sections 40A(1) and 40B(1) provides that the communication must not have been made to the relevant agency head or another agency staff member in the course of a person's duties as a staff member.

812. Consistent with corresponding elements of the offence in subsection 18(2) of the ASIO Act (as amended by this Schedule), the phrase 'in the course of the person's duties' is intended to include only the duties of the specific position assigned to the employee at the time he or she engaged in the conduct under paragraph (1)(a). This may include duties set out in a formal duty statement in relation to a person's position, as well as formal duties of

general application to all employees of the agency. (The latter may include requirements or obligations set out in the agency's internal personnel-related policy or procedural documents.) Conduct in the course of an employee's duties may also include that which is undertaken on the express direction of an employee's manager or superior (provided that such direction is not manifestly unlawful, or otherwise manifestly exceeds the authority of the relevant manager or superior). Subparagraph (i) is also intended to include conduct which is commonly understood by an employee and his or her manager or superior to be part of the employee's duties. For the avoidance of doubt, subparagraph (i) is not intended to include any duties of an agency employee undertaken in a previous position within the agency, or in respect of a matter on which the person no longer works within their current role.

(ii) Communication to the agency head or another agency staff member in accordance with a contract, agreement or arrangement

813. Subparagraph (c)(ii) of each of subsections 40A(1) and 40B(1) provides that the communication must not have been made to the relevant agency head or another agency staff member by the person in accordance with a contract, agreement or arrangement.

814. The terms 'contract', 'agreement' and 'arrangement' are intended to take a consistent meaning to that in subsection 18(2) and section 18A and 18B of the ASIO Act as amended by this Schedule. Consistent with the above commentary on those provisions, a contract may include, for example, contractors or consultants engaged by or on behalf of the relevant agency who access and deal with a record in accordance with their retainer to provide services. An agreement may include an instrument in the nature of a memorandum of understanding with a foreign liaison partner, recording the conditions on which access to information or records is provided (such as limitations on use, handling and disclosure).

815. The term 'arrangement', is intended to be a generic term that covers a person's relationship with the relevant agency (or an intermediary) through which he or she is authorised to deal with certain information or records, generally for specified purposes and on specified conditions. This may include, for example, persons (such as officers of other Commonwealth agencies) who have received a security briefing to receive certain classified information. Security briefings may be used as a pre-requisite to a person's receipt of such records or information. Such briefings can require a person to agree to certain terms on which the records or information are to be provided. These include conditions on the person's use, handling and disclosure of such records or information.

816. The inclusion of an 'arrangement' in subparagraph (ii) is designed to ensure that otherwise culpable conduct does not go unpunished on the basis of a technical determination of the legal nature of the relevant relationship, if it is unclear whether an individual has a contractual or some other form of agreement-based relationship.

(iii) Communication by the person in the course of the person's duties as a staff member, within the limits of authority conferred on the person by the agency head

817. Subparagraph (c)(iii) requires the prosecution to prove that the communication was not made by the person in the course of his or her duties as a staff member, within the limits of authority conferred upon him or her by the relevant agency head. For example, the agency head may authorise a person, as part of his or her duties, to communicate certain information to certain persons.

(iv) Communication with the approval of the agency head or another authorised staff member

818. Subparagraph (c)(iv) requires the prosecution to prove that the person did not make the communication with the approval of the relevant agency head or another staff member having the authority of the relevant agency head.

819. This subparagraph covers instances in which the relevant agency head or another authorised staff member specifically approves a particular communication as distinct from a staff member's general authorisation in the course of his or her duties as provided for in subparagraph (c)(iii).

Maximum penalty: subsection (1)

820. The offences in subsections 40A(1) and 40B(1) carry a maximum penalty of 10 years' imprisonment, consistent with the maximum penalty applying to subsections 39(1), 39A(1) and 40(1) (as amended by this Schedule). The policy justification set out above in relation to sections 39, 39A and 40 therefore applies equally to subsections 40A(1) and 40B(1).

Exception – information or matter lawfully available: subsection (2)

821. Subsection (2) of each of sections 40A and 40B contains an identical exception to that in subsection (2) of sections 39, 39A and 40 (as amended by this Schedule) in relation to information or matter that has already been communicated or made available to the public with the authority of the Commonwealth. As such, the commentary set out above on the intended meaning of subsections 39(2), 39A(2) and 40(2) applies equally to subsections 40A(2) and 40B(2).

822. In particular, the exception does not apply to the unauthorised public communication or disclosure of information or matter, such as that in the nature of a 'leak'. Similarly, the exception does not apply to exculpate a person who makes an unauthorised communication of information or matter which is subsequently made public with the authority of the Commonwealth. This reflects the policy intent of the offence to ensure that persons who are entrusted with sensitive information are held to an appropriately high standard of conduct in relation to its use, handling and disclosure.

Item 18 – New offences – unauthorised dealing with records:

- New section 40C – ASIS
- New section 40E – AGO
- New section 40G – ASD
- New section 40J – ONA, and
- New section 49L – DIO

823. Item 18 inserts new offences in relation to the unauthorised dealing with records that were acquired by or prepared for by or on behalf of an IS Act agency in connection with its functions, or records which relate to the performance of an IS Act agency of its functions. These offences are based on the offence in subsection 18A(1) of the ASIO Act. The relevant

offences, which are drafted on an agency specific basis, are in subsection (1) of each of the new sections 40C, 40E, 40G, 40J and 40L.

824. As the elements of each agency specific offence are uniform, they are explained collectively below, together with a collective explanation of the uniform offence-specific defences and alternative verdict provisions applying to each agency specific offence.

Physical element 1 – dealing with a record: paragraph (1)(a)

825. Paragraph (1)(a) of each of the new sections 40C, 40E, 40G, 40J and 40L requires the prosecution to prove that the person engaged in a form of conduct specified in subparagraphs (1)(a)(i)-(v) (the 'relevant conduct'). That is, copying, transcribing, retaining, removing or dealing in any other manner with a record.

826. Subparagraphs (1)(a)(i)-(v) of new sections 40C, 40E, 40G, 40J and 40L are identical to those in subparagraphs 18A(1)(d)(i)-(v) of the ASIO Act as inserted by this Schedule to the Bill. Accordingly, these provisions are intended to have a uniform interpretation. The above commentary on the interpretation of subparagraphs 18(1)(d)(i)-(v) of the ASIO Act is intended to apply equally to subparagraphs (1)(a)(i)-(v) of each of sections 40C, 40E, 40G, 40J and 40L of the IS Act.

827. As paragraph (1)(a) of each of sections 40C, 40E, 40G, 40J and 40L is comprised of the physical element of conduct, the attendant fault element of intention applies by reason of subsection 5.6(1) of the Criminal Code. The prosecution must prove that the person means to engage in one of the forms of relevant conduct.

Physical element 2 – reason by which record was obtained by the person: paragraph (1)(b)

828. Paragraph (1)(b) of each of the new sections 40C, 40E, 40G, 40J and 40L requires the prosecution to prove that the record was obtained by the person by reason of one of the circumstances set out in subparagraphs (i)-(iii). These are that the person is, or was, a staff member or agent of the relevant agency, the person has entered into any contract, agreement or arrangement with the relevant agency or the person has been an employee or an agent of a person who has entered into a contract, agreement or arrangement with the relevant agency.

829. The terms 'contract', 'agreement' and 'arrangement' are intended to take the same meaning as they are used in all other offence provisions in new Division 1 of Part 6 of the IS Act, and in subsection 18(2) and sections 18A and 18B of the ASIO Act, as amended or inserted by this Schedule to the Bill. The above commentary accompanying these provisions applies equally to paragraph (1)(b) of the new sections 40C, 40E, 40G, 40J and 40L.

830. As the physical element in paragraph (1)(b) of the new sections 40C, 40E, 40G, 40J and 40L is that of a circumstance, the prosecution must prove that the person was reckless in relation to that circumstance by reason of subsection 5.6(2) of the Criminal Code. This means that the prosecution must prove that the person was aware of a substantial risk that he or she obtained the record by reason of one of the circumstances in subparagraphs (b)(i)-(iii), and that he or she nonetheless and unjustifiably in the circumstances took the risk of engaging in the relevant unauthorised conduct. The fault element of recklessness may also be satisfied by proof of a person's knowledge of the relevant circumstances. Hence, the prosecution may alternatively prove that the person was aware of one of the circumstances set out in subparagraphs (b)(i)-(iii).

Physical element 3 – connection of the record to the agency's functions: paragraph (1)(c)

831. Paragraph (1)(c) requires the prosecution to prove that the record was either: acquired or prepared by or on behalf of the relevant agency in connection with its functions or relates to the performance of the relevant agency of its functions.

832. The term 'acquired' is intended to take the same meaning as the term as used in the unauthorised communication of information offences in sections 39, 39A, 40, 40A and 40B of the IS Act, as amended or inserted by this Schedule to the Bill. In particular, it is intended to cover records that have come into the possession of the relevant agency by any means, whether or not the agency has made a request or has merely received the record without any action on that agency's part. This is consistent with the usage of the term 'acquired' elsewhere in the Commonwealth statute book, and the ordinary meaning of the term in respect of a record, being to come into a person's possession.

833. As the physical element in paragraph (1)(c) of the new sections 40C, 40E, 40G, 40J and 40L is that of a circumstance, the prosecution must prove that the person was reckless in relation to that circumstance (by reason of subsection 5.6(2) of the Criminal Code). Recklessness may be alternatively satisfied by proof of a person's knowledge.

Physical element 4 – relevant conduct was not authorised: paragraph (1)(d)

834. Paragraph (1)(d) of each of the new sections 40C, 40E, 40G, 40J and 40L requires the prosecution to prove that the relevant conduct under paragraph (1)(a) was not engaged in pursuant to one of the forms of authorisation in subparagraphs (1)(d)(i)-(iv). The forms of authorisation set out in subparagraphs (1)(d)(i)-(iv) are consistent with the forms of authorisation set out in subparagraphs (1)(c)(i)-(iv) of sections 39, 39A, 40A and 40B of the IS Act (as these provisions are amended or inserted by this Schedule to the Bill). As such, these provisions are intended to have a uniform meaning. The above commentary on the interpretation of the corresponding provisions in sections 39, 39, 39A, 40, 40A and 40B therefore applies equally to subparagraphs (1)(d)(i)-(iv) of new sections 40C, 40E, 40G, 40J and 40L.

835. As the physical element in paragraph (1)(d) of new sections 40C, 40E, 40G, 40J and 40L is a circumstance, the prosecution must prove that the person was reckless in relation to that circumstance (per subsection 5.6(2) of the Criminal Code). Recklessness may alternatively be satisfied by proof of a person's knowledge.

Maximum penalty

836. The offences in new subsection (1) of each of sections 40C, 40E, 40G, 40J and 40L carry a maximum penalty of three years' imprisonment. This is consistent with the maximum penalty applicable to the corresponding offence in new section 18A of the ASIO Act. It is also consistent with the maximum penalties applying to the new unauthorised recording offences in the IS Act (new sections 40D, 40F, 40G, 40K and 40M), and to the unauthorised recording offence in new section 18B of the ASIO Act.

837. The policy justification for a penalty of three years' imprisonment in relation to sections 40C, 40E, 40G, 40J and 40L is identical to that in relation to sections 18A and 18B of the ASIO Act as set out above. In particular, it is appropriate that the offences in

sections 40C, 40E, 40G, 40J and 40L apply a higher maximum penalty than other secrecy offences of general application due to the sensitive nature of the information placed at risk, which may jeopardise Australia's national security. This is consistent with a legitimate expectation that those persons who are entrusted with intelligence-related information are held to a high standard of conduct in relation to its use, handling and disclosure. The penalty also gives effect to Commonwealth criminal law policy that a heavier penalty is appropriate where the consequences of the offence are particularly dangerous or damaging. Criminal conduct which carries a significant risk of jeopardising Australia's national security, by placing at risk the confidentiality of intelligence-related information, is one such instance of particularly dangerous or damaging conduct. Consequently, while some Commonwealth secrecy offences of general application, such as that in section 70 of the Crimes Act, attract a maximum penalty of two years' imprisonment, it is appropriate that the offences in sections 40C, 40E, 40G, 40J and 40L of the IS Act attract a higher maximum penalty of three years' imprisonment.

Exception – record lawfully available – subsection (2)

838. Subsection (2) of each of sections 40C, 40E, 40G, 40J and 40L contains a similar exception to that in subsection (2) of sections 39, 39A, 40, 40A and 40B of the IS Act, and sections 18, 18A and 18B of the ASIO Act (as amended by this Schedule to the Bill). These exceptions apply to records that have already been communicated or made available to the public with the authority of the Commonwealth.

839. As such, the commentary set out above on the intended meaning of subsections 39(2), 39A(2), 40(2), 40A(2) and 40B(2) of the IS Act (and sections 18A and 18B of the ASIO Act) applies equally to subsections 40C(2), 40E(2), 40G(2), 40J(2) and 40L(2). In particular, as the note to subsection (2) confirms, a defendant bears an evidential burden in relation to the exception, by reason of subsection 13.3(3) of the Criminal Code. This means that the defendant must adduce or point to evidence suggesting a reasonable possibility of prior, authorised disclosure. The prosecution must then negate this matter to the legal standard.

840. The exception is limited to records that were already made lawfully available to the public at the time of the person's otherwise unauthorised dealing with a record. It does not apply to the disclosure of information previously released without authorisation (in the nature of 'leaks'). It further does not apply to exculpate persons who engage in an unauthorised dealing with a record which is subsequently communicated or made publicly available with the authority of the Commonwealth. This reflects the Government's legitimate expectation that persons to whom sensitive records are entrusted will handle those records in strict compliance with the scope of their authority at all times.

Alternative verdict provisions: subsections (3) and (4)

841. Subsections (3) and (4) of each of sections 40C, 40E, 40G, 40J and 40L contain alternative verdict provisions, consistent with those applying to sections 18A and 18B of the ASIO Act (as inserted by this Schedule to the Bill).

842. The effect of these provisions is that a person who is prosecuted for an unauthorised dealing offence under subsection (1) of sections 40C, 40E, 40G, 40J and 40L ('the prosecuted offence') may be convicted of an unauthorised recording offence under subsection (1) of sections 40D, 40F, 40H, 40K or 40M as applicable to the relevant agency

(the 'alternative offence'). This is provided that the trier of fact is not satisfied the person is guilty of the prosecuted offence, but is satisfied beyond reasonable doubt that the person is guilty of the applicable alternative offence to that agency, and the person has been accorded procedural fairness in relation to the finding of guilt on the alternative offence.

843. For example, the alternative verdict provisions may be engaged if a person is prosecuted for an unauthorised dealing offence said to be constituted by the unauthorised transcription of a record. The jury may not be satisfied that the person transcribed the record, but rather made a note of its contents after having accessed the record, based on his or her recollection of them. (Hence, the person created a new record of information, in contravention of the unauthorised recording offence provisions.) In this instance, provided that the trial judge is satisfied that the person has been accorded procedural fairness in relation to a finding of guilt on the unauthorised recording offence as applicable to the particular agency, it would be open to the jury to reach a verdict of guilty on the alternative offence.

844. The alternative verdict provisions in subsections (3) and (4) of each of sections 40C, 40E, 40G, 40J and 40L therefore enable an efficient and procedurally fair means of dealing with persons who engage in an unauthorised dealing with a record, which the trier of fact considers would satisfy the elements of an unauthorised recording of information offence. An alternative verdict provision is appropriate, given that the offences in Division 1 of Part 6 of the IS Act concerning the unauthorised recording of information or matters, and the unauthorised dealing with a record, carry an identical maximum penalty. Their respective elements are also similar because the offences are directed to closely related forms of wrongdoing.

Item 18 – New offences – recording of information or matter:

- New section 40D – ASIS
- New section 40F – AGO
- New section 40H – ASD
- New section 40K – ONA, and
- New section 40M – DIO.

845. Item 18 also inserts new offences in relation to the unauthorised recording of information or matter, which are based on the corresponding offence in section 18B of the ASIO Act. The relevant offences, which are drafted on an agency specific basis, are in subsection (1) of each of the new sections 40D, 40F, 40H, 40K and 40M.

846. As the elements of each agency specific offence are uniform, they are explained collectively below, together with a combined explanation of the uniform offence-specific defences and alternative verdict provisions applying to each agency specific offence.

Physical element 1 – making a record of any information or matter – paragraph (1)(a)

847. Paragraph (1)(a) of new sections 40D, 40F, 40H, 40K and 40M requires the prosecution to prove that the person has made a record of any information or matter. The fault element of intention applies to this element by reason of subsection 5.6(1) of the

Criminal Code. The term 'record' is defined in section 3 of the IS Act, as per amending item 6 of this Schedule to the Bill.

848. The making of a record may include, for example, the conduct of a person who hears a conversation or sees a written report in the course of his or her employment by the relevant agency, or in accordance with a contract, agreement or arrangement, and later writes down a note of the contents of the conversation or report based on his or her recollection.

Physical element 2 – reason by which the information or matter has come to the knowledge or into the possession of the person – paragraph (1)(b)

849. Paragraph (1)(b) of new sections 40D, 40F, 40H, 40K and 40M requires the prosecution to prove that the information or matter has come into the knowledge or into the possession of the person by reason of one of the circumstances in subparagraphs (i)-(iii). These are that the person is or has been a staff member of the relevant agency, the person has entered into any contract, agreement or arrangement with the relevant agency, or the person has been an employee or an agent of a person who has entered into a contract, agreement or arrangement with the relevant agency.

850. The terms 'contract', 'agreement' and 'arrangement' are intended to take a uniform throughout new Division 1 of Part 6 of the IS Act, and in subsection 18(2) and sections 18A and 18B of the ASIO Act. As such, the above commentary on amending items to the IS Act and the ASIO Act applies equally to paragraph (1)(b) of sections 40D, 40F, 40H, 40K and 40M.

851. As the physical element in paragraph (1)(b) is a circumstance, the prosecution must prove that the person was reckless as to the existence of one of the circumstances in subparagraphs (b)(i)-(iii), by reason of subsection 5.6(2) of the Criminal Code. The prosecution may alternatively prove that the person knew of one of these circumstances.

Physical element 3 – connection of information or matter to the agency's functions or performance of its functions: paragraph (1)(c)

852. Paragraph (1)(c) of new sections 40D, 40F, 40H, 40K and 40M requires the prosecution to prove that the information or matter was acquired or prepared by or on behalf of the relevant agency in connection with its functions, or relates to the performance by the agency of its functions. As this element is a circumstance, the fault element of recklessness applies pursuant to subsection 5.6(2) of the Criminal Code, which may alternatively be satisfied by proof of a person's knowledge as to the existence of the circumstance.

853. The terms 'acquired' and 'prepared' are intended to take a uniform meaning throughout new Division 1 of Part 6 of the IS Act and subsection 18(2) and sections 18A and 18B of the ASIO Act. In particular, the term 'acquired' is intended to include all information or matters that have come into the possession of the relevant agency, whether or not the agency requested them or received them without engaging in any kind of positive action.

Physical element 4 – unauthorised making of record: paragraph (1)(d)

854. Paragraph (1)(d) requires the prosecution to prove that the person made a record of the information or matter without one of the forms of authorisation under subparagraphs (d)(i)-(iv).

855. The matters in subparagraphs (d)(i)-(iv) are consistent with those in paragraph (1)(c) of sections 39, 39A, 40, 40A and 40B of the IS Act as amended or inserted by this Schedule to the Bill. Accordingly, the above commentary on the interpretation of subparagraphs (1)(c)(i)-(iv) of sections 40A and 40B applies equally to subparagraphs (1)(d)(i)-(iv) of sections 40D, 40F, 40H, 40K and 40M.

856. As the physical element in paragraph (1)(d) of sections 40D, 40F, 40H, 40K and 40M is a circumstance, the fault element of recklessness applies by reason of subsection 5.6(2) of the Criminal Code. Proof of recklessness can also be satisfied by proof of a person's knowledge of one of the circumstances in subparagraphs (1)(d)(i)-(iv) of sections 40D, 40F, 40H, 40K and 40M.

Maximum penalty

857. The offences in subsection (1) of each of sections 40D, 40F, 40H, 40K and 40M carry a maximum penalty of three years' imprisonment. This is consistent with the maximum penalty applying to the corresponding offence in section 18B of the ASIO Act.

858. The policy justification set out in relation to section 18B of the ASIO Act applies equally to these offences. In particular, it is appropriate that sections 40D, 40F, 40H, 40K and 40M attract a higher maximum penalty than other secrecy offences of general application due to the sensitive nature of the information placed at risk, which may jeopardise Australia's national security. This is consistent with a legitimate expectation that those persons who are entrusted with intelligence-related information are held to a high standard of conduct in relation to its use, handling and disclosure. The penalty also gives effect to Commonwealth criminal law policy that a heavier penalty is appropriate where the consequences of the offence are particularly dangerous or damaging. Criminal conduct which carries a significant risk of jeopardising Australia's national security, by placing at risk the confidentiality of intelligence-related information, is one such instance of particularly dangerous or damaging conduct. Consequently, while some Commonwealth secrecy offences of general application, such as that in section 70 of the Crimes Act, attract a maximum penalty of two years' imprisonment, it is appropriate that the offences in sections 40D, 40F, 40H, 40K and 40M of the IS Act attract a higher maximum penalty of three years' imprisonment.

Exception – information lawfully available: subsection (2)

859. Subsection (2) of each of sections 40D, 40F, 40H, 40K and 40M sets out an exception to the offences in subsection (1) of these sections. The exception provides that the offences do not apply to information or a matter that has been communicated or made available to the public with the authority of the Commonwealth.

860. These provisions are identical to the exceptions to the offences in subsection 18(2) and sections 18A and 18B of the ASIO Act. Accordingly, it is intended that subsection (2) of sections 40D, 40F, 40H, 40K and 40M is to be interpreted in identical terms to the

corresponding exceptions in the ASIO Act. In particular, the exceptions do not apply to unauthorised disclosures of information in the nature of 'leaks'. Similarly they do not apply to exculpate persons who make unauthorised recordings of information, where the relevant information is subsequently made publicly available with the authority of the Commonwealth.

861. Similarly, the policy justification set out above in relation to sections 18, 18A and 18B of the ASIO Act applies equally to sections 40D, 40F, 40H, 40K and 40M of the IS Act.

Alternative verdict provisions: subsections (3) and (4)

862. Subsections (3) and (4) of each of sections 40D, 40F, 40H, 40K and 40M set out alternative verdict provisions. They provide that a person who is prosecuted with an unauthorised recording offence under subsection (1) of sections 40D, 40F, 40H, 40K and 40M ('the prosecuted offence') may be convicted of an offence in respect of the unauthorised dealing with records ('the alternative offence' – being an offence against sections 40C, 40E, 40G, 40J and 49L, as applicable to the relevant agency). This is provided that the trier of fact is not satisfied that the person is guilty of the prosecuted offence, but is satisfied beyond reasonable doubt that the person is guilty of the alternative offence, and the person has been accorded procedural fairness in relation to the alternative offence.

863. For example, the alternative verdict provision in subsections 40D(3) and (4) will apply if a person is prosecuted for an offence against subsection 40D(1) (unauthorised recording of information or matter – ASIS), but the jury is not satisfied that the person is guilty of that offence, but is satisfied beyond reasonable doubt that the person is guilty of an offence against subsection 40C(1) (unauthorised dealing with records), it could find the person guilty of the latter offence provided that the trial judge is satisfied the person has been accorded procedural fairness in relation to the latter offence.

864. The use of an alternative verdict provision is consistent with the alternative verdict provisions in sections 40C, 40E, 40G, 40J and 49L of the IS Act, and the alternative verdict provisions in sections 18A and 18B of the ASIO Act. These provisions enable an efficient and procedurally fair means of dealing with persons who engage in unauthorised conduct in relation to information, which the trier of fact considers would satisfy the elements of an offence in respect of the unauthorised dealing with a record of that information.

865. An alternative verdict provision is appropriate given that the IS Act offences concerning the unauthorised recording of information or matter, and the unauthorised dealing with a record, carry an identical maximum penalty. Their elements are also similar because they are directed to closely related forms of wrongdoing.

Items 19-21 – General rules for new and amended offences

Items 19 and 20 – Technical amendments to subsections 41(1) and 41(2)

866. Items 19 and 20 make technical amendments to subsections 41(1) and (2) which are consequential to the amendments made by item 21, concerning geographical jurisdiction and the initiation of prosecutions in relation to offences against sections 39-40M.

867. Item 19 removes the numbering applying to subsection 41(1) (offence of publication of identity of staff). This amendment is consequential to the repeal of subsection 41(2) by

item 20 (prosecutorial consent requirement in relation to the subsection 41(1) offence). Item 20 is necessary because item 21 relocates the prosecutorial consent requirement in subsection 41(2) to new section 41A, and applies this requirement to all offences in Division 1 of Part 6 of the IS Act.

Item 21 – offences against Division 1 of Part 6 – general rules: section 41A

868. Item 21 inserts new section 41A. Subsections (1) and (2) make provision for the application of extended geographical jurisdiction to the offences in Part 6. Subsections 41A(3)-(5) further set out the requirements for obtaining the Attorney-General's consent to the commencement of prosecutions for an offence against Division 1 of Part 6. These provisions are consistent with those in section 18C of the ASIO Act.

Extended geographical jurisdiction - subsections 41A(1)-(2)

869. New subsection 41A(1) proves that the offences in Division 1 of Part 6 of the IS Act are subject to Category D extended geographical jurisdiction under section 15.4 of the Criminal Code. Subsection 41A(1) is identical to section 18C of the ASIO Act, which applies extended geographical jurisdiction to the offences in subsection 18(2) and sections 18A and 18B of that Act.

870. The application of Category D extended geographical jurisdiction means that the offences in new Division 1 of Part 6 of the IS Act apply whether or not the relevant conduct occurs in Australia, and whether or not the person alleged to have committed the offence is an Australian citizen, and whether or not there is an equivalent offence in the law of the local jurisdiction in which the conduct constituting the offence is said to have occurred.

871. Category D extended geographical jurisdiction is necessary to ensure the effective operation of the IS Act offences. These offences must necessarily apply to persons other than employees of the relevant IS Act agencies, into whose possession records have come, or into whose knowledge information has come, by reason of their status as staff members, or persons in a contract, agreement or arrangement with the relevant agency, or persons who are employees or agents of such persons. This may potentially include foreign officials or other persons who are based outside Australia. Given the risks to national security interests presented by any unauthorised dealing with intelligence information by any person to which such information has been entrusted, it is appropriate that flexibility is retained to bring such persons to justice, should they deal with records or information acquired or prepared by one of the relevant agencies in connection with its functions, or which relates to the performance by the agency of its functions, in a manner that contravenes the terms on which access was provided.

872. The commencement of a prosecution of a person other than an Australian citizen, in relation to conduct occurring wholly in a foreign country, is subject to the Attorney-General's consent under section 16.1 of the Criminal Code. This operates as a safeguard to ensure that such prosecutions are not commenced in inappropriate circumstances, having regard to public policy considerations in relation to international relations and national security. This consent requirement is additional to a general consent requirement applying to the offences in new Division 1 of Part 6 of the IS Act, whether or not they are prosecuted under extended geographical jurisdiction (new subsections 41A(3)-(5) refer).

873. Subsection 41A(2) confirms that the application of extended geographical jurisdiction under section 15.4 of the Code to the offences in Division 1 of Part 6 does not modify or otherwise affect the geographical jurisdiction applying to any other offence provision in the IS Act. This is necessary because some offences in the IS Act, which are located outside of new Division 1 of Part 6, were enacted prior to the commencement of Part 2.7 of the Criminal Code on 24 May 2001 and do not include a provision for the application of geographical jurisdiction under Part 2.7 of the Criminal Code. As such, the geographical jurisdiction applying to these offences is determined on an interpretation of individual offence provisions. Subsection 41A(2) is designed to ensure that subsection 41A(1) does not alter or otherwise modify the application of general principles of statutory interpretation to these pre-2001 offence provisions.

Initiation of prosecution – subsections 41A(3)-(5)

874. Subsections 41A(3)-(5) set out prosecutorial consent requirements in relation to the offences in Division 1 of Part 6. These consent requirements are identical to those in new section 18C of the ASIO Act, applying to the offences in subsection 18(2) and sections 18A and 18B of that Act. A prosecutorial consent requirement is an additional safeguard to the operation of the offences.

875. Subsection 41A(3) requires the prior consent of the Attorney-General (or a person acting under his or her direction) to the institution of a prosecution of an offence against Part 6. Subsection 41A(4) clarifies that such consent need not be obtained before a person charged with an offence against Part 6 is arrested, or a warrant is issued or executed. Such a person may also be remanded in custody or released on bail in the absence of the Attorney-General's consent to a prosecution. Subsection 41A(5) further clarifies that subsections (3) and (4) do not prevent an accused person from being discharged if proceedings are not continued within a reasonable time.

Item 22 – New Division 2 of Part 6 – Other matters

876. Item 22 creates a new Division 2 in Part 6 of the IS Act titled 'Other matters'. The rest of Part 6 will sit in Division 2.

Item 23 – Application of amendments

877. Item 23 contains application provisions in respect of the secrecy offences in new Division 1.

878. Item 23 provides that the offences in Division 1 are of prospective application. That is, the person must have engaged in the relevant unauthorised conduct (being the communication of information, dealing with a record, or making a record of information or a matter) after the amendments in Schedule 6 to this Bill have commenced. This is consistent with the established principle of Commonwealth criminal law policy that offences should not apply retrospectively.

879. The item further provides that the offences may apply to a person who has obtained a record, or who has obtained knowledge or possession of information or a matter, before or after the amendments in Schedule 6 have commenced. This reflects the fact that the culpable conduct targeted by the offences in new Division 1 is a person's unauthorised dealing with

records or information. As such, the time at which a person obtained, on an authorised basis, the relevant record, information or matter is not material to the application of the offence. Rather, the culpable conduct is the unauthorised communication or dealing with a record or information by a person who was entrusted with access to that record or information.

Part 2 – Consequential amendments

880. Part 2 of Schedule 6 to this Bill contains consequential amendments to provisions of other Commonwealth Acts which refer to the secrecy offences in the ASIO Act and the IS Act.

Australian Crime Commission Act 2002

Item 24 – Schedule 1

881. Item 24 amends Schedule 1 to the Australian Crime Commission Act 2002 (ACC Act) to include a reference to the offences in sections 18A and 18B of the ASIO Act, in addition to the existing reference to section 18.

882. Schedule 1 to the ACC Act is material to the offence provision in subsection 20(4) of that Act, which applies to persons who fail to comply with a notice to produce information to the ACC or a notice to appear at an ACC examination. This offence provision is subject to an exemption in relation to the existence of 'prescribed provisions' listed in Schedule 1 to the ACC Act that would prevent a person from complying with the notice. Schedule 1 lists as prescribed provisions the secrecy offences in sections 18, 81 and 92 of the ASIO Act. It is appropriate that the new offences in sections 18A and 18B of the ASIO Act are also identified as prescribed provisions because the ASIO Act makes provision for the sharing of information with other agencies, including law enforcement agencies. This includes the authorisation-related elements of the secrecy offences in subsections 18(2) and sections 18A and 18B of the ASIO Act and specific information-sharing provisions such as subsection 18(3) and sections 19 and 19A of the ASIO Act.

Crimes Act 1914

Item 25 – Subsection 15LC(4), note 2

883. Item 24 amends the offence specific defence in subsection 15LC(4) of the Crimes Act, which provides for an exception to the offences in subsections 15LC(1)-(3), concerning the disclosure of information about an assumed identity. Note 2 to subsection 15LC(4) clarifies the relationship between the offence-specific defence in subsection 15LC(4) and potential liability under the secrecy offences in another Act. Note 2 refers to subsections 39 and 41 of the IS Act as examples of offences which may potentially be open even if subsection 15LC(4) applies.

884. Item 25 amends note 2 to subsection 15LC(4) to include a reference to all of the offences in new Division 1 of Part 6 of the IS Act. This will provide guidance on the existence of other secrecy offences to which a person may be liable even if subsection 15LC(4) of the Crimes Act is exculpatory in relation to the offences in subsections 15LC(1)-(3) of that Act.

Privacy Act 1988

Items 26 and 27 – Subsection 80P(7) (paragraphs (a) and (c) of the definition of *designated secrecy provision*)

885. Items 26 and 27 amend the definition of a 'designated secrecy provision' in subsections 80P(7)(a) and (c) of the Privacy Act 1988 (Privacy Act) to include references to the new and amended offences in the ASIO Act and the IS Act as inserted by this Bill. That is, sections 18, 18A and 18B of the ASIO Act, and sections 39-40M of the IS Act. Items 26 and 27 update the existing references in paragraph 80P(7)(a) to the offences in sections 18 and 92 of the ASIO Act, and the references in paragraph 80P(7)(c) to the offences in sections 39-41 of the IS Act.

886. Items 26 and 27 mean that all of the secrecy offences in subsection 18(2) and sections 18A and 18B of the ASIO Act and in Division 1 of Part 6 of the IS Act are 'designated secrecy provisions' for the purpose of Part VIA of the Privacy Act, which governs the handling of personal information in declared emergencies or disasters. Accordingly, the secrecy offences in the ASIO Act and the IS Act are excluded from the general immunity from liability in subsection 80P(2) of the Privacy Act. Subsection 80P(2) provides that persons who disclose personal information in accordance with subsection 80P(1) (authorised collection, use and disclosure of personal information when an emergency declaration is in force in relation to an emergency or disaster) are immune from liability under a secrecy provision, other than a designated secrecy provision as defined in subsection 80P(7).

887. It is appropriate that the secrecy offences in the ASIO Act and the IS Act are carved out of the general immunity in subsection 80P(2) of the Privacy Act, because the ASIO Act and the IS Act already make adequate provision for the disclosure of information in these circumstances. In particular, the secrecy offences in the ASIO Act and the IS Act do not apply if a person has authorisation or approval from the relevant agency head (or another authorised person) to communicate information or deal with a record. Hence, it is open to an agency head to authorise or approve the communication of information for the purpose of Part VIA of the Privacy Act (including any dealings with records or information in preparation for the communication of information). In addition, subsection 18(4B) of the ASIO Act makes express provision for the communication of information under Part VIA of the Privacy Act.

888. It is further appropriate that the secrecy offences in the ASIO Act and the IS Act apply to persons who communicate information or engage in an unauthorised dealing with a record for the intended purpose of Part VIA of the Privacy Act, but who do not have the relevant agency's authorisation or approval to do so. Such conduct is properly regarded as culpable because the unauthorised nature of the disclosure of information or dealing with a record places it at risk, irrespective of the person's motivation for engaging in that conduct.

Schedule 7—Renaming of Defence agencies

Overview of measures

889. Defence makes an important contribution to Australia's broader national security arrangements and co-operation with other Commonwealth Departments and agencies will intensify over the next five years as new whole-of-government arrangements in areas such as cyber security and national security science and innovation are institutionalised.

890. Defence will play a key leadership role in these arrangements. This will better reflect the contribution of Defence to Australia's broader national security.

891. As part of these arrangements, the Defence Imagery and Geospatial Organisation (DIGO) is to be renamed the Australian Geospatial-Intelligence Organisation (AGO) and the Defence Signals Directorate (DSD) is to be renamed the Australian Signals Directorate (ASD) to better reflect the national roles that those organisations play in support of Australia's security.

Part 1 – Main Amendments

Intelligence Services Act 2001

892. Items 1 to 57 amend the *Intelligence Services Act 2001* (IS Act) to replace all references to DIGO and DSD with AGO and ASD, respectively.

Part 2 – Consequential amendments

893. Part 2 makes consequential amendments to other legislation to replace all references to DIGO and DSD with AGO and ASD respectively.

894. Items 58 to 63 and 65 to 143 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*, and

(l) *Public Interest Disclosure Act 2013*.

895. Item 64 provides for a minor correction to section 5 (definition of 'DIO') of the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006*. This item omits the 'Department of Defence' and substitutes the 'Defence Department'. This is a minor correction for consistency with the definitions. The term 'Defence Department' and not the 'Department of Defence' is defined in the Act.

896. Item 134 amends subsection 35(2B) of the *Inspector-General of Intelligence and Security Act 1986* to provide that the Inspector-General of Intelligence and Security (IGIS) can annually report on the extent of compliance by ASIS, ASD and AGO with rules made under section 15 of the IS Act. Currently the IGIS does not have a specific reporting function on AGO but reports on their compliance so this amendment will streamline the legislation to reflect current practice.

Part 3 – Transitional provisions

897. Part 3 establishes transitional arrangements for Schedule 7 to the Bill.

Item 144 – Transitional—subsection 25B(1) of the *Acts Interpretation Act 1901*

898. Item 144 provides that section 25B(1) of the Acts Interpretation Act 1901 (Acts Interpretation Act) applies to the renaming of DIGO and DSD to AGO and ASD, respectively, as if DIGO and DSD were bodies. This subsection provides that where a body alters its name, that body continues in existence under the new name so that its identity is not affected. This will ensure that any exemptions that currently apply DIGO and to DSD will continue to apply to those organisations when they are renamed to AGO and ASD, respectively.

899. Without limiting the generality of the application of subsection 25B(1) of the Acts Interpretation Act, item 144 will specifically ensure that the extant Ministerial directions under section 8, Ministerial authorisations under section 9, Inspector-General of Intelligence and Security certificates under section 14, rules to protect the privacy of Australians under section 15 and offence provisions under sections 39A and 40 of the IS Act will continue in effect if the draft Bill is enacted and commences. It will also ensure that the exemptions from the operation of the *Freedom of Information Act 1982* and the *Privacy Act 1988* that both DIGO and DSD have will continue to apply in relation to documents that originated with or were received from those agencies. In addition, it will ensure that any inquiries under the *Inspector-General of Intelligence and Security Act 1986* that were commenced prior to the Bill being enacted and taking effect remain valid.

Item 145 – Transitional rules

900. This item provides for the Minister, by legislative instrument, to make rules in relation to transitional matters arising out of the amendments and repeals made by Parts 1 and 2. This item provides a mechanism to deal with any unforseen transitional matters that item 144 does not address.