Australian Government
Department of Home Affairs

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

Parliamentary Joint Committee on Intelligence and Security

21 February 2022

Introduction

1. The Department of Home Affairs (the Department) welcomes the opportunity to make a supplementary submission to the Parliamentary Joint Committee on Intelligence and Security's (the Committee's) review of the National Security Legislation Amendment (Comprehensive Review and Other Measures No.1) Bill 2021 (the Bill). This submission addresses matters raised in the Law Council of Australia's (Law Council) submission.
2. The Department is pleased that the Law Council supports in their current form, or seeks only further supporting information for, 10 of the Bill's 14 schedules. The Law Council has also raised issues of a technical nature with the Bill's first four schedules.
3. This submission provides the further information requested by the Law Council to explain the measures in the Bill, including the reasons for the technical drafting decisions made in the first four schedules. In particular, this submission:
    - responds to the Law Council's 11 recommendations on Schedules 1-5, 8 and 9, and
    - addresses the Law Council's other commentary on Schedules 6, 9, 10 and 12.
4. This submission is silent on Schedules 7, 11, 13 and 14 as the Law Council raised no issues for response by the Department.
5. This submission also responds to matters raised in other submissions before the Committee, where appropriate.

Schedule 1 – Emergency authorisations

Law Council Recommendation 1 – seriousness of the risk to an Australian person under ISA s 9D

- **Proposed subsection 9D(1) or (2) of the ISA should be amended to require the agency head to be satisfied that there is a serious or significant risk to safety of an Australian person, as a precondition to issuing the authorisation (in addition to that risk being imminent).**
- **That is, the amendment should align the criteria for granting an authorisation under proposed section 9D more closely with the existing authorisation condition for emergency agency head authorisations under subparagraph 9B(2)(c)(ii) ('serious risk'), or the cancellation condition in proposed section 9D(12) ('significant risk').**

Department's response

6. First and foremost, the amendments in Schedule 1 to the Bill only apply in the very limited circumstances in which it is reasonable for the agency head to believe the Australian person would consent to intelligence being collected, if they were able to do so.
7. As part of this assessment, the agency head must have regard to the nature and gravity of the risk. It is not possible to issue an authorisation without considering the nature and gravity of the risk.
8. Making the seriousness or significance of the risk part of the authorisation *threshold*, as distinct from a consideration, could prevent authorisations from being granted for risks that are imminent but which cannot be immediately quantified. Uncertainty over the significance of the risk could prevent the emergency authorisation from being used in the precise situations it is designed for.
9. Schedule 1 includes a safeguard which ensure the authorisation cannot continue if, after being issued, it is determined that the risk is not significant. Under proposed new subsection 9D(12), the agency head must cancel the authorisation if there is no longer a significant risk to the Australian person. After receiving the emergency authorisation, the Minister must also consider whether to cancel it, and may cancel it at any time thereafter (subsection 9D(6)).
10. In situations where there is a serious risk of harm to an Australian person overseas but this risk is not imminent, the existing ministerial authorisation framework would apply.

Law Council Recommendation 2 – explicit requirement in section 9D of the ISA as to the primary purpose for which intelligence is to be produced

- **Proposed subsection 9D(1) of the ISA should be amended to provide that an agency head may only issue an authorisation if they are satisfied that the primary purpose of producing intelligence on the Australian person whose safety is at risk is to assist that person (that is, by seeking to abate the risk to the person's life or safety).**

- **If the primary objective of producing intelligence on the Australian person is, in fact, to gain insight into one or more specified risks to Australia's security, international relations or economic well-being (and the intelligence would only be used in an incidental or secondary way to assist the person) then there should be clear statutory provision that the authorisation mechanism under section 9D is not available in these circumstances. Rather, the agency should be required to proceed under the authorisation mechanisms in existing sections 9, 9A or 9B of the ISA (as applicable).**

Department's response

11. The purpose of the new emergency authorisation is to help Australians at risk in urgent circumstances. The emergency authorisation will only be available to agencies to produce intelligence on *an* Australian overseas where *that* Australian's safety is at imminent risk. Further, the authorisation can only be granted if it is reasonable to believe the person would consent to the production of intelligence.

12. In any other circumstance, agencies would need to use the existing authorisation framework in the *Intelligence Services Act 2001* (IS Act).

13. If an Australian is at imminent risk and it is reasonable to believe the person would consent, it would be appropriate to use the new authorisation, even if there are ancillary purposes. If an Australian is not at imminent risk, the new emergency authorisation provisions cannot be used, and an authorisation must instead be sought under the existing provisions.

14. In practice, if a person or entity poses an imminent risk to an Australian person, the emergency authorisation will have at least two purposes: first, to protect the Australian person, and second, to learn about the source of the threat. It would be a perverse outcome if such a situation might lead to a slower process being used, even though the person is at imminent risk and it is reasonable to believe that the person would consent. A 'primary purpose' test could introduce uncertainty as to whether the threshold has been met, potentially introducing delays and hindering agencies' ability to immediately assist Australians at risk.

Law council recommendation 3 – maximum period of effect of ISA section 9D authorisations

- **Proposed paragraph 9D(9)(a) of the ISA should be amended to provide that an authorisation issued under section 9D has a maximum period of effect of 48 hours. Proposed subsection 9D(6) should also be amended to require the responsible Minister to specifically consider whether the section 9D authorisation should be replaced with an MA under section 9 or 9A, in addition to considering whether to cancel it under proposed subsection 9D(10).**
- **In this way, the new agency head authorisation mechanism in proposed section 9D would reflect the primacy of Ministerial responsibility and accountability in the same way as the agency head authorisation mechanism in existing section 9B.**

- **Accordingly, all of the agency head authorisation mechanisms in the ISA would ensure that an authorisation given by an agency head could only remain in force until such time as the responsible Minister for the agency could determine whether to authorise the agency's intrusive intelligence collection activities.**

Department's response

15. There is no practical or legal difference between the mechanism in the Bill and the Law Council's recommendation.

16. Under the Bill, the agency head must notify the responsible Minister of the authorisation within eight hours and, within 48 hours, provide the Minister with a copy of the authorisation and a summary of facts. The Minister must, as soon as practicable thereafter, consider whether to cancel the authorisation. The Minister may also cancel the authorisation at any time after this.

17. If the Minister decides not to cancel the emergency authorisation, it is equivalent to the Minister having issued the authorisation themselves and therefore the maximum period has been aligned with other authorisations under the framework.

Law Council recommendation 4 – requirements for the issuance of ISA section 9D authorisations in relation to Australian children

- **Proposed subsection 9D(1) of the ISA should be amended to provide specific statutory requirements, at least at a high-level, in relation to authorisations to produce intelligence on an Australian child.**
- **The objective of such statutory guidance should be to remove any possibility that section 9D could be capable of authorising an ISA agency to produce intelligence on an Australian child, in circumstances in which the agency would be required to seek an authorisation under section 9, 9A or 9B of the ISA to produce intelligence on an Australian adult.**
- **In particular, there should be:**
    - **an explicit requirement for the agency head to take into account the best interests of the child, consistent with Australia's obligations under the Convention of the Rights of the Child, when deciding whether to issue an authorisation under proposed section 9D. (This should not be left solely to the general requirement in proposed paragraph 9D(2)(a) and supporting instruments such as Ministerial directions made under section 8 of the ISA, or operational policies);**
    - **specific statutory guidance on the assessment of whether there is an imminent risk to the child's safety under proposed paragraph 9D(1)(a) by reason of the child's developmental and legal status as a minor; and**
    - **specific statutory guidance on the application of the consent requirements in proposed paragraphs 9D(1)(c) and (d) in circumstances in which a child may be assessed as lacking legal capacity to consent to the production of intelligence, because of their status as a minor (as distinct to practical limitations on the ability of the agency to make contact with the person).**

Department's response

18. An emergency authorisation can only be granted if *having regard to the nature and gravity of the risk*, it is reasonable to believe that *the person would consent if they were able to do so*. Where the Australian at risk is a child, or otherwise incapable of consenting, this test would inherently involve child-specific considerations, including whether producing intelligence would be in their best interests.

19. Introducing any additional child-specific requirements into the authorisation process could introduce additional delays that hinder agencies' ability to help. Any delays could prevent the authorisation from being used in the precise situations it is designed for. It would create a perverse outcome if the legislative provisions meant it was easier to assist adults who faced an imminent risk to their safety than children in the same circumstances.

20. The threshold for obtaining an emergency authorisation is the same for adults and children. It should not be easier, or more difficult, to obtain an authorisation for one over the other.

Law Council recommendation 5 – Power of delegation in ISA subsection 9D(14)

Preferred option

- **The agency head's power of delegation in proposed subsection 9D(14) of the ISA should be amended to exclude the power to issue an emergency authorisation under proposed subsection 9D(2).**

Alternative option

- **If the Committee is persuaded that ISA agency heads should be able to delegate their power to issue authorisations under proposed subsection 9D(2), the power of delegation in proposed subsection 9D(14) should be amended to further limit the class of prospective delegates.**
- **This class should be defined as staff members of the agency (excluding contractors or consultants) who hold a position which is classified as a prescribed level of seniority, potentially in an analogous manner to the definition of a 'senior position holder' in section 4 of the Australian Security Intelligence Organisation Act 1979 (Cth) (ASIO Act).**

Department's response

21. There is a strong operational need for this power to be devolved to ensure that appropriate decisions can be made quickly where there is a imminent threat to an Australian person's safety. The new emergency authorisation is for the limited scenario in which an immediate or near-immediate response is required. Introducing additional delay into the authorisation process could make the new authorisation framework unworkable and potentially defeat its purpose by putting Australians at further risk. Crucially, the scenario is also limited to where it is reasonable to believe that the person would consent to the production of intelligence if they were able to do so.

22. Overseas staff operate in different time zones, with differing levels of seniority. Seeking the approval of the agency head, or another senior officer back in Australia, could cause undue delay and result in lost opportunities to prevent or lessen harm or risk to an Australian person's safety. Officers in the field are often best placed to assess the immediacy of the threat, and the most effective way to gather intelligence to assist the Australian person whose safety is at risk.

23. In practice, it is expected decisions would usually be made by the most senior officer in the relevant location. However, the level of these officers can differ between different locations. The delegation ensures it is possible for appropriately qualified individuals in the relevant location and timezone to make decisions if required.

24. There are a number of further safeguards in the Bill permitting a reassessment of whether the authorisation was appropriate. For example:

    - the agency head must cancel the authorisation if it is determined the risk is not significant
    - the Minister must be notified within 48 hours and must consider whether to cancel the authorisation, and may cancel the authorisation at any time thereafter, and
    - delegates must comply with any written directions given by the agency head under the delegation.

25. Further, in the unlikely circumstances where no senior officer can be located, the operational need for approval by a junior officer to immediately act in potentially life or death situations, coupled with the strong safeguards and the need for fast consideration by the agency head and Minister, outweighs any limited risks posed by junior staff being delegated this power in these specific set of circumstances where Australians are at risk.

NSW Council for Civil Liberties Recommendation 5:

- **Before an emergency authorisation is granted, all reasonable efforts should be made to contact the relatives of the affected Australian person to seek their consent on behalf of the Australian person if it is not possible to obtain the consent of the person themself.**

Department's response

26. The new emergency authorisation is designed to help Australians at risk in urgent circumstances. Any requirement to seek the consent of a person's relatives beforehand would introduce delays into time critical situations. It would be unlikely to be quicker to seek consent from relatives than to seek a ministerial authorisation, or an emergency authorisation from the agency head under the existing emergency provisions in section 9B. This is particularly the case given that, before relatives could be contacted, they would need to be identified and contact details obtained – a potentially time consuming process.

27. Consent in this context is also something that would need to be given personally, rather than by a family member who might not have authority to give such consent. For this reason, the provision has been framed to only be used where it is reasonable to believe the person *themselves* would give consent.

Schedule 2 - Authorisations relating to Counter-Terrorism

Law Council recommendation 6 – circumstances in which a person is taken to be 'involved with' a terrorist organisation under proposed ss 9(1AAA) and 9(1AAB) of the ISA

- **Consideration should be given to exhaustively defining the circumstances in which a person is taken to be 'involved with' a terrorist organisation for the purpose of the class authorisation ground in proposed subsection 9(1AAA). In particular, consideration should be given to transforming the illustrative list of circumstances in proposed subsection 9(1AAB) into an exhaustive definition, noting the significant breadth of those activities.**
- **In any event, consideration should be given to amending the deemed grounds of 'involvement' in proposed paragraphs 9(1AAB)(e) and (f) so that they only cover the provision of 'non-financial support' to a terrorist organisation, or 'advocacy' for and on behalf of that organisation which is likely to be material to the organisation's engagement in, or capacity to engage in, terrorism-related activities.**

Department's response

28. Certain activities, although seemingly innocuous in isolation, may be valuable pieces of a larger overall intelligence picture. This is particularly true where methodologies employed by terrorists have become more discreet than in the past and methods for obfuscation of activities more sophisticated. A non-exhaustive definition allows ministers greater flexibility in determining how they define an individual class authorisation.

29. The purpose of this amendment is to enable agencies to more efficiently and effectively collect intelligence, particularly in relation to threats to Australia's national security. Setting out an exhaustive definition of what it means to be 'involved with' a terrorist organisation could prevent agencies from collecting valuable intelligence. The fact that a class authorisation can only be relied on to collect intelligence on an Australian person who *is, or is likely to be,* involved with a listed terrorist organisation already provides a high threshold to meet in terms of collecting intelligence on an Australian person. Limiting the types of involvement that an Australian person can have with a listed terrorist organisation, before an agency can collect intelligence on that person, would be an unnecessary limitation on the ability of agencies to collect intelligence on security threats. It could also lead to the need for further amendments to legislation to introduce new grounds in response to emerging threats and future operational needs.

30. Limiting the deemed grounds of involvement in paragraph 9(1AAB)(e) to cover only non-financial support would materially hinder agencies' ability to collect intelligence on suspected terrorists. Financial flows are critical to the functioning of terrorist organisations and excluding the ability to obtain a class authorisation to collect intelligence on those involved in funding a terrorist organisation could result in valuable intelligence being lost.

31. Similarly, limiting the deemed grounds in paragraph 9(1AAB)(f) to advocacy that is 'material to the organisation's engagement in… terrorism related activities' would preclude agencies from producing intelligence whose involvement may have only just started and may yet be minor, but could nonetheless result in valuable intelligence. It would also distort the threshold: what is material to a smaller terrorist organisation may not be material to a larger organisation, resulting in a threshold that would in practice operate differently for different organisations.

32. The reforms also include a new oversight mechanism. Agency heads will be required to:

    - ensure a list is kept that:
        - identifies each Australian on whom activities are being undertaken under the class authorisation
        - gives an explanation of the reasons why that person is a member of the class, and
        - includes any other information the agency head considers appropriate
    - provide the list to the Director-General of Security, and
    - make the list available to the Inspector-General of Intelligence and Security (IGIS) for inspection.

33. Agencies are also required to report to the Minister on the activities under the class authorisation, to ensure that agencies are accountable for their activities.

34. Class authorisations will be subject to IGIS oversight. The IGIS has the power to examine both the legality and the propriety of action taken by intelligence agencies in the performance of these functions, including how and who they determine to be members of the class.

Schedule 3 – Authorisations in support of the Australian Defence Force

Law Council recommendation 7 – Maximum period of effect for Defence Minister's requests to provide assistance to the ADF in overseas military operations

- **Paragraph 9(1)(d) of the ISA should be amended to apply a six-month maximum period of effect to written requests made by the Defence Minister for an ISA agency to provide assistance to the ADF in support of military operations outside Australia.**

Department's response

35. The primary safeguard is that ministerial authorisations themselves are only valid for six months at a time. Requests for assistance for the Australian Defence Force (ADF) may relate to matters where the timing is unknown, such as a long-term war or conflict. A six-month renewal of the request for assistance would constitute an unnecessary additional burden for an arbitrary timeframe, when authorisations must already be reconsidered each 6 months.

36. Each time an authorisation is granted, the Minister must be satisfied of a range of matters to issue an authorisation, including that the activities are necessary for the proper performance of the agency's functions and that the nature and consequences of acts done in reliance of the authorisation are reasonable. As a matter of practice, the relevant Minister will also take into account whether those matters, including the Defence Minister's written request, accurately reflect contemporary circumstances. It would not be possible to satisfy the thresholds for seeking a class authorisation if the underlying request from the Defence Minister was outdated and no longer relevant.

37. The Defence Minister is also the minister responsible for the Australian Signals Directorate (ASD) and Australian Geospatial-Intelligence Organisation (AGO). The Minister for Foreign Affairs, who would also be fully across Australia's foreign military operations, is responsible for ministerial authorisations for the Australian Secret Intelligence Service (ASIS), and would be aware if the Defence Minister's request was no longer relevant.

38. Implementing a six-month maximum period of effect to written requests made by the Defence Minister would also not be viable as this would reduce the standard maximum duration of a ministerial authorisation, which is six months, as an authorisation is not likely to be granted immediately upon request. Given this, the timeframe for the renewal request would also need to be brought forward, meaning again that less intelligence from the initial authorisation could be included to justify a renewal.

39. Robust safeguards continue to apply. The IGIS will continue to oversee agency activities, to ensure they act legally and with propriety, comply with ministerial guidelines and directives and respect human rights. The Defence Minister may cancel or revoke the request at any time.

Other Law Council commentary

126. The Law Council suggests that the credible possibility of a practical expansion of intelligence collection activities in this context would provide a timely opportunity for the Committee to seek information from relevant ISA agencies about their practices in relation to providing intelligence to the ADF in circumstances which may enable individuals (whether Australians or otherwise) to then be targeted for the use of lethal force.

127. Ideally, unclassified information about contemporary practices to ensure human rights compliance should be placed on the public record, to provide the public and the Parliament with tangible assurances about them. There may also be value in the Committee pursuing this matter in further detail with agencies via classified evidence as needed, and reporting its conclusions to the Parliament.

Department's response

40. IS Act agencies must comply with applicable legal obligations and direction when providing intelligence to the ADF. IS Act agencies do not participate in the ADF decision-making process for the application of lethal force.

41. The ADF is responsible for making lawful targeting decisions on operations, including when using information provided by an IS Act agency. IS Act agency intelligence is vital in supporting ADF operations to assist the ADF to make informed targeting decisions. This enables the ADF to be satisfied that their decisions to apply lethal force are based upon the most accurate and timely information available.

42. Targeting decisions are made by the ADF in accordance with Government direction, and in compliance with domestic and international legal obligations (in particular the Laws of Armed Conflict). The Laws of Armed Conflict provide applicable rules and safeguards for the conduct of targeting activities by the ADF in wartime.

43. Consistently with the Laws of Armed Conflict, the ADF has robust internal mechanisms and procedures governing targeting activities, including Rules of Engagement and Targeting Directives.

44. Further, consistent with the Government response to recommendation 60 of the Comprehensive Review of the Legal Framework of the National Intelligence Community (Comprehensive Review), IS Act agencies advise their minister, when seeking a ministerial authorisation to cooperate with the ADF or ASIS, that intelligence provided through the authorisation may be used to achieve a direct effect on an Australian person.

Schedule 4 – Authorisations for producing intelligence on Australians

Law Council recommendation 8 – uncertain meaning of 'covert and intrusive' activities in new subsection 8(1B) of the ISA

- **The Government should provide further explanation of the policy intent, in relation to whether the types of activities discussed at paragraphs [137]-[156] of this submission are intended to be characterised as 'covert and intrusive' and therefore subject to the requirement to obtain prior Ministerial authorisation. (That is, geospatial intelligence collection, human intelligence collection including the use of covert human intelligence sources, accessing telecommunications data, and interrogating bulk personal datasets.)**
- **Consideration should be given to amending the Bill to provide further statutory guidance about the meaning of the expression 'covert and intrusive' in proposed subsection 8(1B) of the ISA. This could potentially include some of the relevant factors set out in section 26 of the Regulation of Investigatory Powers Act 2000 (UK).**

NSW Council for Civil Liberties Recommendation 8

- **To ensure accountable oversight and control as a means to ensure the ethical surveillance of citizens, surveillance and intelligence productions relating to Australians should require ministerial authorisation where there is the potential for interference with a person's civil rights or liberties.**

Department's response

45. The intent of the reforms is to provide clarity on what it means for an IS Act agency to produce intelligence. It will make clear that, consistent with current practice, agencies do not have to seek a ministerial authorisation for actions that are not 'covert and intrusive'.

46. The expression 'covert and intrusive' reflects the way agencies already interpret the requirement to seek ministerial authorisations. While the amendment will provide greater clarity to agencies, the concept is not exhaustively defined, because intelligence capabilities are continually evolving and prescriptive definitions quickly become obsolete. Whether in a particular case an activity will meet the definition depends on the individual circumstances. An attempt to define the term further risks omitting instances which should in the particular circumstances be the subject of a ministerial authorisation.

47. To the extent there is any doubt about whether an action is covert and intrusive, IS Act agencies would seek an authorisation for the avoidance of doubt, as they already do in practice.

48. Agency assessment of whether the threshold applies is and remains subject to the oversight of the IGIS. Agencies will develop greater clarity on the meaning of 'covert and intrusive' through a combination agency practice and IGIS oversight.

Schedule 5 – ASIS cooperating with ASIO

Law Council recommendation 9 – further information about the necessity and implications of the proposed repeal of paragraph 13B(1)(b) of the ISA

- **Further information should be provided about the necessity of the proposal to enable ASIS to undertake domestic intelligence collection under section 13B of the ISA. It should address the following matters:**
    - **the reasons that it is not considered practicable for ASIO to utilise the operational assistance of individual ASIS staff members as secondees to ASIO ('ASIO affiliates'), and why ASIS should be permitted to act in its own legal capacity (with its own operational command and governance arrangements);**
    - **how risks of overlap, conflict, inconsistency or lack of coordination—which may arise from two agencies operating domestically to collect the same kinds of intelligence—will be managed in practice; and**
    - **why there is no Ministerial involvement in the approval process for ASIS to collect domestic security intelligence in support of ASIO under section 13B of the ISA (as amended); notwithstanding that ASIO requires ministerial approval under section 27B of the ASIO Act to collect foreign intelligence in Australia (even though the collection activities do not require authorisation under a warrant).**

Department's response

49. Schedule 5 to the Bill implements the Government response to recommendation 57 of the Comprehensive Review.

50. While the Comprehensive Review did recommend against changes to the cooperation regime, contending that any problems could be mitigated by focusing on collaboration, its primary concern was that ASIS should continue to require a written notice from ASIO that ASIS's assistance is required. The Comprehensive Review described its key concern as follows:

> 22.64 Expanding section 13B to apply to ASIS's activities onshore *could increase the instances in which ASIS undertakes activities without prior request* [emphasis added], relying on a reasonable belief that it is not practicable in the circumstances for ASIO to make the request of ASIS. In our view, it would only be appropriate in exceptional circumstances for ASIS to operate onshore without prior request from ASIO, and such circumstances were not put to the Review.

51. The Comprehensive Review did not explicitly consider whether onshore cooperation should be permitted in circumstances where a written notice would be mandatory.

52. Consistent with the Government response, the reforms included in the Bill address this concern by ensuring that ASIS cannot act unilaterally. The proposed amendments will always require ASIS to have a written notice from ASIO that ASIS's assistance is required onshore. The urgent circumstances exemption for offshore activities, which permits ASIS to act without written notice from ASIO where it cannot be practicably obtained in the circumstances, does not apply to onshore activities.

53. This amendment will enhance cooperation between the agencies in support of ASIO's functions and enable Australia to better detect and defeat threats to security.

54. ASIS is required to report to the Minister for Foreign Affairs on any activities under section 13B of the IS Act each financial year.

Why a secondment arrangement is not practicable

55. The purpose of section 13B is to enable ASIO to request assistance from ASIS to support ASIO in the performance of its functions. It is not restricted to assistance from *individual ASIS officers*, but rather assistance from ASIS as an organisation.

56. Section 13B has operated effectively to support cooperation between the two agencies for many years. The proposed amendments in Schedule 5 build on this existing cooperation framework, and simply removes the geographic limitation that currently restricts section 13B cooperation to activities outside of Australia only. It does not create a 'new cooperative scheme', as the Law Council describes it (paragraph 175 of its submission).

57. A secondment arrangement for this objective would be unworkable and impractical. Secondments, and the procedures that enable them, are designed for long-term exchanges rather than short-term operational objectives. The cooperation framework proposed in the Bill would permit cooperation at short notice. This type of assistance would not be possible under the Law Council's proposal.

Risk of overlap, conflict, inconsistency and lack of coordination

58. ASIS can only undertake activities to produce security intelligence on an Australian person inside Australia *at ASIO's written request*. This does not give rise to any risk of overlap, conflict, inconsistency and lack of coordination, as by definition the activities of ASIS are at ASIO's request and in support of ASIO's functions.

59. ASIO would clearly set the operational parameters of the cooperation arrangements to mitigate this risk. For example, existing subsection 13B(2), which is not affected by the Bill, permits ASIO to specify conditions under which ASIS is to undertake its activities.

No ministerial involvement

60. The reforms will allow ASIS to cooperate with ASIO onshore in relation to activities for which ASIO does not require a warrant or any other ministerial authorisation. These will mirror the existing arrangements for cooperation offshore.

61. It would be needlessly excessive for ASIS to require ministerial approval for those activities that it would not be otherwise unlawful to perform, and for which ASIO does not require ministerial authorisation or a warrant to perform itself.

62. This can be contrasted with ASIO performing foreign intelligence functions to assist other agencies, which require either a warrant or a ministerial authorisation (under sections 27A and 27B of the ASIO Act) in order to perform this function.

Schedule 6 – AGO cooperating with authorities of other countries

Other Law Council comment

> **[211] … the Committee may wish to make inquiries of AGO about its supporting governance framework for assessing whether cooperation with a foreign authority is 'significant', particularly in the context of assessing any risk that AGO's cooperation may enable the government of the foreign country (or the governments of other countries) to engage in human rights violations. The Committee may also wish to consider recommending revision of the human rights statement of compatibility in the Explanatory Memorandum to the Bill to specifically address this matter, noting the suggestion in the present version that the measures in Schedule 6 do not engage any human rights.**

Department's response

63. AGO's functions under paragraphs 6B(1)(e), (ea) and (h) of the IS Act are non-intelligence functions and do not involve covert or intrusive activities. AGO's non-intelligence functions are concerned with hydrographic, meteorological etc. data and technologies, and do not relate to individuals or individuals' rights.

64. Human rights are a key consideration for all AGO international engagement. This provision related to non-intelligence data that supports efforts such as Humanitarian Assistance and Disaster Recovery, and the safety of life at sea work of the Australian Hydrographic Office.

65. To the extent that any cooperation would affect individuals or individual rights, such as providing assistance to emergency response functions, AGO is subject to the same human rights obligations as the rest of the Australian Government.

66. In addition, IGIS will oversee AGO's supporting governance framework for assessing whether cooperation with a foreign authority is 'significant', ensuring AGO acts legally, with propriety and consistent with human rights.

67. Under the proposed amendments, AGO will continue to be required to report to the Minister for Defence and the IGIS on any significant non-intelligence cooperation undertaken with authorities of other countries.

68. AGO is currently undertaking further work to define when cooperation is 'significant', in consultation with the IGIS and other IS Act agencies, to be provided to the Minister for Defence for consideration.

Schedule 8 – Suspension of travel documents

Law Council recommendation 10 – Necessity of proposed doubling of suspension timeframe

- **Further information should be provided about the necessity of the proposal to double the maximum period of interim suspension of Australian or foreign travel documents.**
- **In particular, further information should be provided as to why a permanent doubling of the statutory maximum period of effect is needed in preference to taking administrative action (such as increasing and re-prioritising resources) in order to meet the 14-day time period. This should include explanation of why any spike in current caseload is anticipated to be ongoing or sufficiently long-term as to justify statutory intervention (which will last indefinitely).**
- **While it may be necessary for the Committee to obtain such evidence in camera, by reason of its classified nature, consideration should be given to placing on the public record as much additional information as possible about the necessity of the proposed amendments, as distinct to the gains in convenience or efficiency.**

Department's response

69. ASIO's operational experience has demonstrated the current 14 day suspension period is often not sufficient for ASIO to undertake all appropriate investigative steps, before preparing a security assessment, including:

    - comprehensively reviewing its intelligence holdings on the person
    - planning and undertaking intelligence collection activities, including activities that require the Director-General of Security to request warrants from the Attorney-General
    - requesting information from Australian and foreign partner agencies
    - assessing all such information, to produce a detailed intelligence case, and

- where possible, interviewing the person to put ASIO's concerns to them, consistent with the requirements of procedural fairness, and assessing their answers.

70. Given the gravity of the decision to permanently cancel a person's Australian passport or foreign travel document, it is critical that ASIO has sufficient time to undertake all necessary and appropriate investigative steps, such that the decision to cancel is both procedurally fair and based on correct and sufficient information.

71. The reform will allow the time required for assessments to be made in more complex cases, including where the subject was previously unknown to ASIO.

72. The alternative would be that passports have to be returned before an individual's threat to security can be assessed, with a potentially disproportionate impact on security compared to the inconvenience of a further 14 days' suspension.

73. The amendments do not address a specific spike in case-load. Rather, they address the reality of how long it takes to properly perform a security assessment. Additional resources will not necessarily reduce the time it takes to conduct a security assessment. Additional resources will not materially reduce the time it takes to conduct a security assessment. The work involves a structured, sequential, and methodical approach across a range of investigative and analytical activities – additional resources would not reliably expedite this process, so additional time is required .

Schedule 9 – Online activities

Law Council recommendation 11 – implementation of the Committee's recommendation 10 on the SOCI Bill, in relation to ASD, ASIS and AGO

- **The Government should implement recommendation 10 in the Committee's advisory report on the SOCI Bill, in relation to the expansion of the immunity in Division 476 of the *Criminal Code Act 1995* (Cth) (Criminal Code) in favour of ASD staff members, and the proposed expansion in favour of ASIS and AGO staff members.**

Department's response

74. The Government responded to recommendation 10 of the Committee's advisory report through its revised *Security Legislation Amendment (Critical Infrastructure) Act 2021* (SLACI Act), which was passed by the Parliament in November 2021.

75. The amendments proposed in the Bill for ASIS and AGO are consistent with the amendments extending immunity to ASD in the SLACI Act. It is important for all agencies to have the same immunity on a consistent basis, as recommended by the Comprehensive Review.

76. The proposed amendments in Schedule 9, including those in the SLACI Act, did not create a new immunity framework. Prior to the SLACI Act, ASD, AGO and ASIS all had the same immunity from the computer offences in the *Criminal Code Act 1995* for acts done outside Australia. Consistent with recommendation 74 of the Comprehensive Review, this immunity is extended to circumstances where officers reasonably believe the acts are done outside Australia, whether or not they in fact take place outside of Australia. This has already occurred in relation to ASD through the SLACI Act, and the Bill seeks to mirror this for AGO and ASIS.

77. The proposed amendments also align the immunity provisions in the Criminal Code with the general protections available to AGO, ASD and ASIS under section 14 of the IS Act, such that the same provisions apply to each agency.

Schedule 10 – Privacy

Other Law Council comment – Part 3

[227] The Law Council does not necessarily object to the enactment of those of the Schedule 10 measures which exceed the scope of recommendation 12 of the Richardson Review (noting that the latter recommendation was confined to information obtained via the performance of ONI's open source function).

[228] However, the Law Council suggests that there is a need for further explanation of the reasons for including these additional measures. For the reasons outlined below, there is also a need for further examination of their implications for the level of protection given to any confidential personal information that ONI obtains through means other than the performance of its open source function.

Department's response

78. The majority of the Assessments and Reports the Office of National Intelligence (ONI) produces under its all source analytical functions (subsections 7(1)(c) and (d)) of the *Office of National Intelligence Act 2018* (ONI Act)) are strategic in nature and do not focus on individuals.

79. The sensitive information ONI is provided with to perform these analytical functions generally comes from other intelligence agencies. This information (if it includes information about Australian persons) is communicated to ONI in accordance with the privacy regimes of those agencies and is therefore subject to existing safeguards, which could include, among other things, privacy rules, ministerial authorisations, warrants, or authorities to conduct special intelligence operations. Agency compliance with their privacy regimes is overseen by the IGIS. Part 4 of the ONI Act also includes a number of protections for the information, doucments or things another NIC agency provides to ONI.

80. Under the proposed amendments, ONI's Privacy Rules will continue to apply to sensitive information about Australians that ONI communicates for the purpose of performing its all source analytical functions. After it is received, this information is 'assembled, correlated and analysed' by ONI to 'produce the intelligence' which make up ONI Assessments and Reports. If an ONI Assessment or Report contains intelligence about an Australian person, ONI's Privacy Rules are applied to the entire Assessment or whole Report, and this will be unchanged by the Bill.

81. The amendments will ensure that ONI's Privacy Rules apply to all ONI's analytical functions and not to other information. The practical effect of this is that ONI's Privacy Rules will not apply to, for example, the communication of publicly available information (such as a news article) or administrative and staffing information. The privacy risks of communicating such information is low because this information is already in the public domain or voluntarily provided to ONI. This is consistent with the government response to recommendation 12 of the Comprehensive Review as well as the intention of privacy rules which is to ensure that the privacy of Australian persons is preserved as far as is consistent with the proper preformance by ONI of its functions (see subsection 53(3)).

Schedule 12 – Authorities of other countries

Other Law Council comment

[251] The Law Council therefore queries whether there would be benefit in also amending section 13 ONI Act to include the same clarification as that proposed in Schedule 12 in relation to the ISA. The Committee may wish to consider exploring this matter with the proponents of the Bill and ONI.

Department's response

82. The amendment to the IS Act was driven by the need for clarity when seeking ministerial authorisations for the foreign intelligence collection agencies.

83. The Government will consider similar amendments to the ONI Act should the need arise. However, noting ONI's functions and activities are much less operational in nature than most other NIC agencies, it is unlikely the need would ever arise.