Australian Government
Department of Home Affairs

Department of Home Affairs submission to the review of the National Security Legislation Amendment (Comprehensive Review and Other Measures No. 1) Bill 2021

Parliamentary Joint Committee on Intelligence and Security

25 January 2022

Table of Contents

List of Abbreviations

Term	Meaning
ADF	Australian Defence Force
AGO	Australian Geospatial-Intelligence Organisation
AHO	Australian Hydrographic Office
ASD	Australian Signals Directorate
ASIO	Australian Security Intelligence Organisation
ASIO Act	*Australian Security Intelligence Organisation Act 1979*
ASIO Minister	Minister responsible for administering the *Australian Security Intelligence Organisation Act 1979*
ASIS	Australian Secret Intelligence Service
The Bill	National Security Legislation Amendment (Comprehensive Review and Other Measures No. 1) Bill 2021
The Committee	Parliamentary Joint Committee on Intelligence and Security
Comprehensive Review	*Comprehensive Review of the Legal Framework of the National Intelligence Community*
Crimes Act	*Crimes Act 1914*
Criminal Code	*Criminal Code Act 1995*
The Department	Department of Home Affairs
DIO	Defence Intelligence Organisation
Foreign Passports Act	*Foreign Passports (Law Enforcement and Security) Act 2005*
Hope Royal Commissions	*1974-77 Royal Commission on Intelligence and Security & 1983 Royal Commission on Australia's Security and Intelligence Agencies*
IGIS	Inspector-General of Intelligence and Security
IGIS Act	*Inspector-General of Intelligence and Security Act 1986*
Independent Intelligence Review	*2017 Independent Intelligence Review*
IS Act	*Intelligence Services Act 2001*
IS Act agencies	Australian Secret Intelligence Service, Australian Signals Directorate and Australian Geospatial-Intelligence Organisation

Term	Meaning
NIC	National Intelligence Community
ONI	Office of National Intelligence
ONI Act	*Office of National Intelligence Act 2018*
Passports Act	*Australian Passports Act 2005*
Privacy Act	*Privacy Act 1988*
TIA Act	*Telecommunications (Interception and Access) Act 1979*

1. Introduction

1. The Department of Home Affairs (the **Department**) welcomes the opportunity to make this submission to the Parliamentary Joint Committee on Intelligence and Security's (the **Committee**) review of the National Security Legislation Amendment (Comprehensive Review and Other Measures No. 1) Bill 2021 (the **Bill**).

2. The Bill implements the Government's response to a number of recommendations made by the *Comprehensive Review of the Legal Framework of the National Intelligence Community* (**Comprehensive Review**) led by Mr Dennis Richardson AC. The Bill also implements recommendations made by the *2017 Independent Intelligence Review* led by Mr Michael L'Estrange AO and Mr Stephen Merchant PSM (**Independent Intelligence Review**), and addresses other pressing operational issues facing Australia's intelligence agencies.

3. The Bill ensures that the legal framework of the National Intelligence Community (**NIC**) keeps pace with an increasingly complex operational environment. The Bill introduces narrow, targeted reforms to the powers and oversight of Australia's intelligence agencies to address critical operational challenges they now face.

4. Through 14 schedules of amendments, the Bill improves the workability of the ministerial authorisation framework, strengthens intelligence agencies' cooperation arrangements, enhances and supports existing intelligence agency powers, and improves the transparency of agencies' privacy protections for Australians.

5. The Bill does not grant Australia's foreign intelligence agencies new powers to produce intelligence on Australians that would otherwise be unlawful without a warrant.[1]

6. As noted by the Comprehensive Review, Australia's intelligence agencies are highly professional and work hard to protect Australia and Australians and advance the national interest. The measures in the Bill will assist agencies to continue to carry out this important work.

7. Alongside the measures in the Bill, Australia's intelligence agencies remain subject to a range of strict safeguards, independent oversight, and transparency and accountability mechanisms under Australian law.

8. This includes high thresholds to authorise the use of powers, and robust oversight arrangements, including by the Inspector-General of Intelligence and Security (**IGIS**). The role of the IGIS is an important and unique oversight mechanism for intelligence agency activities. The IGIS has significant powers akin to a Royal Commission and is able to inquire into the legality and propriety of intelligence agency activities, as well as agency compliance with ministerial guidelines, directives and internal policies.

[1] A news article inaccurately reported that the Bill would enable the Australian Signals Directorate to undertake signals intelligence collecting on people in Australia without a warrant if there is an imminent risk to life, or in respect of domestic terrorist suspects: Sarah Basford Canales, *Domestic spying for ASD a possibility*, Friday 26 November 2021, The Canberra Times.
The Department published a statement on its website correcting these inaccuracies: https://www.homeaffairs.gov.au/news-media/on-the-record.

2. Background

9. On 18 July 2017, the then Prime Minister, the Hon Malcolm Turnbull MP, released the findings of the Independent Intelligence Review. The Independent Intelligence Review examined the intelligence community environment, the current structural, legislative and oversight mechanisms, and how effectively they serve Australia's interests. A central theme of the Review was to provide a pathway to take those areas of individual agency excellence to a higher level of collective performance through strengthening integration across Australia's national intelligence enterprise. The Review concluded that progress towards this objective required changes to the co-ordinating structures of the NIC, new funding mechanisms to address capability gaps, and the streamlining of legislative arrangements. The review made a series of recommendations, including that a comprehensive review should be undertaken into the legislation governing Australia's intelligence community.

10. On 30 May 2018, the then Attorney-General, the Hon Christian Porter MP, announced that the Government had commissioned a comprehensive review of the legal framework governing the NIC to be undertaken by Mr Dennis Richardson AC. As a consequence of this decision, it was appropriate to defer the implementation of some recommendations of the Independent Intelligence Review until the findings of the Comprehensive Review were clear.

11. On 4 December 2020, the then Attorney-General released the unclassified report of the Comprehensive Review and the Government response. The Comprehensive Review was the most significant review of intelligence legislation since the Royal Commissions of the 1970s and 1980s led by Justice Robert Hope AC CMG QC (the **Hope Royal Commissions**).The Comprehensive Review comprehensively examined the effectiveness of the legislative framework governing the NIC and found that, on the whole, the legal framework governing Australia's intelligence agencies is based on sound principles and has been well-maintained. However, the Comprehensive Review recognised the need for some targeted reforms to the legislation governing the NIC, in addition to the key recommendations to undertake wholesale reform of Australia's electronic surveillance laws. These targeted reforms are necessary to ensure our intelligence agencies can undertake their functions effectively and keep Australians safe.

12. The Bill implements the Government response to 13 Comprehensive Review recommendations, including four measures recommended by both the Comprehensive Review and the Independent Intelligence Review. The Bill also makes amendments that were not considered by either review, but which nonetheless address pressing operational issues facing Australia's intelligence agencies.

3. The Bill

3.1. Schedule Summary

13. The Bill contains the following 14 Schedules. A summary of the Schedules including which Comprehensive Review and Independent Intelligence Review recommendations each is implementing is at **Annexure A**.

- **Schedule 1** - enables the Australian Security Intelligence Service (**ASIS**), Australian Signals Directorate (**ASD**) and Australian Geospatial-Intelligence Organisation (**AGO**) to immediately undertake activities to produce intelligence on an Australian person without ministerial authorisation offshore where there is, or is likely to be, an imminent risk to the safety of an Australian person, and the Australian person would be likely to consent to the intelligence being collected, if they were able to do so.

- **Schedule 2** - enables ASIS, ASD and AGO to seek ministerial authorisation to produce intelligence on a class of Australian persons who are, or are likely to be, involved with a listed terrorist organisation.
- **Schedule 3** - enables ASD and AGO to seek ministerial authorisation to undertake activities to produce intelligence on one or more members of a class of Australian persons when the agencies are operating in the course of providing assistance to the Australian Defence Force (**ADF**) in support of military operations or intelligence matters.
- **Schedule 4** - inserts new provisions which:
    - clarify the requirement for ASIS, ASD and AGO to obtain ministerial authorisation to produce intelligence on an Australian person to circumstances where the agencies seek to use covert and intrusive methods, which include methods for which the Australian Security Intelligence Organisation (**ASIO**) would require a warrant to conduct inside Australia.
    - make explicit the long-standing requirement for ASIS, ASD and AGO to seek ministerial authorisation before requesting a foreign partner agency to produce intelligence on an Australian person.
- **Schedule 5** - enables ASIS to undertake less intrusive activities to produce intelligence on Australians inside Australia where ASIO has requested that assistance for the purposes of ASIO's functions.
- **Schedule 6** - enables AGO to cooperate with an authority of another country without ministerial approval where the cooperation is in regards to its non-intelligence functions.
- **Schedule 7** - requires the Office of National Intelligence (**ONI**) to seek the Director-General of ONI's approval in order to cooperate with public international organisations.
- **Schedule 8** - extends the period for which travel documents may be suspended or temporarily surrendered from 14 to 28 days, to allow sufficient time for ASIO to undertake all appropriate investigative activities to inform a security assessment.
- **Schedule 9** - extends the immunity provisions for ASIS and AGO for certain computer offences, where a staff member or agent acted on a reasonable belief that the computer-related activities occurred outside Australia.
- **Schedule 10** - requires the Defence Intelligence Organisation (**DIO**) to have legally binding privacy rules, requires ASIS, ASD, AGO and DIO to make their privacy rules publicly available, and updates ONI's privacy rules provisions so that they apply to intelligence about an Australian person under ONI's analytical functions.
- **Schedule 11** - includes ASD in the Assumed Identities regime in Part IAC of the *Crimes Act 1914* to allow ASD officers to operate assumed identities.
- **Schedule 12** - clarifies the meaning of an authority of another country in the *Intelligence Services Act 2001*.
- **Schedule 13** - permits the Director-General of Security to authorise a class of persons to exercise authority under an ASIO warrant in the *Telecommunications (Interception and Access) Act 1979*, clarifies the permissible scope of classes under section 12 of that Act and under section 24 of the *Australian Security Intelligence Organisation Act 1979*, and introduces additional record-keeping requirements regarding persons exercising authority under all ASIO warrants.
- **Schedule 14** - makes technical amendments to correct a referencing error and a minor omission in the *Intelligence Services Amendment (Establishment of the Australian Signals Directorate) Act 2018* to ensure that there is an appropriate time limit on all ministerial authorisations issued under section 9 of the IS Act.

14. The Bill amends the:

- *Intelligence Services Act 2001* (**IS Act**)
- *Criminal Code Act 1995* (**Criminal Code**)
- *Crimes Act 1914* (**Crimes Act**)
- *Australian Passports Act 2005* (**Passports Act**)
- *Foreign Passports (Law Enforcement and Security) Act 2005* (**Foreign Passports Act**)
- *Office of National Intelligence Act 2018* (**ONI Act**)
- *Inspector-General of Intelligence and Security Act 1986* (**IGIS Act**)
- *Australian Security Intelligence Organisation Act 1979* (**ASIO Act**), and
- *Telecommunications (Interception and Access) Act 1979* (**TIA Act**).

3.2. Schedule 1 – Emergency authorisations

15. Under existing law, ASIS, ASD and AGO (**IS Act agencies**) must obtain a ministerial authorisation to produce intelligence on an Australian citizen or permanent resident. This is an important safeguard to protect the privacy of Australians. In an emergency, these agencies may obtain an oral authorisation from a relevant Minister (section 9A of the IS Act), or in situations where a relevant Minister is not available, an authorisation may be given by the relevant agency head (section 9B of the IS Act).

16. There is currently no scope for agencies to act outside these processes, even to address situations of an Australian person at imminent risk of harm overseas, where it is reasonable to expect that the Australian would consent to action being taken.

17. Schedule 1 amends the IS Act to permit the agency head of an IS Act agency to authorise the production of intelligence on an Australian person, without first obtaining ministerial authorisation, in circumstances where there is an imminent risk to the person's safety *outside Australia*. The agency head may delegate this ability to other staff members in the IS Act agency.

18. This only applies in the very narrow situation where it is reasonable to believe that the person would consent to the IS Act agencies taking the action.

19. This means that in these very limited circumstances, the agency can take swift action in situations of imminent risk to an Australian person's safety overseas, such as a kidnapping or hostage situation, without first undertaking a ministerial authorisation process.

20. In emergency circumstances, time is of the essence. The ministerial authorisation process, including the existing emergency authorisation provisions, can constitute a significant delay. Operational experience has demonstrated that the current emergency authorisation provisions in sections 9A and 9B do not support expeditious action by the relevant agencies where an Australian person's life may depend on immediate action.

21. According to the Independent Intelligence Review, currently 'the emergency authorisation provisions can be an unnecessary delay' in situations that pose a threat to the safety of Australians.[2] The Comprehensive Review agreed with the Independent Intelligence Review, noting that 'hostage situations are readily distinguishable from the vast majority of emergency authorisations…, in that they are situations where it is reasonable to believe a person would consent to the IS Act agency producing intelligence on them'.[3] The Comprehensive Review supported the Independent Intelligence Review recommendation to amend the IS Act to 'permit IS Act agencies to act immediately and without a ministerial authorisation in situations where it is reasonable to believe that an Australian person consents to the IS Act agency producing intelligence on that person'.[4] These amendments implement recommendation 52 in the Comprehensive Review, and recommendation 16(e) of the Independent Intelligence Review.

22. Our foreign intelligence agencies are often best placed to assist in efforts to protect Australians overseas. However, in circumstances where an Australian has been kidnapped overseas, our foreign intelligence agencies will be required to act quickly to assist in producing intelligence to locate them. The delays involved in obtaining ministerial authorisations, even emergency authorisations, can hinder agencies' abilities to respond as quickly as they otherwise may be able to. Any unnecessary delay – even a matter of minutes – can mean a missed opportunity to respond effectively.

23. In an emergency, enabling the swift production of intelligence on an Australian person would have the real possibility of mitigating the risk of harm as the immediate collection of intelligence may 'help identify where a person may be, who may have kidnapped them and what intermediaries may be involved'.[5]

24. The authorisation in this Schedule is for the protection and benefit of individual Australians and can only be used in very narrow circumstances – to collect intelligence on an Australian who is at imminent risk of harm overseas, and where that Australian is likely to want, and indeed expect, the Government to take every action to assist them.

25. There has been a suggestion that the Bill would enable ASD to undertake signals intelligence collection on people in Australia without a warrant if there is an imminent risk to life, or in respect of domestic terrorist suspects.[6] This is not correct. The new emergency authorisation only operates in relation to an Australian person outside Australia.[7]

26. The Bill amends the IS Act to introduce section 9D. This new section permits IS Act agency heads (or their delegate/s) to authorise the production of intelligence on an Australian person, without first obtaining authorisation from a Minister.

Issuing of a section 9D emergency authorisation

27. In order to issue an emergency authorisation, the head of the relevant agency (or their delegate) must be satisfied that:

- there is, or is likely to be, an imminent risk to the safety of an Australian person who is outside Australia, and
- it is necessary or desirable to undertake an activity/ies for the specific purpose/s of producing intelligence on the persons, and
- it is not reasonably practicable to obtain the person's consent to the agency producing that intelligence, and

[2] Commonwealth of Australia, Department of the Prime Minister and Cabinet, *2017 Independent Intelligence Review*, paragraph 6.45.
[3] *Comprehensive Review of the Legal Framework of the National Intelligence Community by Mr Dennis Richardson*, Volume 2, paragraph 21.51.
[4] Ibid, paragraph 21.52.
[5] Ibid, paragraph 21.49.
[6] Sarah Basford Canales, *Domestic spying for ASD a possibility*, Friday 26 November 2021, The Canberra Times.
[7] Proposed new paragraph 9D(1)(a); see item 2 of Schedule 1 to the Bill.

- having regard to the nature and the gravity of the risk, it is reasonable to believe that the person would consent to the agency producing that intelligence if the person were able to do so.

28. The section 9D emergency authorisation can only be issued where there is an *imminent* risk to the Australian person's safety and it is not reasonably practicable to obtain their consent to the production of that intelligence, but it is reasonable to believe that the person would consent if they were able to do so (subsection 9D(1)).

29. Imminent risk in this instance is to be given its natural meaning, which is something that is 'about to happen'. Imminent risk therefore relates to something that is about to happen that would put an Australian's life at risk or cause them harm. Such a situation could arise in situations where, for example, an Australian person was kidnapped or involved in a hostage situation, or an ongoing terrorist or mass casualty attack.

30. Consistent with the existing ministerial authorisation framework, the agency head may authorise the production of intelligence on an Australian person only if they are satisfied that the facts would justify the responsible Minister giving an authorisation under section 9, and that the responsible Minister would have given the authorisation. The authorisation is subject to any conditions specified by the agency head.

Notification, cancellation and duration

31. Once a section 9D authorisation has been issued, the agency head must, as soon as practicable (but no longer than eight hours after), notify the responsible Minister orally or in writing of the authorisation. This provides the responsible Minister with notification, as early as possible, of the fact that an authorisation has been issued to produce intelligence on an Australian overseas who is at imminent risk of harm.

32. As soon as practicable after the authorisation has been issued (and no longer than 48 hours after), the agency head must provide the responsible Minister with a copy of the authorisation, a written summary of the facts of the case that led to the agency head being satisfied they were justified in giving the authorisation, and an explanation of the Minister's obligations in considering the authorisation (paragraph 9D(5)(c)). If the Australian person is likely to be involved in an activity/ies that are prejudicial to security, the Attorney-General and the Minister responsible for administering the ASIO Act (**ASIO Minister**), must also be provided with a copy of the authorisation and summary of the facts.

33. As soon as practicable after being given these documents, the responsible Minister must consider whether to cancel the authorisation (subsection 9D(6)). The responsible Minister may take into account any advice given by the Attorney-General. The timeframes for alerting the responsible Minister to the authorisation, providing the Minister with the appropriate documentation, and an opportunity to cancel the authorisation ensures that Ministers will continue to have clear visibility of and decision-making power over the actions of Australia's foreign intelligence agencies as they concern Australian persons.

34. The responsible Minister may choose to cancel the authorisation at this point or at any point throughout the duration of the authorisation. Once cancelled, the Minister must, as soon as practicable, provide written notice to the IGIS, and, if relevant, the Attorney-General and ASIO Minister.

35. As soon as practicable after the authorisation has been issued (and no longer than 48 hours after), the agency head must also provide the IGIS with a copy of the authorisation and summary of the facts. Within 30 days of the provision of these documents, the IGIS must consider whether the agency head complied with the requirements in section 9D, provide the responsible Minister with a report on the IGIS' views of the extent of that compliance, and provide a copy of the conclusions of the report to the Committee. These provisions ensure timely oversight of the actions of the agency head in making a section 9D authorisation.

36. Further to the Minister's ability to cancel a section 9D emergency authorisation, the agency head must cancel the authorisation if they are satisfied that there is not, and not likely to be, a significant risk to the safety of the Australian person (subsection 9D(12)).

37. The different threshold for the issuing ('imminent') versus the cancelling ('significant') of a section 9D emergency authorisation reflects the importance of continuing to gather intelligence while the risk remains significant, even if the immediacy has passed.

38. For example, where an Australian person has been taken hostage overseas, the agency head may be satisfied that there is an imminent risk to the safety of that person and issue an emergency authorisation. Should a ransom demand be received, the risk to the person's safety may no longer be imminent while the request remains outstanding. Despite this, the risk may remain significant, and it is entirely possible for the risk to become imminent again at any moment. In such a case, allowing the agency to continue to produce intelligence on the Australian person maximises the Australian Government's ability to ensure the person's safety.

39. If the agency head cancels the authorisation under subsection 9D(12) they must, as soon as practicable, provide written notice to the responsible Minister, IGIS, and if relevant the Attorney-General and the ASIO Minister.

40. The maximum duration of a section 9D emergency authorisation is 6 months. This is because, if the Minister has considered the emergency authorisation and determined *not* to cancel it, the authorisation should have the same effect as if the Minister had made the authorisation personally. This timeframe is therefore consistent with the duration of ministerial authorisations under the existing ministerial authorisation framework.

41. The 6 month duration also reflects the fact that although the risk may be imminent at the time the authorisation is given, it does not automatically follow that the risk will only last a short amount of time. There may be situations where it is necessary that intelligence continue to be produced on the Australian because the risk of harm is still significant, even if it is no longer imminent. So while the duration is consistent with the current framework and provides the necessary flexibility required in such serious circumstances, the cancellation provisions ensure that authorisations do not continue longer than necessary.

42. In the same hostage example as above, should a ransom demand be received, it would be appropriate for the agency to continue to produce intelligence on the Australian person throughout the chain of events, to maximise the ability of the Australian Government to ensure the person's safety.

Delegation provisions

43. As part of section 9D, the agency head may, in writing, delegate to an agency staff member (other than a consultant or contractor) any or all of the powers, functions or duties of the agency head under section 9D (subsection 9D(14)).

44. The requirement that the power be expressly delegated, rather than conferred automatically on all agency staff, ensures that this exceptional power will be exercised only in appropriate circumstances, and by IS Act agency staff members who, in the opinion of the agency head, possess the necessary skills and training to make time critical judgments about the production of intelligence.

45. There is a strong operational need for this power to be devolved. Overseas staff operate in different time zones, with differing levels of seniority, and contacting the agency head for approval could cause undue delay and result in lost opportunities to prevent or lessen harm or risk to an Australian person's safety.

46. Staff members will be required to comply with any written directions given by the agency head when exercising a power, performing a function or discharging a duty under the delegation (subsection 9D(15)).

Accountability measures

47. All of the safeguards applying to activities subject to a ministerial authorisation under the IS Act will apply to activities undertaken under the new section 9D emergency authorisation.

48. As discussed above, section 9D introduces a range of new accountability measures including timely notification to the relevant Minister/s and the IGIS, cancellation provisions for both the responsible Minister and the agency head, and timely compliance reporting by the IGIS to both the responsible Minister and the Committee.

3.3. Schedule 2 – Authorisations relating to counter-terrorism

49. Under existing law, an IS Act agency must obtain a ministerial authorisation to produce intelligence on an Australian person. Each agency must obtain an individual ministerial authorisation for each separate Australian on whom it seeks to produce intelligence.[8]

50. Schedule 2 amends the ministerial authorisation regime in the IS Act by introducing a counter-terrorism class authorisation to allow IS Act agencies to expeditiously produce intelligence on Australians who are, or are likely to be, involved with proscribed terrorist groups. This measure will better protect Australians by enabling IS Act agencies to operate with greater agility in producing intelligence on Australians involved with a listed terrorist organisation.

51. The Independent Intelligence Review said that it is 'important to give Ministers greater flexibility to issue ministerial authorisations that cover a class of Australians whose involvement with terrorist organisations proscribed by the Attorney-General under the [Criminal Code] constitutes a threat to national security. The use of class authorisations would allow the IS Act agencies to respond quickly to developing threats from previously unidentified individuals'.[9] It considered that the 'existing provisions of the IS Act do not meet contemporary needs given both the seriousness of the threat and the number of Australians with connections to international terrorist groups'.[10]

52. The Comprehensive Review considered that 'the intention of the recommendation [of the Independent Intelligence Review] was to give ministers greater flexibility to issue ministerial authorisations covering a class of Australians whose involvement with terrorist organisations proscribed under the Criminal Code constituted a threat to national security'.[11] The Independent Intelligence Review envisaged that the class would include both official members of a proscribed terrorist organisation as well as those involved with such an organisation.[12] It provided that 'limiting the class to listed terrorist organisations would help to ensure that the class is tightly defined'.[13]

53. These amendments implement recommendation 45 of the Comprehensive Review and recommendation 16(a) of the Independent Intelligence Review.

54. The Schedule amends the existing ministerial authorisation framework to introduce a counter-terrorism class authorisation for the production of intelligence on Australians who are, or are likely to be, involved with listed terrorist organisations. For the purpose of the authorisation, listed terrorist organisation will have the same meaning as the definition of 'listed terrorist organisation' in subsection 100.1(1) of the Criminal Code. That is, an organisation that is specified by the regulations for the purposes of paragraph (b) of the definition of terrorist organisation in section 102.1 of the Criminal Code.

[8] The only existing exception to requiring individual authorisations is that the Minister for Foreign Affairs can authorise ASIS to produce intelligence on a class of Australians to assist the ADF in military operations (see Section 3.4 –Schedule 3 for more detail).
[9] *2017 Independent Intelligence Review*, paragraph 6.31.
[10] Ibid, paragraph 6.30.
[11] *Comprehensive Review of the Legal Framework of the National Intelligence Community by Mr Dennis Richardson*, Volume 2, paragraph 20.47.
[12] Ibid, paragraph 20.47.
[13] Ibid, paragraph 20.50.

55. In addition to the existing preconditions set out in subsections 9(1) and 9(1A), a Minister must be satisfied that a class of Australian persons is, or is likely to be, 'involved with' a listed terrorist organisation and obtain the Attorney-General's agreement before issuing this type of class authorisation (subsection 9(1AAA)).

56. New subsection 9(1AAB) provides a non-exhaustive list of activities which amount to being 'involved' with a terrorist organisation. Involvement with a listed terrorist organisation includes directing or participating in the activities of the organisation; recruiting a person to join, or participate in the activities of, the organisation; providing, receiving or participating in training to, with or from the organisation; being a member of the organisation; providing financial or other support to the organisation; or advocating for, or on behalf of, the organisation. The concept of 'support' does not capture mere sympathy for the general aims or ideology of an organisation. Some examples of activities that would be captured under the concept of providing 'support' include logistical support, or the provisions of weapons to the organisation.

57. Schedule 2 also introduces record keeping requirements which apply to all class authorisations in the IS Act (section 10AA). Each IS Act agency head must ensure that a list is kept which identifies each Australian person in relation to whom the agency intends to undertake activities under a class authorisation, explains why the agency believes the person is a member of the relevant class, and includes any other information the agency head considers appropriate (subsection 10AA(2)). The agency head must ensure that the list is available for inspection by the IGIS. This list of all persons on whom intelligence has been produced under a class authorisation was recommended by the Comprehensive Review as an oversight mechanism to ensure both the responsible Minister and the IGIS have appropriate visibility of the activities involving Australians.

58. If the class authorisation required the agreement of the Attorney-General, then this list must be provided to the Director-General of Security. This will ensure that ASIO continues to have visibility of potential threats to security – including Australians who are involved with listed terrorist organisations overseas.

59. The agency head must also provide a report to the responsible Minister in respect of activities undertaken under a class authorisation, accompanied by a statement identifying every Australian person who was included on the list during the period the authorisation was in effect (subsection 10A(3)). Once again this is intended to facilitate oversight and ensure that agencies are accountable for their activities.

60. As identified by both the Independent Intelligence Review and the Comprehensive Review, the use of class authorisations, in addition to existing individual authorisations, will strengthen the ability of agencies to investigate terrorist organisations. Specifically, reducing barriers to the ability of agencies to investigate classes of persons with links to terrorist organisations will enhance their ability to identify previously unidentifiable individuals of security concern. Allowing agencies to seek a ministerial authorisation to cover a class of persons, rather than requiring them to seek separate ministerial authorisation for each individual that would fall within the class, allows for the production of intelligence that is timelier, more agile and more responsive to the contemporary security environment, particularly where methodologies employed by terrorists have become more discreet than in the past and their methods for obfuscation of their activities more sophisticated.

61. One hypothetical case study to demonstrate this would be if ASD is producing intelligence on an Australian person under a ministerial authorisation. The person is a member of a listed terrorist organisation – Islamic State of Iraq and the Levant (ISIL). The Australian person orders three ISIL members to conduct an attack. The ISIL members are of unknown nationality but presumed Australian. Currently, ASD would not be able to target communications of these unknown persons to confirm their nationalities, identities or intentions without first seeking individual authorisations on all three. The grounds for seeking the three ministerial authorisations would be very similar to the grounds on which the existing ministerial authorisation was given – that the person is, or is likely, involved in activities that are, or a likely to be, a threat to security, given their membership of a listed terrorist organisation. Under the proposed amendments, all four members of ISIL could be covered

under a class authorisation, enabling ASD to produce intelligence on newly identified associates immediately as soon as they are discovered to ensure security and law enforcement agencies are best positioned to disrupt an attack.

3.4. Schedule 3 – Authorisations for activities in support of the Australian Defence Force

62. Schedule 3 amends section 8 of the IS Act to enable ASD and AGO to seek ministerial authorisation to undertake activities to produce intelligence on one or more members of a class of Australian persons when the agencies are operating in the course of providing assistance to the ADF in support of military operations or cooperating with the ADF on intelligence matters.

63. Currently, only ASIS can seek class authorisations for activities to provide assistance to the ADF in support of military operations, and cooperate with the ADF on intelligence matters. There are no corresponding provisions for ASD and AGO despite all three agencies having a statutory function to assist the ADF in support of military operations and to cooperate with the ADF on intelligence matters.

64. Currently, when ASD and AGO are supporting ADF operations, they must seek a ministerial authorisation for each individual Australian person who is determined to be part of, for example, a foreign militia group that is conducting operations against the ADF. In the context of a high-tempo conflict, this requirement can delay ASD's and AGO's ability to respond rapidly and identify new threats to the ADF and its operations.

65. The Independent Intelligence Review considered that all IS Act agencies should 'be able to obtain an authorisation to produce intelligence on one or more members of a class of Australian persons when providing assistance to the ADF in support of military operations'.[14]

66. The Comprehensive Review agreed with the Independent Intelligence Review, stating 'the Review sees no principled reason why the ability to obtain ministerial authorisation in relation to a class of Australians when providing support to the ADF should not be extended to AGO and ASD. All IS Act agencies have a clear and well established function of assisting the ADF. A class ministerial authorisation which is only available in respect of that function is specific and targeted'.[15]

67. These amendments implement recommendation 46 of the Comprehensive Review, and recommendation 16(b) of the Independent Intelligence Review.

68. In the context of a high-tempo conflict, the requirement to seek individual ministerial authorisations can delay agencies' ability to respond rapidly and identify new threats to the ADF and its operations. In these situations, ASD and AGO would benefit from the ability to seek authorisation to produce intelligence on a class of individuals to support the ADF in military operations, such as Australian foreign fighters who chose to fight for ISIS, rather than having to seek individual authorisations for each Australian.

69. Adding ASD and AGO to the existing provision allowing for ASIS to seek class authorisations when assisting the ADF will ensure ASD and AGO are able to provide critical operational support to the ADF, including providing timely intelligence on, and more readily discover new, adversary threats. This is necessary to assist the ADF in responding to threats to life – for example, imminent risks to the security of ADF personnel.

[14] *2017 Independent Intelligence Review*, paragraph 6.36.
[15] *Comprehensive Review of the Legal Framework of the National Intelligence Community by Mr Dennis Richardson*, Volume 2, paragraph 20.62.

70. The additional record keeping and reporting requirements introduced by Schedule 2 (new section 10AA and amended subsection 10A(3)) will apply to class authorisations in support of the ADF. This means each IS Act agency head must ensure that a list is kept which identifies each Australian person in relation to whom the agency intends to undertake activities under a class authorisation, explains why the agency believes the person is a member of the relevant class, and includes any other information the agency head considers appropriate (subsection 10AA(2)). The agency head must ensure that the list is available for inspection by the IGIS. This list of all persons on whom intelligence has been produced under a class authorisation was recommended by the Comprehensive Review as an oversight mechanism to ensure both the responsible Minister and the IGIS have appropriate visibility of the activities involving Australians.

71. If the class authorisation required the agreement of the Attorney-General, then this list must be provided to the Director-General of Security. This will ensure that ASIO continues to have visibility of potential threats to security – including Australians who are involved with listed terrorist organisations overseas.

72. The agency head must also provide a report to the responsible Minister in respect of activities undertaken under a class authorisation, accompanied by a statement identifying every Australian person who was included on the list during the period the authorisation was in effect (subsection 10A(3)). Once again this is intended to facilitate oversight and ensure that agencies are accountable for their activities.

3.5. Schedule 4 – Authorisations for producing intelligence on Australians

73. Schedule 4 clarifies the situations in which an IS Act agency is considered to be 'producing intelligence' on an Australian or class of Australians and thereby when IS Act agencies are required to seek a ministerial authorisation. The Schedule also amends the definition of 'intelligence information' in the IS Act.

74. This Schedule implements recommendation 41 of the Comprehensive Review and recommendation 16(d) of the Independent Intelligence Review. Both Reviews recommended that a definition of 'producing intelligence' be included in the IS Act to clarify the range of activities for which IS Act agencies require ministerial authorisation.

75. Currently, the IS Act agencies must obtain a ministerial authorisation before undertaking an activity with a specific purpose of producing intelligence on an Australian. The IS Act does not provide any guidance as to what constitutes 'producing intelligence'. The absence of guidance in the legislation creates uncertainty as to whether routine preliminary inquiries – that are not intrusive and that do not involve the use of covert intelligence collection capabilities – are 'producing intelligence' and require ministerial authorisation.

76. Both the Independent Intelligence Review and the Comprehensive Review, identified that the original intention of the ministerial authorisation regime in the IS Act was to require IS Act agencies to obtain a ministerial authorisation to use covert and intrusive intelligence collection capabilities in relation to an Australian person overseas, particularly where that collection method would require a warrant if conducted in Australia.

77. As stated by the Comprehensive Review, the meaning of 'producing intelligence' 'is central to determining whether an IS Act Agency must obtain ministerial authorisation before undertaking an activity', as 'the way this term is interpreted and applied goes directly to the level of ministerial control exercised in relation to intrusive intelligence activities impacting Australians'.[16] The Independent Intelligence Review recommended defining the meaning of 'producing intelligence' so that Ministerial

[16] *Comprehensive Review*, Volume 2, paragraph 19.122.

authorisation is required for the 'use of covert intelligence collection capabilities.'[17] The Comprehensive Review stated a clear definition of 'producing intelligence' is required to foster public trust and confidence in the work of intelligence agencies, and provide IS Act agencies with sufficient certainty regarding their statutory mandate.[18]

78. New subsection 8(1A) clarifies that an IS Act agency is 'producing intelligence' only if the agency undertakes a 'prescribed activity' to obtain that intelligence, or the agency expressly or impliedly requests an approved authority (approved under subsection 13(1)(c)) to undertake a 'prescribed activity' to obtain that intelligence.

79. This makes it clear that IS Act agencies must obtain ministerial authorisation before requesting a partner agency or an authority of another country to produce intelligence on an Australian on their behalf. Under these provisions, an IS Act agency does not 'produce intelligence' if it receives unsolicited intelligence from another body or group. This means an agency will not be placed in a situation where intelligence on an Australian is provided in an unsolicited manner with the agency having had no opportunity to seek a ministerial authorisation.

80. A definition of 'prescribed activity' is introduced in section 3 and subsection 8(1B) to mean a covert and intrusive activity, or series of activities. This includes, but is not limited to, activities that ASIO could not undertake without a warrant.

81. It is intended that activities will not fall within the definition of 'prescribed activity' unless they are both covert and intrusive. IS Act agencies might conduct an activity overtly, for example by conducting an interview where the interviewee knows they are dealing with the Australian Government, which could be considered intrusive depending on the nature of the information requested, but not covert. Similarly, an agency could conduct an activity that is covert but not intrusive, such as observing a person in a public place where there is no legitimate expectation of privacy. In these cases, the requirement to seek ministerial authorisation would be disproportionate to the nature of the activity.

82. These amendments remove uncertainty around whether ministerial authorisations are required for a range of administrative and preliminary activities not involving the use of covert and intrusive intelligence collection capabilities. This reflects the original intention of the ministerial authorisation framework.

83. Subsection 15(5) of the IS Act provides that IS Act agencies must not communicate 'intelligence information' concerning Australian persons, except in accordance with the Privacy Rules issued by the responsible Minister. When the IS Act was enacted, the definition of 'intelligence information' meant information obtained by ASIS or ASD under those agencies' intelligence collection functions. However, the definition was amended by the *Intelligence Services Legislation Amendment Act 2005*, which extended the definition in respect of ASIS to include all information obtained by ASIS in the performance of its functions. This had the unintended consequence of extending the application of the privacy rules to a wide range of routine information obtained by ASIS, for example, the sharing of media articles about Australians, or the curricula vitae of visiting Australians to partner agencies.

84. The Independent Intelligence Review (recommendation 16(d)) recommended that the definition of 'intelligence information' be amended to rectify the unintended and unnecessary administrative burden that has arisen from the current definition.

85. The amendment to the definition of 'intelligence information' in Section 3 of the IS Act, to remove the word 'information', will address the unintended consequences of the 2005 amendments. The amended definition means that agencies' will need to apply their Privacy Rules when communicating *intelligence* and not when an agency is communicating routine, publicly available information. 'Intelligence' is not defined, but can include information that is obtained by covert and intrusive means.

[17] *2017 Independent Intelligence Review*, paragraph 6.42.
[18] *Comprehensive Review*, Volume 2, paragraph 19.121.

86. The practical impact of this is that agencies will not have to apply required processes under their privacy rules when communicating routine, publicly available information concerning Australians. This could include, for example, the sharing of media articles about Australians, or the CVs of visiting Australians to partner agencies. Although not covered by privacy rules, these types of activities will continue to be subject to oversight by the IGIS.

3.6. Schedule 5 – ASIS cooperating with ASIO

87. Schedule 5 amends the IS Act to enable ASIS to conduct less intrusive activities to produce intelligence on an Australian inside Australia, where ASIO requests that assistance for the purposes of ASIO's functions.

88. Currently under section 13B of the IS Act, ASIS can undertake less intrusive activities to produce intelligence on an Australian person offshore following a written request from ASIO, for the purpose of assisting ASIO to perform its functions. In these instances, ASIS does not also need to seek an authorisation from the Minister for Foreign Affairs. This cooperation is limited to activities outside of Australia and ASIS can only assist ASIO under this framework by undertaking less intrusive activities – that is activities for which ASIO would not require a warrant in Australia. So, if ASIO could not undertake a particular act in at least one state or territory without it being authorised by a warrant, then ASIS still may not undertake that act as part of the section 13B regime. For example, ASIS could task an agent to obtain information, but could not intercept a person's communications as this would require a warrant.

89. While this tool works well for activities that are purely offshore, it leads to situations where important intelligence collection activities must be stopped because of the geographical limit in the legislation. For example, ASIS must currently direct an agent overseas not to contact possible sources in Australia for information, even if those contacts might have key information – such as the location or intention of an Australian foreign fighter based overseas.

90. Allowing ASIS to assist ASIO by undertaking less intrusive activities that extend onshore will enhance cooperation and integration between the agencies, and enable Australia to better thwart attacks and defeat other threats to security. The amendments do not authorise or provide a legal basis for ASIS to undertake activities inside Australia that would otherwise be unlawful.

91. This change implements recommendation 18(b) of the Independent Intelligence Review, which emphasised that 'cooperation among agencies is essential to maximise the likelihood of success in thwarting attacks and defeating other threats to Australia's national security'.[19] The Independent Intelligence Review recommended that the geographical limitation in section 13B(1) be removed to enable cooperation under section 13B to operate in Australia.

92. The Comprehensive Review recommended against amending section 13B, noting that any concerns regarding the continuity of intelligence collection could be addressed by agencies working more collaboratively together.[20] However, the Comprehensive Review's primary concern was that ASIS should continue to require a written notice from ASIO that ASIS's assistance is required. It did not explicitly consider whether onshore cooperation should be permitted where written notice has been provided.

[19] *2017 Independent Intelligence Review*, paragraph 6.54.
[20] *Comprehensive Review*, Volume 2, paragraph 22.65.

93. The amendments provided by Schedule 5 remove the geographical limitation on ASIS' cooperation with ASIO in section 13B of the IS Act. However, the amendments do not replicate the urgent circumstances exemption to offshore activities. The urgent circumstances exemption permits ASIS to act without written notice from ASIO where it cannot be practicably obtained in the circumstances. As such, ASIS will always be required to have a written notice from ASIO when cooperating under the section 13B regime onshore. In this way, the amendments have been developed in a way which addresses the primary concern of the Comprehensive Review.

94. The provisions in section 13B remain otherwise unchanged. Section 13B allows ASIS to cooperate with ASIO in support of ASIO's functions, which include gathering intelligence for purposes relevant to security. Security, as defined in the *Australian Security Intelligence Organisation Act 1979* (**ASIO Act**), includes the protection of the people of the Commonwealth from acts such as politically motivated violence, espionage and foreign interference.

95. Under the existing provisions, in giving a written notice under section 13B, ASIO must act in accordance with the ASIO Act, including by:

- ensuring that the intelligence requirement relates to ASIO's statutory functions which, relevantly, relate to the obtaining of intelligence relevant to 'security'—which is defined in the ASIO Act and includes the protection of, and of the people of, the Commonwealth and the several states and territories from matters such as espionage, acts of foreign interference, and politically motivated violence,
- adhering to the requirement in section 17A of the ASIO Act, that the exercise of the right to lawful advocacy, protest or dissent shall not be regarded as prejudicial to security, and
- complying with the Director-General of Security's special responsibility, set out in section 20 of the ASIO Act, to take all reasonable steps to ensure that the work of ASIO is limited to what is necessary for the purpose of the discharge of its functions.

96. The Director-General must be satisfied that there are satisfactory arrangements in place to ensure that activities will be undertaken only for the specific purpose of supporting ASIO in the performance of its functions, and that the nature and consequences of the acts done will be reasonable, having regard to the purposes for which they are carried out.

97. Further, all notices from ASIO must be kept by ASIS and made available for inspection on request by the IGIS. ASIS must also give its responsible Minister a written report in respect to activities undertaken as soon as practicable after each year ending on 30 June.

3.7. Schedule 6 – AGO cooperating with authorities of other countries

98. Schedule 6 amends the IS Act to provide that AGO is not required to seek ministerial approval in order to cooperate with an authority of another country, where the cooperation is for the purpose of performing AGO's non-intelligence functions under paragraphs 6B(1)(e), (ea) and (h) of the IS Act.

99. Section 13 of the IS Act establishes a framework under which AGO, ASD and ASIS may cooperate with Commonwealth authorities, State and Territory authorities and authorities of other countries in the performance of the agencies' own functions. In the case of cooperation with an authority of another country, cooperation can only occur where those authorities are approved by the responsible Minister as being capable of assisting the agency in the performance of its functions. The requirement to seek ministerial approval for cooperation with authorities of other countries was originally designed to capture only intelligence activities, which constituted all of AGO's functions. However, over the years, AGO's functions have been extended to a number of non-intelligence activities.

100. AGO is currently required to seek ministerial approval for all cooperation (related to both intelligence and non-intelligence functions) with authorities of another country. The practical effect of this has been, in certain circumstances, to hinder AGO's ability to effectively carry out its non-intelligence functions.

101. These non-intelligence functions include the Australian Hydrographic Office (AHO), a part of AGO, which produces official nautical charts and publications, and delivers services which support safety of navigation. The AHO is involved in the exchange of nautical information and the development, coordination and implementation of international hydrographic and maritime geospatial standards, and in undertaking these functions, cooperates with academic institutions, international organisations, other hydrographic offices, and foreign governments. AGO's other non-intelligence functions include providing geospatial data, mapping products, software and research to support regional partners, organisations and universities in circumstances such as following a natural or humanitarian disaster.

102. The purpose of ministerial approval for cooperating with authorities of other countries is to provide an additional layer of oversight where the cooperation, by virtue of involving potentially sensitive, covert or intrusive activities and capabilities, carries particular foreign relations and other risks. AGO's non-intelligence functions clearly do not fall within this scope.

103. Under the amendments, AGO will be required to report to its Minister and the Inspector-General of Intelligence and Security (IGIS) on any significant cooperation AGO undertakes with authorities of other countries. As with all AGO activities, the IGIS will continue to have oversight of cooperation AGO undertakes with authorities of other countries.

104. These provisions mirror existing arrangements in the IS Act for ASD's non-intelligence functions.

3.8. Schedule 7 – ONI cooperating with other entities

105. Schedule 7 amends the *Office of National Intelligence Act 2018* (**ONI Act**) to extend the approval regime that applies to cooperation with the authorities of other countries to cooperation with public international organisations. As a result, ONI's cooperation with public international organisations will be subject to approval by the Director-General of ONI.

106. Recommendation 24 of the Comprehensive Review found that section 13 of the ONI Act did not require broad amendment, on the basis that the legislative requirement for the Director-General to approve cooperation arrangements with an authority of another country is appropriate.

107. The Government response agreed with that position, but stated that section 13 of the ONI Act would be amended to require Director-General approval for cooperation with public international organisations. This is because the Government considered additional safeguards were required for cooperation arrangements with particular types of 'entities', specifically public international organisations, because of the international relations risks involved.

108. In the case of cooperation with an authority of another country, the Director-General of ONI is required to authorise such cooperation before it can take place (subsection 13(2)). The Director-General must also notify the Prime Minister of any approvals given on a monthly basis (subsection 13(3)). Once an authorisation has been given, it remains in place until amended or revoked by the Director-General or cancelled by the Prime Minister (subsection 13(5)).

109. Currently, public international organisations are considered 'entities' under paragraph 13(1)(b) of the ONI Act. This means that ONI can cooperate with public international organisations without seeking Director-General approval for that cooperation. The Director-General must approve cooperation arrangements with 'another country' but does not need to approve cooperation arrangements with an 'entity' (which would include a public international organisation). This schedule amends section 13 of the ONI Act to extend the approval regime that applies to cooperation with the authorities of other countries to cooperation with public international organisations. The approach to 'entities' more broadly is being amended.

110. The amendment adopts the existing definition of public international organisation from section 70.1 of the Criminal Code, which defines public international organisations as being those which comprise two or more countries. Public international organisations that fall within this definition include, for example, the United Nations, the World Health Organisation and the European Union.

111. The inclusion of 'public international organisations' in section 13 will not change the existing cooperation arrangements in the ONI Act for other entities or persons within or outside Australia.

112. The amendments provided by this schedule represent a necessary safeguard on cooperation with public international organisations and ensure that the Director-General of ONI is responsible for making decisions regarding cooperative arrangements which may impact Australia's foreign relations, and to ensure the Prime Minister has oversight of this cooperation.

3.9. Schedule 8 – Suspension of travel documents

113. Schedule 8 amends the *Australian Passports Act 2005* (Passports Act) and *Foreign Passports (Law Enforcement and Security) Act 2005* (Foreign Passports Act) to extend the period of passport suspension and foreign travel document surrender from 14 to 28 days.

114. Currently, the Minister for Foreign Affairs may order the suspension or surrender of a person's passport or foreign travel document for 14 days at the request of the Director-General of Security. The Director-General of Security may make a request where they suspect on reasonable grounds that a person may leave Australia to engage in conduct that might prejudice the security of Australia or a foreign country – for example, to commit a terrorist act, and the person's travel documents should be suspended or temporarily surrendered in order to prevent the person from engaging in that conduct (section 22A of the Passports Act and section 16A of the Foreign Passports Act).

115. The temporary suspension or surrender is intended to be an interim measure that can be taken in order to prevent a person from travelling before a security assessment recommending cancellation or long-term surrender can be made. The powers are typically used in cases where ASIO has little warning that a person intends to travel overseas. The 14 day suspension period is intended to give ASIO an opportunity to undertake all appropriate investigative activities and compile a security assessment to enable the Minister to consider whether to cancel the passport or order the long-term surrender of foreign travel documents.

116. Before compiling a security assessment, ASIO must:

- comprehensively review its intelligence holdings on the person concerned,
- plan and undertake intelligence collection activities, this could include activities that require the Director-General of Security to request warrants from the Attorney-General,
- request information from Australian and foreign partner agencies,
- assess all such information, to produce a detailed intelligence case, and
- where possible, interview the person to put ASIO's concerns to them, consistent with the requirements of procedural fairness, and assess their answers.

117. Operational experience has demonstrated that 14 days can be insufficient time to resolve these investigative activities and prepare a subsequent security assessment, giving full consideration to the need to ensure any recommendation for permanent action is appropriate. ASIO advises that there have been multiple occasions on which ASIO has not been able to finalise all appropriate investigative activities and furnish the Minister for Foreign Affairs with a security assessment concerning passport cancellation within the 14-day passport suspension period.

118. On a number of occasions, the first time a person has come to ASIO's attention has been as they are preparing to imminently travel overseas to a foreign conflict zone, and it has therefore been necessary to take action in a very short timeframe to prevent them from leaving Australia.

119. Extending the period to 28 days protects national security by allowing time for all appropriate investigative activities to be resolved, a properly considered security assessment to be prepared, and for all relevant information to be presented to the Minister to consider whether to cancel or require the permanent surrender of an individual's travel documents.

120. No extension beyond 28 days is available. When an order expires, any subsequent request for a suspension must be based on information gathered after the expiry of the first order. In addition, the IGIS has oversight of any request for passport suspension or temporary surrender made by the Director-General. If, following suspension, a person's passport is ultimately cancelled, the person has review rights in the Administrative Appeals Tribunal in relation to both that decision and the adverse security assessment relied upon to support passport cancellation.

121. Extending the passport suspension period is not a matter of administrative convenience. The Government must have the power to stop people from travelling overseas to commit terrorist attacks and other prejudicial activities. The reality is that security investigations take time, and often cannot be completed within a fortnight—particularly when cases come up on short notice.

3.10. Schedule 9 – Online activities

122. Schedule 9 amends the Criminal Code to provide staff members and agents of ASIS and AGO with immunity against computer offences in the Criminal Code where they reasonably believe that the conduct is likely to cause a computer related act, event, circumstance or result to take place outside Australia (whether or not it in fact takes place outside Australia).

123. This will align the immunities for ASIS and AGO with those of ASD following passage of the *Security Legislation Amendment (Critical Infrastructure) Act 2021*. In the Committee's *Advisory Report on the Security Legislation Amendment (Critical Infrastructure) Bill 2020 and Statutory Review of the Security of Critical Infrastructure Act 2018*, recommendation 10 was for the Government to consider whether the expanded immunity should also include AGO and ASIS.

124. These amendments are also consistent with Recommendation 74 of the Comprehensive Review, which recommends the current immunity in section 476.5 of the Criminal Code for IS Act agencies should be extended to apply where a staff member or agent reasonably believes the relevant conduct is likely to take place outside Australia, whether or not it in fact takes place outside Australia. The Comprehensive Review provides that criminal liability should not apply to a staff member or agent of an agency who 'acts in genuine belief that the activity is outside Australia'.[21] As the Comprehensive Review found, 'internet-based communications are increasingly untethered to geographic identifiers',[22] making it difficult for agencies to perform their functions under the current law. Since 'it is not always possible to determine the geographic location of a device or computer … extending the immunity afforded to agencies under section 476.5 in this manner would protect staff from criminal liability who have acted in good faith in the proper performance of the agency's functions'.[23] The amendments reflect the 'increasingly complex online environment', where it is not always possible to determine the geographic location of a computer, a person's location, or a communication's origins and end point.[24]

125. The underlying purpose of the immunities framework is to ensure that the staff members and agents of IS Act agencies are protected from civil and criminal liability for activities that are done in the proper performance of their functions, and that are intended and required by Government.

[21] *Comprehensive Review*, Volume 2, paragraph 24.202.
[22] Ibid.
[23] *Comprehensive Review*, Volume 2, paragraph 24.200.
[24] *Comprehensive Review*, Volume 2, paragraphs 24.201 and 24.202.

126. Extending immunities for staff members and agents of ASIS and AGO ensures that agencies can continue to efficiently perform their functions to protect Australia's national security, foreign relations and national economic well-being in response to changes in technology. This amendment is required to allow these agencies to continue to operate effectively in an increasingly complex online environment, where it is not always possible to reliably determine the geographic location of a device or computer, particularly where an adversary (such as foreign intelligence services, persons engaged in proliferation-related activities and terrorist organisations) takes active steps to conceal or obfuscate their location. For agencies to be able to effectively perform their functions in such an environment, it is necessary to protect staff members and agents from liability if they inadvertently affect a computer or device located inside Australia.

127. Extending the immunity to apply in circumstances where staff members and agents conduct computer-related activities on the reasonable belief that they will take place outside Australia (but which may inadvertently affect a computer or device inside Australia) is necessary to ensure that the scope of the legal immunity reflects the technological reality of the environment in which these persons operate. Protecting staff members and agents from liability for engaging in such conduct, in the proper performance of a function of a relevant agency, is necessary to ensure that those staff members and agents can undertake such activities in accordance with the Australian Government's requirements without fear of personal liability.

128. Section 476.5 of the Criminal Code was introduced by the *Cybercrime Act 2001*. As originally introduced, subsection 476.5(1) provided immunity from civil and criminal liability for the staff members and agents of ASIS and ASD (then known as the Defence Signals Directorate) whose computer-related activities done outside Australia, in the proper performance of their functions, were intended and required by Government. The *Intelligence Services Legislation Amendment Act 2005* extended the immunity to apply to AGO (then known as the Defence Imagery and Geospatial Organisation).

129. Currently, sections 476.5 and 476.6 provide immunity to staff members and agents of ASIS, AGO and ASD for certain computer-related acts. Section 476.5 provides that staff members and agents of ASIS and AGO are not subject to any civil or criminal liability for computer-related acts done outside Australia if the act is done in the proper performance of a function of the relevant agency. The *Security Legislation Amendment (Critical Infrastructure) Act 2021* introduced section 476.6 which: mirrors the immunity in section 476.5 for ASD; and extends the immunity to circumstances where the staff member or agent of ASD act on a reasonable belief that a computer-related activity occurred outside Australia, even where that activity actually occurred inside Australia. These amendments will add ASIS and AGO to the immunity provisions in section 476.6 and will repeal section 476.5.

130. The immunities for computer-related acts in the Criminal Code supplement the general immunities for ASIS, ASD and AGO under subsection 14(1) of the IS Act, to ensure Australian law, including the computer offences in Part 10.7 of the Criminal Code, does not prohibit these agencies from doing computer-related acts outside Australia in the proper performance of their functions.

131. The amendments are limited to circumstances where staff members and agents engage in conduct in the proper performance of a function of a relevant agency, including in compliance with the requirement under the IS Act to obtain ministerial authorisation to produce intelligence on an Australian person. Staff members and agents will not be immune for conduct engaged in otherwise than in the proper performance of a function of a relevant agency.

132. The immunity is also limited to circumstances where staff members and agents engage in conduct on the reasonable belief that it will cause a computer-related act, event, circumstance or result to take place outside Australia (paragraph 476.6(1)(a)). A staff member or agent will not be immune if they believe that their conduct will take effect inside Australia, or if their belief is not reasonable in the circumstances. In this regard, the scope of the immunity reflects the well-established defence of mistake of fact, contained in section 9.1 of the Criminal Code.

133. An agency will be required to report to the IGIS on activities that cause material damage, interference or obstruction to a computer in Australia.

3.11. Schedule 10 – Privacy

134. To perform their functions effectively, Australia's intelligence agencies must be able to protect sensitive sources, techniques and capabilities. For this reason, intelligence agencies are either exempt or partially exempt from the provisions of the *Privacy Act 1988* (**Privacy Act**).[25] Instead, these agencies are subject to direct ministerial control, IGIS oversight, and importantly, privacy rules made by the responsible Minister, which regulate the communication and retention of intelligence information concerning Australian persons.

135. The privacy rules provide a necessary and important protection for the privacy of Australian persons. Special protections for Australians is a long-standing, core principle of accountability for Australian intelligence agencies. This principle was recognised by the Hope Royal Commissions and was acknowledged as a relevant principle by both the Comprehensive Review and Independent Intelligence Review.

136. The Independent Intelligence Review identified that there is "an emphasis on the special rights to privacy and civil liberties of Australian persons" and argued that "that underpinning continues to be important and the privileging of Australian persons in the mandates of … Australian intelligence agencies and in Australian law remains strong".[26] The Comprehensive Review found that "the legislative framework for the collection and production of foreign intelligence appropriately distinguishes between Australians and non-Australians" and, "additional procedural steps for … intelligence collection activities in respect of Australians … [is] a deliberate decision by the Parliament".[27]

Part 1 - Privacy rules of ASIS, AGO, ASD

137. Part 1 of Schedule 10 amends the IS Act to introduce a requirement that IS Act agencies must, as soon as is practicable after their respective privacy rules have been made, publish those rules on their websites.

138. Recommendation 189 of the Comprehensive Review concluded that while the IS Act agencies continue to meet the relevant criteria justifying their exemption from the Privacy Act, and that their current privacy regimes are adequate, minor changes should be made to their privacy arrangements to improve transparency. Specifically, it considered that these agencies should be required, by legislation, to maintain and publish their own legally binding privacy rules, and that these rules should be required to be made by the relevant Minister. This is consistent with a recommendation made by the Australian Law Reform Council in its 2008 review.[28]

139. Currently, section 15 of the IS Act requires IS Act agencies to have legally binding privacy rules made by their responsible Minister. As a matter of practice, these agencies already make their privacy rules publicly available. However, there is no current legislative requirement for them to do so. Part 1 of Schedule 10 amends section 15 of the IS Act to make the publication of IS Act agencies' privacy rules a formal statutory requirement.

[25] Exemptions from the Privacy Act are contained in the *Freedom of Information Act 1982*. ASIS and ASD are fully exempt from the operation of the Privacy Act, while AGO is not listed as an exempt agency, as it is not an independent statutory agency—rather it is an entity that is part of the Department of Defence. AGO is exempt where the acts and practices that impact on privacy relate to is functions. This includes all operational documents. Accordingly, AGO is considered to be 'fully exempt'.
[26] *2017 Independent Intelligence Review*, paragraph 2.22
[27] *Comprehensive Review,* Volume 1, paragraph 3.35
[28] Australian Law Reform Council, *For your Information*, Volume 2, paragraph 34.105.

140. Recommendation 183 of the Comprehensive Review concluded that the IS Act should be amended so that the Committee may review agency privacy rules as made, but not agency *compliance* with agency privacy rules, which is the role of the IGIS. Enabling the Committee to review privacy rules as made will enhance confidence in agency privacy safeguards, and improve both transparency and accountability. Retaining IGIS oversight of agency compliance with its privacy rules will ensure there is no overlap between the Committee and the IGIS, and is consistent with the Government's position that IGIS, and not the Committee, should oversee operational matters.

141. Under existing legislation, the Committee is expressly prohibited from reviewing the privacy rules which apply to ASIS, ASD and AGO (paragraph 29(3)(f)). Part 1 of Schedule 10 amends section 29 of the IS Act to provide that it is a function of the Committee to review ASIS, ASD and AGO's privacy rules, as made by the relevant responsible Minister, while providing that it is not a function of the Committee to review agencies' *compliance* with such privacy rules. It is the Government's longstanding position that it is the role of the IGIS to oversight agencies' compliance with their privacy rules.

Part 2 - Privacy rules of DIO

142. Part 2 of Schedule 10 amends the IS Act to introduce a requirement for the responsible Minister in relation to DIO to make written rules regulating the communication and retention by DIO of intelligence information concerning Australian persons, and for these rules to be, as soon as is practicable, published on DIO's website.

143. DIO is exempt from the operation of the Privacy Act where the acts and practices impacting privacy relate to the performance by DIO of its mandate. Recommendation 189 of the Comprehensive Review concluded that, while DIO continues to meet the relevant criteria justifying its exemption from the Privacy Act, and that its current privacy regime is adequate, minor changes should be made to its privacy arrangements to improve transparency. As with the IS Act agencies, DIO should also be required, by legislation, to maintain and publish its own legally binding privacy rules, and these rules should be required to be made by the relevant Minister.

144. Currently, DIO has publicly available privacy rules approved by the Minister for Defence. However, these are not mandated by legislation. This is in contrast to IS Act agencies and ONI who all have provisions in legislation for their responsible Minister to issue privacy rules. While DIO, unlike the IS Act agencies and ONI, is not established under an Act, the Comprehensive Review considered that it would be legislatively possible to require it to have privacy rules, as has been done in relation to other matters in the IS Act that relate to DIO, such as secrecy. Agencies that provide information to DIO include foreign intelligence collection agencies ASIS, ASD and AGO, whose legislation and rules distinguish between Australians and non-Australians.

145. Part 2 of Schedule 10 amends the IS Act to introduce new section 41C. Section 41C formalises in legislation the requirement for the responsible Minister in relation to DIO to make written rules regulating the communication and retention by DIO of intelligence information concerning Australian persons. Section 41C also introduces the requirement that the responsible Minister in relation to DIO must ensure, as soon as is practicable, that DIO's privacy rules be published on DIO's website.

146. As with Part 1, Part 2 of Schedule 10 amends section 29 of the IS Act to provide that it is a function of the Committee to review DIO's privacy rules, as made by the responsible Minister. The amendments provide that it is not a function of the Committee to review DIO's compliance with its privacy rules.

147. Part 2 of Schedule 10 also makes minor amendments to the *Inspector-General of Intelligence and Security Act 1986* (**IGIS Act**) to include DIO as one of the agencies that the IGIS is required to include in its reporting of privacy rules compliance in its annual report.

Part 3 - Privacy rules of ONI

148. Part 3 of Schedule 10 amends the ONI Act so that ONI's privacy rules, as made by the Prime Minister, apply only to ONI's analytical functions and not to ONI's other functions, including the communication of administrative or publicly available information.

149. Recommendation 12 of the Comprehensive Review concluded that the ONI Act should be amended so that the privacy rules apply only to analytical products created pursuant to ONI's open source function in paragraph 7(1)(g). The Government response agreed with this recommendation. However, it considered amendments were required both with respect to products created under ONI's open source function, as well as with respect to information held and communicated by ONI more broadly.

150. ONI is fully exempt from the operation of the Privacy Act. Under section 53 of the ONI Act, the Prime Minister must make privacy rules which regulate the collection of identifiable information under ONI's open source information function (paragraph 7(1)(g)), and the communication, handling and retention of identifiable information by ONI more generally. Identifiable information is personal information about Australian citizens or residents.

151. The Comprehensive Review considered that, in practical terms, the current definition of 'identifiable information' in the ONI Act is overly broad, and could constrain ONI in the performance of its functions. Currently, the privacy rules cover all of ONI's functions, analytical or otherwise. This encompasses a broad range of scenarios, including where the information concerned is either administrative in nature, or, in the case of ONI's open source function, already in the public domain – for example, contained in a news article. ONI is prohibited from communicating or collecting identifiable information, except in accordance with the privacy rules. This hinders ONI from contributing valuable insights to NIC and other government forums, despite some information already being public.

152. It is both impractical and unnecessarily burdensome for the privacy rules to apply to administrative, staffing or publicly available information where the privacy risk associated with communicating that information is low, because that information is either voluntarily provided to the agency, or is already in the public domain. Further, unlike other NIC agencies, ONI does not have covert or intrusive powers to collect intelligence (such as the ability to obtain warrants), nor do ONI's functions include directing a NIC agency to carry out operational activities. As such, personal information about Australian persons that is obtained for the purposes of ONI's non-analytical functions is unlikely to impact on the right to privacy and is therefore outside the intended purpose of the privacy rules. ONI's internal policies and practices provide appropriate privacy protections for personal information that is obtained as part of ONI's non-analytical functions.

153. Part 3 of Schedule 10 amends section 53 of the ONI Act to make a distinction between 'personal information' and 'intelligence information'. The effect of this is to exclude the communication of non-intelligence, administrative and open source products from the privacy rules regime. This means that, under the amended privacy provisions, ONI's privacy rules do not apply to the communication of personal information where that personal information is not also intelligence information. The privacy rules only apply in circumstances where the personal information provided to, or collected or assembled by, ONI is evaluated, analysed, interpreted, integrated and/or tested such that it becomes intelligence. The privacy rules continue to regulate the collection of information concerning Australian persons by ONI when performing its open source function.

154. This difference between 'information' and 'intelligence' is consistent with the meanings of 'intelligence' and 'uses of intelligence' set out in the third report of the Hope Royal Commission:

> *Intelligence is, to some degree, processed information. It is processed information in the sense that a lot of different items of knowledge have been put together, tested against each other for credibility and a judgement made on balance as to the truth, or at least the greatest degree of probability of the truth about some particular situation. It is also assessed as relevant to the consumer. … Intelligence is information gathered for policy makers in government which illuminates the range of choices available to them and enables them to exercise judgment.*[29]

155. Consistent with the Government response to recommendation 12 of the Comprehensive Review, Part 3 of Schedule 10 further amends section 53 of the ONI Act to provide that the privacy rules apply only to personal information about an Australian citizen or permanent resident where that information is also intelligence information under ONI's two other analytical functions (paragraphs 7(1)(c) and (d)). This aligns with the approach described above for the treatment of personal information for ONI's open source function. This means that, under the amended privacy provisions, ONI's privacy rules do not apply, for example, to the communication of administrative and staffing information. This is consistent with the approach taken currently by the IS Act and as amended by Schedule 4 of the Bill (Authorisations for producing intelligence on Australians).

156. Part 3 of Schedule 10 includes an additional provision in section 7 of the ONI Act to clarify that one of ONI's functions is to communicate, in accordance with the Government's requirements, intelligence that is produced under ONI's analytical functions through evaluation, analysis, interpretation and integration.

157. As with Part 1, Part 3 of Schedule 10 amends section 29 of the IS Act to provide that it is a function of the Committee to review ONI's privacy rules, as made by the responsible Minister. The amendments provide that it is not a function of the Committee to review ONI's compliance with its privacy rules.

158. Part 3 of Schedule 10 also makes minor amendments to a note in the IGIS Act to reflect the amendments to ONI's privacy rules.

159. Despite the removal of the privacy rules from ONI's non-analytical functions, ONI continues to be bound by the requirements in sections 7 and 10 of the ONI Act, which set out ONI's functions and powers, and Part 4 of the ONI Act, which provides for, among other things, the protection of information provided to ONI, and secrecy offences that apply to ONI information. These sections provide significant safeguards to ensure that ONI's activities are undertaken consistently with the right to protection against arbitrary and unlawful interferences with privacy. Sections 7 and 10, and Part 4 of the ONI Act, information handling and retention requirements in the Protective Security Policy Framework, IGIS reporting and oversight requirements, and direct ministerial control, ensure that all information is obtained and shared only when it is necessary and proportionate to do so, irrespective of whether it is for the purposes of ONI's analytical or non-analytical functions.

160. These amendments are a necessary measure to remove an impediment to the communication of information where the privacy risk associated with that information is low, for example because the information is for staffing or administrative purposes, or already publicly available. Additionally, the amendments, in clarifying the application of the privacy rules, support greater public understanding of the operation of the legislation, which fosters public trust and confidence in the work of Australia's intelligence agencies. The amendments also provide ONI itself with greater certainty regarding its statutory mandate.

[29] Parliament of the Commonwealth of Australia, Parliamentary Paper No. 92/1977, *Royal Commission on Intelligence and Security, Third Report*, Abridged Findings and Recommendations, pp. 1-2.

Part 4 - Contingent amendments

161. Part 4 of Schedule 10 makes a minor contingent amendment to the IS Act to clarify that the definition of 'intelligence function' in section 3 (contingent upon passage of the Intelligence Oversight and Other Legislation Amendment (Integrity Measures) Bill 2021) is in relation to AUSTRAC only.

3.12. Schedule 11 – Assumed identities

162. Schedule 11 amends the *Crimes Act 1914* (**Crimes Act**) to include ASD in the assumed identities scheme, subject to limitations on acquiring evidence of the assumed identity.

163. The assumed identities scheme allows authorised officers of law enforcement and intelligence agencies to act under false identities in the course of conducting investigations. The scheme enables these agencies to obscure sensitive activities that would be undermined if they were to be connected with a law enforcement or intelligence agency, and protect the true identity of individual officers.

164. Currently, under subsection 15KB(2) of the Crimes Act, an authority to acquire or use an assumed identity can only be granted in connection with one or more specific purposes. These purposes include 'the exercise of powers and performance of functions of an intelligence agency'. A range of Commonwealth, state and territory law enforcement and intelligence agencies have the authority to acquire and use an assumed identity in the Crimes Act. The only intelligence agencies authorised in the existing scheme are ASIO, ASIS and ONI. ASD is not captured by the definition of 'intelligence agency' in Part IAC of the Crimes Act, despite being listed as an intelligence agency elsewhere in the Crimes Act for other purposes.

165. In practice ASIS and ASIO operate assumed identities on ASD's behalf, in accordance with the Crimes Act and other legislation governing the activities of these agencies. This means the Director-General of ASIO or ASIS is required to approve a request from ASD to acquire and use an assumed identity. In addition, a supervisor from either ASIO or ASIS must be appointed to oversee ASD's use of the assumed identity, even in circumstances where ASIO or ASIS has no involvement in the relevant activities or operations. This creates administrative and operational burdens on both agencies and is inconsistent with the approach for other intelligence agencies.

166. Schedule 11 provides ASD with the authority to operate and use an assumed identity. This is important for protecting procurement of sensitive information and communications technology, equipment or services, and other activities undertaken by ASD in accordance with its functions. In particular, this is vital for ASD's cyber operations capability, which could be compromised if, for example, the purchase of sensitive information and communications technology, equipment or services were associated with ASD.

167. The amendments do not enable ASD to acquire evidence of an assumed identity. This is an appropriate limitation, as other agencies have the expertise to acquire evidence of an assumed identity and can perform this function on ASD's behalf.

168. The existing assumed identities scheme has oversight and reporting mechanisms to ensure appropriate use of the assumed identities. ASD will be required to comply with these safeguards which include that the Director-General of ASD must approve the use of an assumed identity and that they can only do so if they are satisfied on reasonable grounds that the assumed identity is necessary in the exercise of the powers and performance of ASD's functions. The Director-General must also comply with record-keeping obligations to ensure effective oversight. For example, in section 15LE, as soon as practicable after the end of each financial year, the chief officer of an intelligence agency must submit a report to the IGIS that includes certain information for the year, including whether or not any fraud or other unlawful activity was identified by an audit under section 15LG during the year, the number of applications and any other information that the IGIS considers appropriate relating to authorities and assumed identities.

169. The scheme also includes safeguards against improper use of an assumed identity through section 15LB, which makes it an offence for an authorised person or authorised civilian to use or acquire evidence of an assumed identity if the person is reckless as to whether the acquisition or use is not in accordance with an authority or the course of duty, with a penalty of imprisonment for two years.

3.13. Schedule 12 – Authorities of other countries

170. Schedule 12 provides greater clarity on what might constitute an 'authority of another country' for the purposes of the IS Act.

171. The IS Act uses, but does not define, the expression 'authority of another country'. This creates uncertainty about the proper interpretation of the term, which appears in several places in the IS Act, including in section 13 regarding cooperation with particular entities. In particular, the IS Act does not clarify whether such an authority needs to be a body linked to an internationally recognised government, or a government that instead exercises effective or de-facto control over all or part of a country.

172. The amendment provides greater clarity on what might be an 'authority of another country' for the purposes of the IS Act. The amendment provides that for a body to be an 'authority of another country' for the purposes of the IS Act, it is not required that the body be established by a law of the country or be connected with an internationally recognised government of a country.

173. This is not intended to be a comprehensive definition of the term, but rather ensures that agencies may cooperate with bodies in other countries even if those bodies are not established by a law of the country or are not connected to, or controlled by, the internationally recognised government of the country.

174. For example, this could occur in situations where the internationally recognised government of a country is disputed, disrupted or not in control of the whole of its territory.

175. This amendment does not alter the ordinary meaning of the term 'authority', in that it generally needs to be performing or purporting to perform one or more traditional functions of government, and exercising its powers for a public, rather than private, purpose.

176. Under section 13 of the IS Act, IS Act agencies are required to seek ministerial approval to cooperate with authorities of other countries. The purpose of this is to provide the Minister with oversight and control over agencies' cooperation with authorities of countries, given that this could raise foreign relations and human rights risks. This amendment does not change this key oversight role of the Minister. Any decision by the Minister in this regard would take into account a range of factors, including the human rights record of the other country and the legality and propriety of any proposed cooperation.

177. In relation to section 13, the amendment ensures that IS Act agencies can seek ministerial approval to cooperate not just with authorities of the internationally recognised government of the country, but other authorities who may exercise effective control over all or part of the country.

178. In circumstances where it may be unclear who the legitimate government is, or where the government is no longer exercising control over all or parts of the territory, it is important that agencies are able to cooperate with those authorities who are actually performing governmental functions in that country or part of the country, subject to ministerial approval. Without the amendment, the application of the cooperation framework in section 13 to such bodies is uncertain. In addition, it is crucial that cooperation in these circumstances be subject to ministerial approval, given the potential foreign relations and human rights issues which could arise.

179. Further, the activities of IS Act agencies also remain subject to the oversight of the Inspector-General of Intelligence and Security, who is responsible for oversight of agencies' compliance with international human rights obligations.

180. The question of what is an authority of another country for the purposes of the IS Act was not considered in the Comprehensive Review, or the Independent Intelligence Review. The amendment is a minor change to provide clarity and remove doubt.

3.14. Schedule 13 – ASIO Authorisations

181. Schedule 13 amends the ASIO Act and the *Telecommunications (Interception and Access) Act 1979* (**TIA Act**) to permit the Director-General of Security to approve a class of persons to exercise the authority of an ASIO interception warrant in the TIA Act and to clarify that where the Director-General of Security approves a class of persons to exercise the authority of a warrant or device recovery provision in either the ASIO Act or TIA Act, that approval accommodates positions within the scope of the class that come into existence after the approval is given. The Schedule also introduces a requirement that the Director-General of Security must ensure accurate records are kept of the person or persons who exercise the authority of ASIO warrants.

182. Schedule 13 implements recommendations 36, 37 and (as it pertains to ASIO warrants) 103 of the Comprehensive Review, which found that:

- the ASIO Act should be amended to clarify the permissible scope of a class of persons approved to exercise the authority conferred by a warrant, and that additional record keeping requirements should apply to the exercise of that authority, and
- similar provisions should be contained in a new electronic surveillance act, including in relation to ASIO's telecommunication interception powers.

183. The Comprehensive Review considered that 'it should be clear on the face of the ASIO Act that the ability to authorise a class of persons to exercise the authority conferred by a warrant captures changes to, and expansions of, the class of persons authorised to execute a warrant after that authorisation has been made'.[30] It considered that this approach should also be taken in relation to ASIO's telecommunications interception warrants. The Review also recommended that ASIO should keep accurate records of all individuals involved in the execution of a warrant.

184. Currently, under subsection 24(2) of the ASIO Act, the Director-General of Security (or a senior position-holder appointed by the Director-General of Security under subsection (3)) may approve a person or class of persons to exercise the authority conferred by a relevant warrant or a relevant device recovery provision.

185. The ASIO Act does not specify whether subsection 24(2) accommodates an expansion to a class of persons subsequent to such an authorisation being made. Such a situation may arise if, for example, the Director-General of Security has approved a particular class of persons to exercise the authority conferred by a particular warrant and, subsequent to that approval being given, an additional position is created that is within the scope of the original approved class—the Act does not specify whether that additional position may exercise the authority conferred by the warrant.

186. Schedule 13 amends section 24 of the ASIO Act to clarify that where the Director-General of Security, or a senior position-holder appointed by the Director-General, approves a person or class of persons holding, occupying or performing the duties of an office or position, the approval extends to an office or position that comes into existence after the approval is given.

187. Section 12 of the TIA Act, provides that the Director-General of Security (or an 'authorising officer') may approve persons to exercise the authority, on behalf of ASIO, of a Part 2-2 warrant. An 'authorising officer' is an ASIO employee or ASIO affiliate appointed by the Director-General of Security.

[30] *Comprehensive Review*, Volume 2, paragraph 19.82.

188. Schedule 13 also amends section 12 of the TIA Act to:

- make clear the Director-General of Security, or an 'authorising officer', can approve a class of persons to exercise, on behalf of ASIO, the authority conferred by a Part 2-2 warrant, and
- consistent with the amendments to section 24 of the ASIO Act, make clear that where the Director-General of Security, or an 'authorising officer', approves a person or a class of persons holding, occupying or performing the duties of an office or position to exercise the authority conferred by a Part 2-2 warrant, the approval extends to an office or position that comes into existence after the approval is given.

189. Schedule 13 also introduces a requirement that the Director-General of Security must ensure accurate records are kept of the person or persons who exercise the authority conferred by a relevant warrant or relevant device recovery provision under the ASIO Act or a warrant issued under Part 2-2 of the TIA Act. In the ASIO Act, a relevant warrant is a warrant issued under Division 2 or Division 3 of the ASIO Act. A relevant device recovery provision is a provision listed in section 24(4) of the ASIO Act.

190. The record keeping requirement captures those people who actually exercise the authority conferred by such warrants or provisions, rather than all persons who are approved to exercise authority conferred by the warrant or provision. This will facilitate effective oversight, by ensuring that records are available to the IGIS of which members of the approved class have actually exercised the authority of the warrant or provision.

191. The amendments will provide greater clarity and certainty about who may exercise the authority of ASIO warrants, while retaining strict and appropriate limits. The introduction of an express provision providing for the approval of a class of persons in the TIA Act allows for consistency in the approach for ASIO warrants across both the ASIO Act and the TIA Act. This approach is also in line with how delegations are treated across Commonwealth law (as set out in section 34AA of the *Acts Interpretation Act 1901*).

3.15. Schedule 14 – Technical Amendments

192. Schedule 14 contains technical amendments to correct a referencing error and a minor omission in the *Intelligence Services Amendment (Establishment of the Australian Signals Directorate) Act 2018*.

193. The first amendment corrects an omission to ensure that there is an appropriate time limit on all ministerial authorisations issued in relation to ASD's cybercrime disruption function under section 9(4) of the IS Act or renewed under section 10(1A) of the IS Act. This ensures consistency with the ministerial authorisation framework under the IS Act.

194. The second amendment corrects a referencing error by amending subsection 13(5) of the IS Act, substituting 'this section' with 'subsection (4)' and substituting 'section (4)' with 'that subsection'. This ensures the Director-General of ASD is required to provide a report about any significant cooperation occurring under subsection 13(4).

Annexure A

National Security Legislation Amendment (Comprehensive Review and Other Measures No. 1) Bill 2021
Summary of Measures

Schedule	Act Amended	Summary	Comprehensive Review of the Legal Framework of the National Intelligence Community	2017 Independent Intelligence Review
Schedule 1 *Emergency authorisations*	*Intelligence Services Act 2001*	Enables the Australian Secret Intelligence Service (**ASIS**), the Australian Signals Directorate (**ASD**) and the Australian Geospatial-Intelligence Organisation (**AGO**) (**IS Act agencies**) to act immediately and without ministerial authorisation in emergency situations where the safety of an Australian person offshore is under imminent threat and it is reasonable to believe that the person would consent to the agency producing intelligence on them.	Government response to recommendation 52	Rec 16(e)
Schedule 2 *Authorisations relating to counter-terrorism*	*Intelligence Services Act 2001*	Allows IS Act agencies to produce intelligence on a class of Australian persons who are, or are likely to be, involved with a listed terrorist organisation. The new class authorisations are accompanied by additional oversight arrangements, consistent with the Comprehensive Review.	Government response to recommendation 45	Rec 16(a)
Schedule 3 *Authorisation for activities in support of the Australian Defence Force*	*Intelligence Services Act 2001*	Enables ASD and AGO to seek ministerial authorisations to undertake activities to produce intelligence on one or more members of a class of Australian persons when the agencies are operating in the course of providing assistance to the Australian Defence Force (**ADF**) in support of military operations and when cooperating with the ADF on intelligence matters. The new class authorisations are accompanied by additional oversight arrangements, consistent with the Comprehensive Review.	Government response to recommendation 46	Rec 16(b)
Schedule 4 *Authorisations for producing intelligence on Australians*	*Intelligence Services Act 2001*	Clarifies that IS Act agencies are only 'producing intelligence' when undertaking covert or intrusive activities, or requesting a foreign authority to undertake such an activity on its behalf. The effect of this is to ensure that ministerial authorisations are only required for the use of covert and intrusive intelligence collection capabilities. This measure also amends the definition of 'intelligence information' to ensure that the Privacy Rules apply only to intelligence produced via agencies' intelligence collection capabilities, and not to routine or open source information.	Government response to recommendation 41	Rec 16(d)

Annexure A

Schedule	Act Amended	Summary	Comprehensive Review of the Legal Framework of the National Intelligence Community	2017 Independent Intelligence Review
Schedule 5 *ASIS cooperating with ASIO*	*Intelligence Services Act 2001*	Extends the framework for cooperation between ASIS and the Australian Security Intelligence Organisation (**ASIO**) under Division 3 of the IS Act to remove the geographic limit requiring that ASIS activities undertaken in support of ASIO be conducted outside of Australia only. The effect of this is to extend the cooperation framework to enable ASIS to assist ASIO onshore, subject to receipt of a written notice from ASIO.	Government response to recommendation 57	Rec 18(b)
Schedule 6 *AGO cooperating with authorities of other countries*	*Intelligence Services Act 2001*	Exempts AGO from section 13 of the *Intelligence Services Act 2001* ministerial authorisation framework regarding cooperation with authorities of other countries for its non-intelligence functions.	N/A	N/A
Schedule 7 *ONI cooperating with other entities*	*Office of National Intelligence Act 2018*	Extends the safeguards that apply to the Office of National Intelligence's (**ONI**) cooperation with the authorities of other countries to cooperation with public international organisations. This will require that cooperation with public international organisations be subject to Director-General approval.	Government response to recommendation 24	N/A
Schedule 8 *Suspension of travel documents*	*Australian Passports Act 2005* *Foreign Passports (Law Enforcement and Security) Act 2005*	Extends the period for passport suspension and foreign travel document surrender from 14 to 28 days, based on operational experience of the time required for ASIO to prepare a security assessment without substantially diverting resources from live investigations.	N/A	N/A
Schedule 9 *Online activities*	*Criminal Code Act 1995*	Extends the immunity for certain computer offences (for ASIS and AGO), under section 476.5 of the Criminal Code, to apply where a staff member or agent of the relevant agency acted on a reasonable belief that a computer-related activity occurred outside Australia, even if that activity actually occurred inside Australia. This complements similar reforms introduced by the Government for ASD in the Security Legislation Amendment (Critical Infrastructure) Bill 2020.	Government response to recommendation 74	N/A

Annexure A

Schedule	Act Amended	Summary	Comprehensive Review of the Legal Framework of the National Intelligence Community	2017 Independent Intelligence Review
Schedule 10 *Privacy*	*Intelligence Services Act 2001* *Inspector-General of Intelligence and Security Act 1986* *Office of National Intelligence Act 2018*	Requires that IS Act agencies must publish their privacy rules on the relevant agency's website. (Part 1) Introduces a requirement that the responsible Minister for DIO must issue privacy rules that must be published on DIO's website. Provides that it is a function of the Inspector-General of Intelligence and Security (**IGIS**) to oversight DIO's compliance with the privacy rules. (Part 2) Amends ONI's privacy provisions to require that ONI's privacy rules only apply to information that is part of ONI's analytical functions. (Part 3) Introduces a function for the Parliamentary Joint Committee on Intelligence and Security (**PJCIS**) to review the privacy rules as made by the relevant Minister (Parts 1, 2 and 3). Provides for contingent amendments relating to passage of the Intelligence Oversight and Other Legislation Amendment (Integrity Measures) Bill 2021. (Part 4)	Government response to recommendations 12, 183 and 189	N/A
Schedule 11 *Assumed identities*	*Crimes Act 1914*	Includes ASD in the assumed identities regime set out in Part IAC of the Crimes Act. The effect of this is that the Director-General of ASD will be able to authorise the acquisition and use of an assumed identity. Authorised officers acting under a false identity under the scheme will not be found responsible for a Commonwealth, state or territory criminal offence.	N/A	N/A
Schedule 12 *Authorities of other countries*	*Intelligence Services Act 2001*	Clarifies the definition of '*authority* of another country' in the IS Act.	N/A	N/A
Schedule 13 *ASIO authorisations*	*Australian Security Intelligence Organisation Act 1979* *Telecommunications (Interception and Access) Act 1979*	Permits the Director-General of Security to authorise a class of persons to exercise authority under an ASIO warrant in the TIA Act. Clarifies the permissible scope of classes under section 24 of the ASIO Act and section 12 of the TIA Act to accommodate certain changes to the class after it is approved. Introduces additional record-keeping requirements regarding people exercising authority under all ASIO warrants.	Government response to recommendations 36, 37 and 103	N/A

Annexure A

Schedule	Act Amended	Summary	Comprehensive Review of the Legal Framework of the National Intelligence Community	2017 Independent Intelligence Review
Schedule 14 *Amendments related to the Intelligence Services Amendment (Establishment of the Australian Signals Directorate) Act 2018*	*Intelligence Services Act 2001*	Makes technical amendments to correct a minor referencing error and an inadvertent omission in the *Intelligence Services Amendment (Establishment of the Australian Signals Directorate) Act 2018*.	N/A	N/A

Domestic spying for ASD a possibility

By Sarah Basford Canales

The Canberra Times
Friday 26th November 2021
458 words
Page 8 | Section: NEWS
286cm on the page

Domestic spying for ASD a possibility

NATIONAL SECURITY ASD on path for domestic spying with narrow scope

Sarah Basford Canales

PROPOSED laws to expand and streamline Australia's spying and intelligence operations will allow one agency to spy on Australians in the country for the first time in its nearly 75-year lifetime.

But while experts say the changes won't result in a nationwide spying regime of Snowden proportions, they have warned the more shadowy intelligence agencies need "a dose of sunshine" to lift public confidence in privacy protections further deteriorated during the COVID-19 pandemic.

Home Affairs Minister Karen Andrews introduced another national security bill to the lower house on Thursday morning, which would implement a number of the changes put forward in a landmark review by former ASIO boss Dennis Richardson.

The bill, which amends nine pieces of legislation, would finally allow for the Australian Signals Directorate to undertake signals intelligence collecting on people within the country without the need of a warrant if there is an imminent risk to life.

It will also provide the signals agency with the ability to undertake domestic spying on suspected terror suspects, and collect intelligence in conjunction with the Australian Defence Force for military operations with ministerial authorisation.

The agencies, which also includes ASIO, Australian Geospatial-Intelligence Organisation and the foreign-focused Australian Secret Intelligence Service, will be required to publicly publish privacy rules on their sites.

The security and intelligence parliamentary committee will be able to review and scrutinise these privacy rules.

It comes more than three years after former News Corp journalist Annika Smethurst reported on a leaked memo between senior officials discussing the granting of extraordinary powers to listen in on Australians without a warrant.

Ms Smethurst's house was raided the following year, along with the alleged leaker of the document. Police last year dropped the charges.

But National Security College policy advisor Dr Will Stoltz said these proposals were very different to the initial plans for ASD first reported on in 2018.

"It's really about those quite time-sensitive, life or death, urgent moments where you need ASD to just be able to, in a matter of hours, pull together some intelligence," Dr Stoltz said.

Australian National University colleague Professor John Blaxland said the federal government, and the national intelligence community, needed to be more transparent to ensure stronger public confidence in the powerful proposed laws.

The general public had developed a "bruised and damaged image" of national security concerns following the police raids on Ms Smethurst, he said.

"If we're going to avoid adding to the momentum of the conspiracists' cause, we need to give [them] a dose of sunshine," he said.

"I think ASD needs to be more transparent much like ASIO has sought to be more transparent."