Law Council of Australia

Comments on the *Minister's Guidelines to the Australian Security Intelligence Organisation*

Tabled in the Senate on 13 August 2020

Contents

Introduction

1. The Law Council of Australia welcomes the revised version of the Minister's Guidelines to the Australian Security Intelligence Organisation (**ASIO Guidelines**). The revised ASIO Guidelines became available publicly when they were tabled in the Senate on 13 August 2020 (on an 'out-of-sitting' basis).

2. The ASIO Guidelines are an important document, as they set the standards and other procedural requirements that ASIO is required to adhere to in the performance of its functions under section 17 of the *Australian Security Intelligence Organisation Act 1979* (Cth) (**ASIO Act**).

3. Under section 8A of ASIO Act, the ASIO Guidelines are administratively binding on ASIO.[1] That is, the Director-General of Security is required to ensure that ASIO complies with the Guidelines in the performance of its functions. However, non-compliance with requirements in the ASIO Guidelines does not invalidate the exercise of a power, or directly trigger a legal sanction for the individuals concerned.[1]

4. Importantly, the ASIO Guidelines provide benchmarks against which the Inspector-General of Intelligence and Security (**IGIS**) may conduct oversight of ASIO's activities and make findings and advisory recommendations to the Australian Government. Further, as a public document, the ASIO Guidelines can provide assurance to the community about the way in which ASIO performs its functions, in addition to legislative requirements.

5. Prior to August 2020, the ASIO Guidelines were last reviewed and re-issued in 2007.[2] There have been significant changes to ASIO's operating environment. This includes changes to the threat environment, rapid technological changes, and numerous expansions of ASIO's intelligence collection powers.

6. The Law Council has supported repeated recommendations of the Parliamentary Joint Committee on Intelligence and Security (**PJCIS**) for the review of the ASIO Guidelines, since at least 2014, to ensure that they are fit-for-purpose in the contemporary environment, and that the public can be assured of this matter.[3]

7. On balance, while there are many valuable improvements in the new ASIO Guidelines, several important matters remain unaddressed. The Law Council is also concerned that some aspects of the revised Guidelines are missing important details. Some provisions also appear to contain ambiguities, which may make it more difficult for the Guidelines to achieve their objective of facilitating compliance, providing clear

---

[1] ASIO Act, subsection 8A(1). See further: the Hon RM Hope, Royal Commission on Australia's Security and Intelligence Agencies, *Report on the Australian Security Intelligence Organization*, (December 1984) at 321-322. In recommending the system of ministerial Guidelines presently in section 8A of the ASIO Act, Justice Robert Hope stated that the Guidelines 'should have the status of administrative directions ... They would not be designed to confer legal rights or impose obligations' (at 321). He further described the Guidelines as being 'binding on ASIO in the sense that any action in breach of them would be in breach of a lawful ministerial direction, and the person or persons responsible for the breach would be accountable administratively. (It would be for the Attorney-General, aided by the Inspector-General, to hold ASIO to account under the Guidelines)' (at 322).

[2] *Attorney-General's Guidelines in relation to the performance by the Australian Security Intelligence Organisation of its function of obtaining, correlating, evaluating and communicating intelligence relevant to security (including politically motivated violence)*, issued September 2007.

[3] See, for example, PJCIS, *Advisory report on the National Security Legislation Amendment Bill (No 1) 2014*, (September 2014), recommendation 4.

benchmarks for independent oversight, and providing transparency and assurance to the public about the manner in which ASIO performs its functions.

Key improvements from the 2007 ASIO Guidelines

8. The revised ASIO Guidelines contain several improvements from the previous version, including:

- ***personal information***—requirements for the collection, handling, retention and destruction of personal information, including:
  - an obligation on the Director-General of Security to take all reasonable steps to apply controls to prevent the collection and processing of personal information in breach of lawful authority (such as a warrant) and to adopt and implement procedures for remediation and reporting; and
  - an obligation on ASIO to maintain policies and procedures for access to, and retention of, personal information, including periodic reviews of its holdings to determine whether retention is reasonable;[4]
- ***proportionality***—the inclusion of additional requirements to guide operational decision-making about the proportionality of particular intelligence-collection techniques, including an assessment of the impact of the collection activity on any person, and the sensitivity and volume of information collected;[5]
- ***immunities from legal liability***—an explicit requirement for relevant ASIO personnel to undertake a proportionality assessment before exercising a power to:
  - confer a civil immunity on a person who is requested to assist ASIO on a voluntary basis under subsection 21A(1) of the ASIO Act; or
  - confer a civil immunity and a limited criminal immunity from computer offences under a Technical Assistance Request (**TAR**) given pursuant to Part 15 of the *Telecommunications Act 1997* (Cth), as enacted by the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (Cth) (**TOLA Act**);[6]
- ***use of force against persons***—explicit requirements for the exercise of the power to use of force against persons under ASIO's special powers warrants, which was conferred by the *National Security Legislation Amendment Act (No 1) 2014* (Cth);[7]
- ***oversight***—explicit obligations on the Director-General of Security to ensure that the IGIS and authorised staff have effective access to all information held by ASIO, that adequate records are kept for compliance auditing purposes, and that the IGIS is given copies of certain policies required to be made under the Guidelines (concerning the use of force against persons, and the handling, retention and destruction of personal information);[8]

[4] ASIO Guidelines, Part 4, especially 13 at [4.2] and [4.3](a)(vi).
[5] Ibid, 11-12 at [3.4](f)-(h).
[6] Ibid, 12 at [3.5].
[7] Ibid, 10 at [2.14].
[8] Ibid, 6 at [1.13].

- ***breach reporting***—requirements for ASIO to include in its reports to the Attorney-General on its warrants and special intelligence operations details of any breaches of applicable legal requirements;[9] and

- ***periodic reviews***—a requirement for the ASIO Guidelines to be reviewed every three years, including in consultation with stakeholders.[10]

Omissions from the revised ASIO Guidelines

9. The Law Council is concerned that the revised ASIO Guidelines do not contain any guidance on the following, essential matters:

   - ***lawyers at interviews***—the attendance and involvement of lawyers at interviews of persons that are conducted on a voluntary basis, as the Law Council has recommended previously;[11]

   - ***categories of particularly sensitive information***—specific guidance on the collection, use, disclosure, storage, destruction or retention of categories of particularly sensitive information, such as:

     – information that is, or is likely to be, subject to client legal privilege or parliamentary privilege;

     – health information (such as medical records) and biometric information (such as fingerprints); and

     – journalistic information, such as the identity of journalists' sources, and the information provided by those sources;[12]

   - ***bulk personal data***—specific guidance on the acquisition, interrogation, retention and destruction of bulk personal datasets;[13]

   - ***TOLA Act measures***—the practical operation of all of the measures enacted by the TOLA Act, including the matters identified by the IGIS in 2018 and 2019 as requiring inclusion in at least the ASIO Guidelines, if not in primary legislation;[14]

---

[9] Ibid, 8-10 at [2.8]-[2.10].

[10] Ibid, 6 at [1.14]-[1.15].

[11] See further: Dr Vivienne Thom, Inspector-General of Intelligence and Security, *Inquiry into the attendance of legal representatives at ASIO interviews, and related matters: public report*, (January 2014).

[12] Cf *Investigatory Powers Act 2016* (UK) (**IPA**), ss 2(2)(b) and 2(5), 26-29, 55, 111-114, 131, 153-154, 194-195, and 222-223. See further the Codes of Practice made under section 241 and Schedule 7, which are published at: Home Office (UK), *Investigatory Powers Act 2016 – Codes of Practice*, (1 August 2019).

[13] A 'bulk personal dataset' refers to a dataset comprised of personal information about a very large number of individuals, the majority of whom are unlikely to be of security concern. (For example, credit card or other financial transaction records, passenger lists or travel itineraries, and drivers' licences or other identity records). These datasets are typically held on intelligence agencies' electronic systems for the purpose of analysis, by inputting specific selectors (that is, search terms or other algorithms). The intelligence value is in identifying correlations and patterns, in a way that may not be possible or feasible from individually reviewing the datasets. This is regulated legislatively in other jurisdictions, such as the United Kingdom: See IPA, Part 7, and Home Office (UK), *Intelligence services' retention and use of bulk personal datasets, Code of Practice made under Schedule 7 of the IPA*, (March 2018).

[14] See further, Inspector-General of Intelligence and Security, *Submission to the Parliamentary Joint Committee on Intelligence and Security review of amendments made by the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 (Cth),* (October 2019).

- ***foreign interference***—guidance on the interpretation and investigation of matters relevant to heads of security in addition to 'politically motivated violence',[15] and in particular, guidance on 'acts of foreign interference' within the meaning of section 4 of the ASIO Act; and

- ***targeting vulnerable persons***—guidance on exercising coercive or otherwise intrusive intelligence collection powers against vulnerable persons, including children, people with disabilities, and people who belong to minority groups.

10. The Law Council acknowledges that some of these matters may presently be dealt with in ASIO's internal, classified operational policies and procedures. However, as recent media reports of the public remarks of the Director-General of Security have noted, one of the objectives of the ASIO Guidelines is to 'reassure Australians that ASIO acts in a targeted, proportionate and ethical way'.[16] The coverage of the above matters in the ASIO Guidelines, at an appropriate level of generality for a publicly available document, would go a considerable way towards meeting that objective.

Recommendation 1—additional matters for inclusion in the ASIO Guidelines

- **The ASIO Guidelines should be further updated, as a matter of priority, to include specific guidance on the matters outlined at paragraph [9].**

Outstanding issues

11. In addition to the omission of the matters noted above, the Law Council has identified further issues in aspects of the revised ASIO Guidelines, which are directed to the following matters:

    - ***proportionality***—the absence of guidance to ASIO personnel in assessing and comparing the relative intrusiveness of different intelligence collection methods, and the omission of other relevant considerations to a proportionality assessment;[17]

    - ***immunities from legal liability***—details of the requirements for assessing proportionality in relation to the powers to confer civil immunities (and immunities from liability to computer offences) are left almost exclusively to policies, and therefore do not provide adequate transparency to the public;[18]

    - ***use of force against persons***—key details of the process for authorising persons to use force against persons under ASIO's warrants appear to be left to policies, which similarly does not provide adequate transparency to the public;

[15] ASIO Guidelines, Part 5 (politically motivated violence).

[16] Rosie Lewis, 'New rules to keep ASIO on right side of the law', *The Australian*, 17 August 2020, 1 (quoting the Director-General of Security, Mr Mike Burgess).

[17] ASIO Guidelines, 11 at [3.4].

[18] Ibid, 12 at [3.5]-[3.6].

- ***periodic review***—the revised Guidelines do not guarantee consultation with civil society, or require reviews to be conducted in public to the greatest possible extent, or require the publication of a report documenting key conclusions;[19]

- ***breach reporting***—there are some apparent ambiguities in the drafting of the requirement for ASIO to report to the Attorney-General on action that required authorisation under a warrant, where no such warrant was obtained;[20]

- ***oversight***—the requirement for ASIO to give copies of certain policies to the IGIS does not extend to policies governing the powers to confer civil immunities under section 21A of the ASIO Act, or civil or limited criminal immunities pursuant to TARs issued under Part 15 of the Telecommunications Act;[21] and

- ***retention of personal information***—there are some apparent ambiguities in the requirements for ASIO to implement policies requiring personal information to be destroyed if it is not, or is no longer, relevant to security.[22]

Proportionality

12. Paragraph [3.4] of the ASIO Guidelines expands the factors that ASIO must consider when assessing the proportionality of its proposed intelligence collection activities. The revised ASIO Guidelines add the factors at paragraphs [3.4](f)-(h), namely:

    - the likely impact on any person of using the technique;
    - whether the person has consented to the use of that technique; and
    - the sensitivity and volume of the information being collected.

13. These factors are additional to the matters in paragraphs [3.4](a)-(e), which were included in the previous version of the Guidelines. Importantly, paragraph [3.4](d) requires ASIO, wherever possible, to use the least intrusive techniques before resorting to more intrusive techniques.

14. While these additional factors are valuable inclusions, the Law Council considers that there are several limitations in the guidance provided in paragraph [3.4]. In particular:

    - ***assessment of relative intrusiveness of different techniques***—there is no guidance, at a level of generality appropriate for inclusion in public materials, on how to assess and compare the degree of intrusion of different intelligence collection methods. Nor is there a requirement for ASIO to make classified policies to guide its operational decision-making on matters of detail that are not able to be included in publicly available Guidelines;

    - ***identifying limitations on human rights***—there is no guidance in determining what constitutes an 'intrusion', by reference to the specific human rights that an intelligence collection technique will, or may, engage (by limiting). ASIO's

[19] Ibid, 6 at [1.14]-[1.15].

[20] Ibid, 8-9 at [2.8](d) and [2.9](c).

[21] Ibid, 6 at [1.13](c). This requirement only refers to the policies made under [2.15] (use of force against persons) and [4.3] (personal information). It does not refer to the policies required to be made under [3.6] (conferral of immunities by making section 21A requests or giving TARs).

[22] Ibid, 13-14 at [4.3].

activities will, almost invariably, limit the right to privacy. However, ASIO's different collection powers may engage additional rights. For example:

- ASIO's decision-making about who is targeted and how they are targeted may engage the rights to equality and non-discrimination;
- ASIO's compulsory questioning powers will engage the rights to liberty and security of the person, and the right to a fair trial; and
- the targeting of vulnerable persons may engage specific rights, such as the rights of the child and the rights of persons with disabilities; and

- ***other relevant considerations***—the factors specified at paragraphs [3.4](a)-(h) do not cover other essential considerations in making a proportionality assessment, including:
  - an assessment of the anticipated significance of the particular intelligence sought to be collected to the particular investigation or inquiry; and
  - an assessment of the significance of the particular investigation or inquiry to the overall national interest.

Recommendation 2—mandatory considerations in assessing proportionality

- **The guidance on assessing proportionality in paragraph [3.4] of the ASIO Guidelines should be amended to include the additional requirements set out at paragraph [14].**

Immunities from legal liability

15. The Law Council welcomes the inclusion of paragraph [3.5] of the ASIO Guidelines. It requires relevant decision-makers within ASIO to expressly consider the proportionality of a proposal to confer a civil immunity on persons who provide voluntary assistance to ASIO under subsection 21A(1) of the ASIO Act; or a civil immunity and criminal immunity from computer offences under a TAR.

16. However, there are two limitations in this requirement (explained below) which should be addressed through amendments to the Guidelines.

Assessment methodology and transparency

17. First, paragraph [3.5] does not provide meaningful guidance on how proportionality must be assessed in the specific and unique context of exercising the extraordinary power to confer an immunity from legal liability. This is left almost entirely to policy, pursuant to the obligation on the Director-General of Security under paragraph [3.6] to maintain policies in respect of the matters at paragraph [3.5].

18. This does not provide adequate transparency to the public. There are no requirements for these policies to be published (whether in full, or in abridged and de-classified form, to the extent possible within the requirements of security). Further, there are no requirements for consultation in the development of these policies, including with relevant oversight bodies and key civil society stakeholders.

Recommendation 3—transparency of requirements for the conferral of immunities

- **Paragraph [3.6] of the ASIO Guidelines should be amended to provide further, direct guidance about the assessment of proportionality in decision-making about the exercise of ASIO's powers to confer immunities.**
- **Alternatively, paragraph [3.6] of the ASIO Guidelines should be amended to require the policies made under that paragraph to be:**
  - **(a) published in full, or in part to the maximum possible extent, consistent with the requirements of security; and**
  - **(b) the subject of consultations, including with key civil society stakeholders, as well as oversight bodies.**

Assessment of impacts on third parties

19. Secondly, the limited guidance provided in paragraph [3.5] of the ASIO Guidelines requires the decision-maker to consider 'the seriousness of any offence or conduct to which the immunity may apply and the impact on **innocent parties**' (emphasis added). The intended meaning of the expression 'innocent parties' is not explained. This risks creating confusion among members of the public about ASIO's functions.

20. The Law Council is concerned that references in the ASIO Guidelines to a person's 'innocence' are incompatible with ASIO's functions as an intelligence agency. The determination of criminal guilt is a judicial function. The investigation and enforcement of a suspected offence against a law of the Commonwealth or a State or Territory is properly the function of the relevant law enforcement agencies of each polity, which do not include ASIO.[23]

21. The expression 'innocent parties' in paragraph [3.5] of the ASIO Guidelines may be intended to denote persons who are **not** of security interest to ASIO and are not the targets of its security investigations. If this is the intended interpretation, the Law Council considers that this is an unjustifiable limitation of the scope of the mandatory proportionality assessment in paragraph [3.5].

22. That is, there is no rational reason that decision-makers should not be required to consider the potential for the voluntary assistance sought to cause loss, harm or damage to non-targets **as well as** to persons who are suspected of having engaged in activities that are prejudicial to security, and the consequent extinguishment of their rights to remedies.

23. A security investigation by ASIO is not a law enforcement investigation that is intended to result directly in punitive outcomes against the targets, such as the imposition of criminal sanctions. Further, a person could be the target of a security investigation by ASIO because they have unknowingly or unwittingly acted as the conduit for others to carry out prejudicial activities. This may occur in the case of communications service providers and other businesses who provide services to the public, including individuals who may be using those services to engage in activities that are prejudicial

[23] See further, ASIO Act, subsection 17(2) and paragraph 20(a), which make clear that ASIO's functions do not extend to matters of law enforcement.

to security. It is also possible that this may occur in the case of vulnerable persons, including children, who are exploited by persons of security concern.

24. The drafting of paragraph [3.5] to single out an assessment of the impacts of an immunity on 'non-targets' to the exclusion of 'targets' may mean that the potential impacts on targets are not considered adequately or consistently in decision-making about the potential exercise of powers to confer immunities.

25. The Law Council is particularly concerned about this risk in relation to ASIO's power to confer civil immunities under subsection 21A(1) of the ASIO Act, which is extremely broad. Subsection 21A(1) confers immunity from civil liability on any person who complies with a request from ASIO to provide any form of assistance, for the purpose of ASIO performing any of its functions.

26. This immunity is capable of covering **any form** of conduct, and is subject only to exclusions of conduct that would constitute an offence, or conduct that causes significant loss of, or damage to, property. The power to confer a civil immunity under subsection 21A(1) does not exclude conduct that causes serious personal injury, which does not constitute an offence. (For example, the tort of negligence may cause death or permanent disability. However, the civil thresholds applying to the tort of negligence fall far short of the criminal fault elements of intention or recklessness that apply to most offences against the person. Hence, the statutory exclusion of conduct constituting an offence is too narrow.) Section 21A of the ASIO Act also does not clearly exclude from the civil immunity conduct that causes significant financial loss without damage to physical property (such as financial loss suffered due to the disruption of a business supply chain).[24]

27. Consequently, a comprehensive assessment of proportionality is essential in relation to this power. (It is also notable that the third Independent National Security Legislation Monitor, Dr James Renwick CSC SC, found that the scope of the civil immunity in subsection 21A(1) of the ASIO Act was disproportionate to the security objectives to which it was directed, and it should be limited to persons who provide information to ASIO, rather than covering any or all acts of assistance.)[25]

28. In effect, the Law Council suggests that paragraph [3.5] of the ASIO Guidelines should require authorising officers to perform due diligence in taking steps to identify the reasonably foreseeable impacts on other persons of the assistance being requested. In addition to ensuring the proportionality of any limitations placed on third parties' rights to remedies, this requirement would demonstrably promote sound risk management, and give the public confidence about ASIO's practices.

Recommendation 4—consideration of third-party impacts of an immunity from legal liability, as part of a proportionality assessment

- **Paragraph [3.5] of the ASIO Guidelines should be amended to remove the expression 'innocent parties' and require ASIO officers to consider the impact of the immunity proposed to be conferred on <u>all persons</u>.**

[24] Ibid, paragraphs 21A(1)(d) and (e).

[25] James Renwick CSC SC, Independent National Security Legislation Monitor, *Trust but verify: a report concerning the Telecommunications and Other Legislation Amendment (Assistance and Access) Act and related matters* (June 2020), recommendation 19. (See also recommendations 20-22.)

Use of force against persons under special powers warrants

Training requirements

29. Paragraph [2.13] of the ASIO Guidelines requires the Director-General of Security to 'take all reasonable steps to ensure that persons … who are authorised to use force against a person under an ASIO warrant are appropriately trained'.

30. While the emphasis on training is important, the Law Council considers that this requirement does not provide an adequate level of protection against the risk of the misuse of force against persons. The requirement in paragraph [2.13] does not impose any administrative conditions on the exercise of the power in section 24 of the ASIO Act to authorise people to exercise authority under ASIO's special powers warrants (and therefore use force against persons under those warrants).

31. The Law Council would prefer to see a stronger safeguard in the ASIO Guidelines in relation to the approval of persons to use force pursuant to special powers warrants. Such a safeguard should provide that:

    - the Director-General or other approving officer **cannot** authorise a person under section 24 of the ASIO Act to exercise authority under a special powers warrant, **unless** that person has satisfactorily completed appropriate training in the use of force against persons; or

    - if a person has not satisfactorily completed appropriate training, only a **partial** section 24 authorisation can be given, which authorises a person to exercise authority under a warrant, **excluding** the power to use force against persons.

Recommendation 5—strengthening authorisation requirements for the use of force

- **Paragraph [2.13] of the ASIO Guidelines should be amended to require the Director-General of Security to implement procedures that prevent a person from being authorised under section 24 of the ASIO Act to exercise authority under a special powers warrant, unless:**

  (a) the person has been appropriately trained in the use of force against persons; or

  (b) the authorisation given under section 24 of the ASIO Act excludes authorisation to exercise the power to use force against persons. (That is, the person is only authorised to exercise a sub-set of the powers conferred by a special powers warrant, which do not include the power to use force against persons).

Presumption of 'appropriate training' in the use of force against persons

32. Paragraph [2.14] of the ASIO Guidelines states that the Director-General of Security is entitled to presume that the following persons are 'appropriately trained' to use force against persons:

    a. sworn members of the Australian Federal Police or a police force of a State or Territory; and

b. other Commonwealth, State or Territory officials who would ordinarily be expected to use force as part of their duties.

33. The Law Council is concerned that the classes of persons covered by paragraph [2.14](b) are too broad and vaguely defined for the purposes of a general presumption in favour of people who are taken to be 'appropriately trained' in a matter as significant as the use of force against persons. In particular:

- paragraph [2.14](b) is not limited expressly to officials who would ordinarily be expected to use force **against persons,** and may be open to interpretation as including officials who are only authorised, and ordinarily expected, to use force **against things**; and

- the scope of the 'presumption of appropriate training' in paragraph [2.14](b) will vary according to the scope of other Commonwealth, State and Territory legislation (both present and future) that confers powers on officials to use force. There may be unintended consequences if any such legislation is overly broad in the classes of officials who are authorised to use force.[26]

34. The Law Council acknowledges that paragraph [2.14](b) of the ASIO Guidelines operates as a presumption rather than a direct authorisation of Commonwealth, State or Territory officials to use force. The Law Council also acknowledges that paragraph [2.15] requires the Director-General to maintain policies about training in relation to the use of force against persons under ASIO's warrants and the general law of self-defence.

35. However, the Law Council submits that the ASIO Guidelines should directly place an onus on the Director-General to take all reasonable steps to satisfy themselves that persons other than sworn police officers are, **in fact**, appropriately trained in the use of force against persons **before** they can be authorised to exercise authority under one of ASIO's warrants (and therefore use force against persons).

Recommendation 6—clarification of the way in which the Director-General may apply the 'presumption' of appropriate training in the use of force against persons

- **Paragraph [2.14] of the ASIO Guidelines should be amended to:**

  (a) include an explanation of the operative effect of the 'presumption of appropriate training' in ASIO's decision-making about the authorisation of its officials to use force against persons; (including ASIO affiliates, such as secondees from other agencies);

  (b) require the Director-General to take all reasonable steps to satisfy themselves that the officials who are 'presumed' to be 'appropriately trained' in the use of force against persons, <u>in fact,</u> possess the requisite skill, experience, training and accreditation, before they are

[26] For example, paragraph 122A(1)(i) of the *Family Law Act 1975* (Cth) confers a power of arrest, including a power to use force, on all members of the Australian Border Force. (It should be noted that the originating Bill that inserted the current version of section 122A in the Family Law Act initially proposed to confer the power of arrest on all employees of the (now) Department of Home Affairs. See: Civil Law and Justice Legislation Amendment Bill 2017, Schedule 6, item 35. The Bill was amended via parliamentary amendments, following adverse comments from several parliamentary scrutiny committees. This example highlights the risks of overbreadth in other legislation authorising officials to use force against persons, which may have further implications for the 'presumption of appropriate training' in paragraph [2.14](b) of the ASIO Guidelines.)

authorised to execute ASIO warrants. (That is, even if a 'presumption of appropriate training' exists, the ASIO Guidelines should still prescribe minimum requirements for ASIO to carry out individual checks about a person's actual skills, experience and training and accreditation before that person can be authorised to exercise authority under an ASIO warrant to use force against persons); and

(c) make explicit that the 'presumption of appropriate training' in paragraph [2.14](b) applies only to Commonwealth, State or Territory officials who would ordinarily be expected to use force against persons as part of their duties.

Transparency of ASIO's policies on the use of force against persons

36. The Law Council welcomes the addition of paragraph [2.15] of the ASIO Guidelines, which requires the Director-General of Security to maintain policies on the matters in paragraphs [2.13] and [2.14] regarding training in the use of force against persons.

37. However, the Law Council is concerned that there is limited transparency in relation to the contents of these policies, and questions whether it is possible to make further details available publicly. The Law Council supports the following enhancements to the transparency of policies on the use of force against persons:

- a requirement to consult with key governmental and civil society stakeholders on proposed policies, to the extent possible within the requirements of security;
- a requirement for those parts of the policies that could be published (including in a de-classified or summary form) to be released publicly; and
- a requirement for ASIO to provide the PJCIS with a copy of its policies on the use of force against persons.

38. The Law Council notes that a requirement to provide the PJCIS with a copy of ASIO's policies on the use of force against persons would reflect the level of concern that this Committee expressed in its 2014 report on the relevant amending legislation, the National Security Legislation Amendment Bill (No 1) 2014, about governance arrangements for the use of force against persons. The PJCIS sought to ensure that there was close operational oversight of the power, and other safeguards implemented, to ensure that force was only used against persons in exceptional circumstances.[27] Giving the PJCIS direct access to policies on the use of force against persons may assist it in monitoring the governance arrangements.

Recommendation 7—transparency of policies on the use of force against persons

- **Paragraph [2.15] of the ASIO Guidelines should be amended to require ASIO to:**

  (a) publish its policies on the use of force against persons (in full, or those parts which are not classified, or are capable of being de-classified);

[27] PJCIS, *Advisory Report on the National Security Legislation Amendment Bill (No 1) 2014* (September 2014), recommendations 3-6 and supporting commentary at 46-49.

(b) consult with key governmental and civil society stakeholders to the greatest possible extent within the requirements of security; and

(c) provide the Parliamentary Joint Committee on Intelligence and Security with a copy of its policies on the use of force against persons, as soon as practicable after the policies are made, and when they are amended.

Periodic review of the ASIO Guidelines

39. The Law Council welcomes the requirements in paragraphs [1.14] and [1.15] of the ASIO Guidelines for the periodic review of those Guidelines every three years.

40. The Law Council shares the concerns raised by members of the PJCIS, the IGIS and others about the extensive delay in issuing new Guidelines, particularly given the numerous, significant changes to ASIO's governing legislation and operating environment since the previous Guidelines were issued in September 2007.

41. An administrative requirement for periodic review may go some way towards preventing the repetition of this delay. However, the Law Council notes that the revised Guidelines do not specify several important parameters for future periodic reviews, to ensure that they are transparent, participatory, comprehensive and timely. The Law Council also continues to support a legislative, rather than purely administrative, requirement for the periodic review of the Guidelines.

Placing the periodic review requirement on a legislative basis

42. While the Law Council welcomes a requirement for the periodic review of the ASIO Guidelines, its preference remains for this to be a statutory obligation under section 8A of the ASIO Act. As the Law Council noted in its recent submission to the PJCIS review of the Australian Security Intelligence Organisation Amendment Bill 2020:

> *The Law Council is concerned by the persistent failure of the ASIO Guidelines to be updated to reflect significant expansions of ASIO's powers.*
>
> *The ASIO Guidelines have not been updated for over 10 years, despite multiple recommendations from this Committee, over at least a six-year period. Those recommendations have been prompted by numerous significant legislative expansions to ASIO's powers; a sustained increase in its operational tempo; the evolution and intensification of security threats (particularly terrorism and foreign interference); and major technological developments.*
>
> *The Law Council considers that this prolonged inaction has become so serious that it is no longer appropriate to place continued reliance on executive assurances to undertake discretionary reviews on a regular basis and to make timely updates.*
>
> *The ASIO Guidelines should instead be subject to greater Parliamentary control and accountability, through the insertion of a legal requirement in section 8A of the ASIO Act, which should provide that the Minister for Home Affairs must cause the periodic review of the ASIO Guidelines every three years (once every Parliamentary term).*
>
> *The Law Council also considers that proposed revisions to the ASIO Guidelines should be subject to expanded consultation requirements before they are issued, in recognition of the significant expansions in ASIO's powers and their consequent*

potential to impact larger numbers of Australians … To ensure that such consultations are duly and consistently undertaken, the Law Council considers that there should be a statutory consultation obligation, rather than an executive undertaking alone.[28]

Recommendation 8— legislative basis for the periodic review requirement

- **Section 8A of the *Australian Security Intelligence Organisation Act 1979* (Cth) should be amended to include, as a legislative requirement, the periodic review mechanisms presently in paragraphs [1.14] and [1.15] of the ASIO Guidelines (as amended in line with recommendation 9 below)**

Essential parameters for periodic reviews

43. The periodic review requirements in paragraph [1.14] and [1.15] of the Guidelines do not address the matters outlined below.

Responsibility for initiating reviews

44. The Guidelines do not specify who is responsible for undertaking or initiating the periodic reviews. To ensure that the requirement is complied with, it would be preferable if the Guidelines expressly imposed an obligation on the relevant official to cause the reviews to be undertaken (for example, the Director-General of Security).

Consultation with civil society

45. Paragraph [1.14] provides that each periodic review must be conducted 'in consultation with relevant stakeholders and ministers as appropriate'. The Law Council is concerned that the participation of civil society in these reviews is left wholly to executive discretion (principally, that of ASIO, the Department of Home Affairs and the Minister for Home Affairs).

46. The Law Council notes the recent evidence of representatives of the Department of Home Affairs to the PJCIS about its exercise of discretion in determining consultation arrangements for the most recent review of the ASIO Guidelines. This evidence was to the effect that it was not considered necessary to consult the Law Council on the revised ASIO Guidelines before they were issued, as the Department considered that the extent of 'appropriate' consultation was with the IGIS.[29]

47. As the Law Council noted in its recent submission to the PJCIS on the Australian Security Intelligence Legislation Amendment Bill 2020, it is important that civil society has a meaningful opportunity to participate in reviews of the ASIO Guidelines, including to comment on proposed revisions before they are finalised. This is particularly important given that recent, significant expansions in ASIO's powers have increased their potential to impact upon larger numbers of Australians. Given the role of the Guidelines in setting standards and procedural requirements that ASIO must follow, including in assessing the proportionality of intrusive intelligence collection

[28] Law Council of Australia, *Submission to the PJCIS review of the Australian Security Intelligence Organisation Amendment Bill 2020*, (July 2020), 95-96 at [403]-[409].
[29] Mr Anthony Coles, First Assistant Secretary, Department of Home Affairs, *Proof Committee Hansard*, Parliamentary Joint Committee on Intelligence and Security, Canberra, 10 July 2020, 58.

measures, it is highly desirable that the standards prescribed in the ASIO Guidelines are informed by the views of civil society, including the legal profession.[30]

48. Accordingly, the Law Council considers that it would be preferable for the Guidelines to provide greater specification of the key stakeholders that must be consulted in all periodic reviews. This should include civil society as well as oversight agencies.

Transparency of periodic review outcomes

49. While paragraph [1.15] requires the Attorney-General to be notified of review outcomes, there is no requirement to publish the outcomes of these periodic reviews (including via the Parliamentary tabling of a statement).

50. The Law Council acknowledges that some information about the outcomes of periodic reviews will need to be classified. However, given the status of the ASIO Guidelines as a public document, it should be possible to provide unclassified information about the key findings and reasoning underlying any recommended changes.

51. The Law Council supports greater transparency, in the form of a requirement in the ASIO Guidelines for at least a summary of the review outcomes to be published and tabled in Parliament.

Timing for the commencement and completion of periodic reviews

52. Paragraph [1.14] requires periodic reviews to be commenced every third anniversary of the Guidelines. However, the Guidelines themselves do not state the date on which they were made or commenced. It appears from evidence given by Commonwealth officials at a public hearing of the PJCIS on 7 August 2020, that the Guidelines were issued at some point during the week commencing 3 August 2020.[31] It is therefore impossible for members of the public to know the date on which periodic reviews must commence.

53. Further, paragraph [1.14] does not prescribe any maximum timeframes for the completion of periodic reviews. This may mean that such reviews could be protracted, and may not be given a level of priority that is commensurate with the importance of the Guidelines. The Law Council therefore supports a requirement for all periodic reviews to be completed within a set period of time, illustratively within six months of their scheduled commencement.

Matters that must be examined, as a baseline, in all periodic reviews

54. The ASIO Guidelines do not provide any direction on matters that must be considered in all periodic reviews. To ensure transparency and rigour in the conduct of reviews, the Law Council recommends that the Guidelines should include such direction.

55. As detailed in the Law Council's recommendation below, the Guidelines should require periodic reviews to examine the effectiveness of the Guidelines in facilitating the lawful and proper performance by ASIO of its functions, including respect for human rights. Reviews should also assess the extent to which the Guidelines

[30] Law Council of Australia, *Submission to the PJCIS review of the Australian Security Intelligence Organisation Amendment Bill 2020*, (July 2020), 95-96 at [403]-[409].

[31] The Hon Margaret Stone AO, IGIS, *Proof Committee Hansard*, Parliamentary Joint Committee on Intelligence and Security, 7 August 2020, Canberra, 10 (The IGIS gave evidence that her office was given a copy of the ASIO Guidelines in the evening of 6 August 2020).

facilitate effective oversight. (It would be possible for the reviews to consider other matters, as appropriate in the circumstances.)

Recommendation 9—requirements for the periodic review of the ASIO Guidelines

- **Paragraphs [1.14] and [1.15] of the ASIO Guidelines should be amended to include the following requirements for the conduct of periodic reviews:**

  (a) expressly identify who is responsible for undertaking the periodic reviews, or causing the periodic reviews to be undertaken;

  (b) identify (on a non-exhaustive basis) the categories of 'relevant stakeholders' who must be consulted. This should include representatives of civil society, and oversight and integrity agencies;

  (c) require the Minister for Home Affairs or the Attorney-General to table in Parliament an unclassified statement on the outcomes of the periodic review, within 15 sitting days of the completion of the review;

  (d) specify a timeframe for completing the periodic reviews, which is no longer than six months after the date on which each periodic review is scheduled to commence;

  (e) specify the date on which the ASIO Guidelines were made and commenced, so that there is certainty about the date on which the periodic reviews must commence; and

  (f) specify matters that must be considered, as a baseline, in all periodic reviews. These matters should include:

    (i) the effectiveness of the Guidelines in facilitating:

      - **ASIO's performance of its functions in relation to security, with legality, propriety and respect for human rights;**
      - **the independent and parliamentary oversight of ASIO's activities;**
      - **public transparency and reassurance about the legality and propriety of ASIO's activities;**

    (ii) the currency and comprehensiveness of the Guidelines, having regard to:

      - **relevant legislative amendments made during the review period;**
      - **relevant advisory findings and recommendations of the Inspector-General of Intelligence and Security, the Parliamentary Joint Committee on Intelligence and Security, and the Independent National Security Legislation Monitor;**
      - **developments in the security environment; and**
      - **developments in human rights jurisprudence.**

Timeframe for the first periodic review of the ASIO Guidelines

56. Paragraph [1.14](a) of the ASIO Guidelines sets specific requirements for the first periodic review. It must commence within 18 months of the date on which the revised Guidelines commenced. It must be completed within three years of the commencement of the revised Guidelines.

57. As noted above, the date on which the revised ASIO Guidelines were issued and commenced is unknown, as the document is undated. Nonetheless, it appears that the first periodic review would need to be completed at some point in August 2023.

58. The Law Council notes that are many pressing issues that will require amendments to the ASIO Guidelines to be made on a more urgent basis than mid-to-late 2023. This includes updates to address outstanding aspects of the TOLA amendments, to the extent that they apply to ASIO. The Law Council also considers that further amendments will be necessary if the Parliament passes the Australian Security Intelligence Organisation Amendment Bill 2020 (**ASIO Amendment Bill**),[32] and the Telecommunications Legislation Amendment (International Production Orders) Bill 2020 (**IPO Bill**).[33]

59. The Law Council therefore calls on the Government to commit to reviewing the ASIO Guidelines before the first periodic review falls due under paragraph [1.14](a).

60. ASIO's re-designed compulsory questioning regime in Schedule 1 to the ASIO Amendment Bill will require particular attention in a future revision of the ASIO Guidelines. This is particularly in relation to:

- the assessment of proportionality, especially in ascertaining the relative degree of intrusion associated with compulsory questioning (and related search and seizure powers, and the secondary use of information obtained from questioning); and
- the interpretation of politically motivated violence in relation to compulsory questioning. In particular, the guidance in Part 5 of the ASIO Guidelines appears to be specific to the exercise of covert collection powers, rather than compulsory questioning. The Law Council considers that this will require revision to take account of the expansion of compulsory questioning powers to politically motivated violence. The Law Council notes, for example, that the scope of targeting in paragraph [5.8] of the ASIO Guidelines[34] would raise significant human rights compatibility issues if it were applied directly to subjects of compulsory questioning. In general, international human rights law does not

[32] The ASIO Amendment Bill proposes to re-design ASIO's warrant based compulsory questioning powers, and to enable it to self-authorise the use of tracking devices in certain circumstances. The Law Council considers that both of these measures should be the subject of specific guidance in the ASIO Guidelines.

[33] The IPO Bill establishes a legislative framework for Australia to implement international agreements with other countries for reciprocal access to communications information (data and content) stored in the other country. The Law Council considers that ASIO's use of this scheme should be the subject of specific guidance in the ASIO Guidelines.

[34] Paragraph [5.8] of the ASIO Guidelines deals with the application of paragraph (b) of the definition of 'politically motivated violence' in section 4 of the ASIO Act to the scenario of public dissent or protest. Paragraph (b) of the definition covers the use of tactic that can reasonably be assessed as likely to result in violence. Paragraph [5.8] of the ASIO Guidelines states that 'a person or group need not initiate violence … for their activities to be assessed as politically motivated violence … it is sufficient that the activities could lead to violence. All that is required is that there is a reasonable likelihood that the activity will produce violence from others'.

regard it as acceptable for those engaged in peaceful advocacy to have their rights to peaceful assembly limited, but rather those who seek to respond with violence should be targeted.[35] Given that compulsory questioning powers can be exercised against adults who are not suspected of personally engaging in activities prejudicial to security (such as politically motivated violence), the Law Council considers that it will be necessary for the ASIO Guidelines to contain clear guidance about the potential exercise of compulsory questioning powers against such persons, especially in the context of politically motivated violence investigations arising from acts of civil protest, dissent or advocacy.

Recommendation 10—additional, earlier review of the ASIO Guidelines to implement recent legislative amendments, and anticipated amendments (if enacted)

- **Prior to the scheduled commencement of the first periodic review of the ASIO Guidelines as required by paragraph [1.14](a), the Government should review and update the ASIO Guidelines to take into account:**
  - **(a) all recent legislative changes made by the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (Cth); and**
  - **(b) further legislative amendments if Bills presently before the Parliament are passed, including the Australian Security Intelligence Organisation Amendment Bill 2020, and the Telecommunications Legislation Amendment (International Production Orders Bill 2020).**

Reporting to the Attorney-General on intelligence collection warrants

Breach reporting requirements

61. Paragraphs [2.8] and [2.9] of the ASIO Guidelines provide that ASIO's statutory reports to the Attorney-General on its intelligence collection warrants must address certain matters. These matters largely repeat the statutory reporting requirements in section 34 of the ASIO Act for special powers warrants, and the requirements in section 17 of the *Telecommunications (Interception and Access) Act 1979* (Cth) (**TIA Act**) for telecommunications interception warrants.

62. However, paragraphs [2.8](d) and [2.9](c) of the ASIO Guidelines impose an additional requirement. They provide that ASIO must report to the Attorney-General on 'any action taken which would have required a warrant where one had not been obtained'. (This breach reporting obligation applies equally to special powers warrants issued under the ASIO Act, and interception warrants under the TIA Act.)

63. The Law Council strongly supports the inclusion of this additional reporting requirement. It will ensure that the Attorney-General (and the IGIS, through their inspection of ASIO's warrant reports to the Attorney-General) are alerted to any activities that are undertaken without the requisite legal authorisation. However, as explained below, the drafting of the relevant provisions in the ASIO Guidelines appears to limit the scope of this obligation. This may be unintentional.

Limitation in the scope of breach reporting obligations in paragraphs [2.8](d) and [2.9](c)

[35] *Platform "Ärzte für das Leben" (Doctors for the Right to Life) v Austria* [1988] ECHR 15 at [31].

64. The reporting obligations in paragraphs [2.8](d) and [2.9](c) are part of a list of matters that must be addressed 'with respect to ASIO Act warrants' or 'with respect to TIA Act warrants' (that is, as part of the reports that must be given to the Attorney-General on ASIO's execution of warrants that have been issued).[36]

65. This connection with ASIO's statutory warrant reports would appear to limit the reporting obligations in paragraphs [2.8](d) and [2.9](c) to circumstances in which ASIO had obtained a warrant, and purported to undertake a particular activity as part of a warrant operation, but the activity, in fact, exceeded the statutory limits of authority under that warrant.

66. The Law Council considers that the ASIO Guidelines should be amended to cast the requirements in paragraphs [2.8](d) and [2.9](c) as 'stand-alone' reporting obligations. That is, these obligations should be clearly expressed as operating **separately** to ASIO's statutory warrant reporting requirements under section 34 of the ASIO Act and section 17 of the TIA Act, which are the subject of further direction in paragraphs [2.8](a)-(c) and [2.9](a)-(b) of the ASIO Guidelines.

67. The result of this amendment would be that:

- if ASIO undertook an activity without obtaining any warrant; and
- ASIO needed to obtain a warrant to lawfully undertake that activity (that is, because the conduct would otherwise constitute an offence); then
- ASIO must provide a written report to the Attorney-General on that incident.

Recommendation 11—clarification of breach reporting requirements

- **Paragraphs [2.8] and [2.9] of the ASIO Guidelines should be amended to make explicit that the obligations in paragraphs [2.8](d) and [2.9](c) to report to the Attorney-General on activities that required a warrant, but were not authorised by a warrant, apply to both:**

  (a) ASIO's statutory reports to the Attorney-General on individual warrant operations, where ASIO officers engaged in activities that were not, in fact, authorised by that warrant (for example, because the activities exceeded the statutory limits of authority conferred under the warrant); and

  (b) instances in which no warrant was obtained at all for the relevant activities. (That is, the activities were <u>not</u> carried out as part of a warrant operation in purported reliance on an extant warrant. For example, if there was a mistaken belief that a warrant was not required to carry out the activity; or reliance was incorrectly placed on an expired warrant.)

- **To avoid doubt, the matter in paragraph (b) above would be a separate reporting obligation to the statutory warrant reporting requirements under section 34 of the *Australian Security Intelligence Organisation Act 1979* (Cth) and section 17 of the *Telecommunications (Interception and Access) Act 1979* (Cth) which are dealt with in paragraphs [2.8](a)-(c) and [2.9](a)-(b) of the ASIO Guidelines.**

[36] See the chapeau (opening text) to paragraphs [2.8] and [2.9] of the ASIO Guidelines.

Reporting to the Attorney-General on 'post-warrant concealment' activities

68. The reporting requirements in paragraphs [2.8] and [2.9] of the ASIO Guidelines are limited expressly to ASIO's warrants. They do not provide any guidance about reporting to the Attorney-General on post-warrant concealment activities pursuant to section 34A of the ASIO Act.[37]

69. The Law Council considers that the ASIO Guidelines should deal comprehensively with the reporting requirements to the Attorney-General, including post-warrant concealment activities. The matters in paragraph [2.8] of the Guidelines generally appear relevant to ASIO's reporting to the Attorney-General on its post-warrant concealment activities under section 34A of the ASIO Act, in addition to its separate warrant reporting requirements in section 34 of that Act.

Recommendation 12—reporting on post-warrant concealment activities

- **Part 2 of the ASIO Guidelines should be amended to provide guidance on reporting to the Attorney-General on post-warrant concealment activities under section 34A of the *Australian Security Intelligence Organisation Act 1979* (Cth).**
- **This guidance should be analogous to the requirements in paragraphs [2.8] and [2.9] of the ASIO Guidelines for warrant reports under section 34 of the *Australian Security Intelligence Organisation Act 1979* (Cth) and section 17 of the *Telecommunications (Interception and Access) Act 1979* (Cth).**

Oversight by the Inspector-General of Intelligence and Security

70. The ASIO Guidelines provide that Director-General of Security is required to ensure that the IGIS is given copies of certain policies that are required to be made under the ASIO Guidelines, as soon as practicable after they are made.

71. In particular, paragraph [1.13](c) requires the Director-General to ensure that the IGIS is given copies of all policies made under paragraphs [2.15] (use of force against persons) and [4.3] (access to, and retention of, personal information).

72. This requirement does not extend to the policies that are required to be made under paragraph [3.6] on the exercise of powers to confer civil immunities under subsection 21A(1) of the ASIO Act, and civil and criminal immunities under TARs. This may be an unintended omission.

73. To avoid any doubt, and ensure clarity for both the public and ASIO, the obligation at paragraph [1.13](c) of the ASIO Guidelines should include an express reference to the policies made under paragraph [3.6] of those Guidelines.

74. Further, the Law Council recommends that the obligations under paragraph [1.13] should be amended to apply expressly to **all amendments** to the policies made under paragraphs [2.15], [3.6] and [4.3] of the ASIO Guidelines. This will help to ensure that

[37] ASIO's powers to undertake post-warrant concealment activities (that is, taking actions to conceal that an act or a thing was done under a warrant, **after** that warrant has expired) were enacted by the TOLA Act in 2018, which relevantly inserted subsections 25A(8), 27A(3C) and 27E(6) into the ASIO Act. The reporting requirement in section 34A of the ASIO Act was also enacted by the TOLA Act.

the public can be confident that the IGIS will be kept apprised, in a timely way, of all changes to those policies.

Recommendation 13—provision of policies to the IGIS

- **Paragraph [1.13](c) of the ASIO Guidelines should be amended to require the Director-General of Security to ensure that the Inspector-General of Intelligence and Security (IGIS) is given copies of all policies made under the ASIO Guidelines. This should expressly include:**

  (a) a requirement to ensure that the IGIS is given copies of policies made under paragraph [3.6] (powers to confer civil and criminal immunities) in addition to the policies made under paragraphs [2.15] (use of force against persons) and [4.3] (treatment of personal information); and

  (b) a requirement to ensure that the IGIS is given copies of all amendments to all policies made under the ASIO Guidelines, as soon as practicable after the amendment is made.

Treatment of personal information

75. The Law Council welcomes the inclusion of Part 4 in the ASIO Guidelines, which deals with the handling of personal information, including access, retention and destruction.

76. The Law Council particularly welcomes the requirement in subparagraph [4.3](a)(vi) for ASIO to maintain policies that provide clear guidance on 'processes for periodic review of its holdings including personal information, to determine whether retention is reasonable'.

77. This requirement may assist in remediating or preventing ASIO from retaining large volumes of personal information for prolonged periods of time, without regular assessment of whether the relevant individuals remain of security interest.

78. This risk arises because the statutory obligation of the Director-General of Security to destroy information obtained under ASIO's warrants only arises if the Director-General become satisfied that it is no longer relevant. There is no statutory obligation on the Director-General to cause ASIO to conduct reviews of its information holdings to determine whether the destruction obligation is enlivened.[38] Further, ASIO is not subject to any statutory obligation under the TIA Act to destroy records of telecommunications data accessed under Part 4-1 of that Act, such as metadata, if it is no longer relevant to security.

79. The PJCIS has previously expressed concerns about the absence of comprehensive review and destruction obligations in relation to personal information in ASIO's holdings, particularly in the case of metadata.[39]

[38] ASIO Act, section 31; TIA Act, section 14.

[39] PJCIS, *Advisory report on the National Security Legislation Amendment Bill (No 1) 2014*, (September 2014), 45 at [3.48]-[3.50] and recommendation 4; and PJCIS, *Advisory Report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014*, (February 2015), 259-262 at [6.217]-[6.225] and recommendation 28.

Retention of personal information

80. The Law Council welcomes the creation of an administrative requirement for ASIO to make policies requiring the periodic review of its holdings of personal information.

81. However, the Law Council is concerned that the requirements in paragraph [4.3](b) of the ASIO Guidelines for the retention of personal information may enable some information to be retained despite it being assessed as not being relevant, or no longer being relevant, to security.

82. Subparagraph [4.3](b)(i) of the ASIO Guidelines provides that ASIO's policies must ensure that it only retains personal information where it is:

- relevant to the proper performance of its functions or exercise of its powers; **or**
- otherwise authorised or required by law.

83. The Law Council considers that the ASIO Guidelines should provide clearer guidance about the interpretation of the expression 'authorised by law' for the purpose of the policies made under paragraph [4.3].

84. In particular, the ASIO Guidelines should explicitly adopt the interpretation applied by the Office of the Australian Information Commissioner (**OAIC**) for the purpose of the *Australian Privacy Principles Guidelines* (**APP Guidelines**) made under the *Privacy Act 1988* (Cth).[40]

85. The APP Guidelines state that, for the purpose of interpreting the phrase 'authorised by or under an Australian law' in the Australian Privacy Principles, 'an act or practice is not authorised solely because there is no law or court/tribunal order prohibiting it'. Rather, an act or practice is taken to be 'authorised' under an Australian law if an entity 'is permitted to take the action but is not required to do so'.[41]

86. The Law Council is concerned to avoid any risk that the absence of a comprehensive statutory requirement for ASIO to destroy all personal information that is not, or is no longer, relevant to security could be interpreted as an 'authorisation' for the purposes of policies made under paragraph [4.3] of the ASIO Guidelines.

87. For example, as noted above, the TIA Act does not require ASIO to destroy, or prohibit it from retaining, metadata that it has accessed under Part 4-1 of that Act, which is not relevant to security, or is no longer relevant to security.

88. The absence of a statutory prohibition on ASIO retaining that metadata should not be interpreted as an 'authorisation under a law of the Commonwealth' to retain it, for the purposes of ASIO's policies made under paragraph [4.3] of the ASIO Guidelines.

Recommendation 14—review and destruction obligations

- **Paragraph [4.3](b) of the ASIO Guidelines should be amended to expressly apply the meaning of 'authorised by law' adopted by the Office of the**

[40] ASIO is not subject to the APPs: *Privacy Act 1988* (Cth), subsection 7(2).

[41] OAIC, *APP Guidelines*, version 1.3 (July 2019), Chapter B, 26 at [B.130]-[B.132].

Australian Information Commissioner in relation to the *Privacy Act 1988* (Cth).

- **That is, paragraph [4.3](b) of ASIO Guidelines should make explicit that the absence of a statutory prohibition on ASIO retaining certain information (such as telecommunications data) does not amount to an 'authorisation' to retain it. Rather, an 'authorisation' requires a law to clearly confer a permission or discretion on ASIO.**

Meaning of 'reference data'

89. Paragraph [4.3](b) of the ASIO Guidelines provides that ASIO's policies on access to personal information must cover 'data and information, which may include reference data'.[42] The term 'reference data' is not defined or explained in the Guidelines. Presumably, it is intended to refer generally to types of data that are used to classify or categorise other data within a database (for example, data codes).

90. As this term is not necessarily widely understood by the public, and it is possible that ASIO may have adopted a more specific or specialised interpretation, it would be preferable for the intended meaning to be defined expressly in the ASIO Guidelines. Precision of terminology is important in the context of the ASIO Guidelines, given the highly intrusive and covert nature of ASIO's functions, and the likelihood of ASIO holding a large volume of sensitive personal information in performing its functions.

91. An explicit definition will ensure that the public understands and interprets the term, and associated obligations under the Guidelines, consistently with the intended meaning given by the Government. This will also facilitate effective oversight by the IGIS of ASIO's compliance with the requirements in paragraph [4.3] of the Guidelines, and the policies that are required to be made under that paragraph.

Recommendation 15—inclusion of a definition of 'reference data'

- **Appendix 1 to the ASIO Guidelines should be amended to include a definition of the term 'reference data' as used in paragraph [4.3] of the Guidelines.**

Transparency of ASIO's policies in relation to personal information

92. While it is positive that the ASIO Guidelines seek to regulate ASIO's access to, and retention of, personal information, there appears to be limited transparency in the substantive policies that must be made under paragraph [4.3].

93. There are no requirements for ASIO to publish these policies, or as much of them as is possible within the requirements of security. There is also no requirement for ASIO to conduct consultations (including with civil society) in developing the policies.

94. Further, there is no requirement for the PJCIS to be given a copy of the policies. As with the comments above on the use of force against persons, the PJCIS has previously expressed concern about the potential for ASIO to retain large volumes of personal information that may no longer be relevant to its functions, and has

[42] ASIO Guidelines, 14 at subparagraphs [4.3](b)(ii) and (iii).

recommended the revision of the ASIO Guidelines to address this concern since 2014.[43]

95. Given the significant parliamentary concern about this matter, the Law Council considers it appropriate that the PJCIS is provided with relevant policies governing ASIO's access to, and retention of, personal information. This would assist the PJCIS in monitoring the applicable governance requirements.

Recommendation 16—requirements for policies in relation to personal information

- **Part 4 of the ASIO Guidelines should be amended to apply the following, additional requirements to the policies that ASIO must make under paragraph [4.3] about its access to, and retention of, personal information:**

  (a) ASIO must undertake consultation in developing the policies, including with the Inspector-General of Intelligence and Security and civil society to the extent possible within the requirements of security;

  (b) ASIO must make the policies available to the public in full, or in part to the greatest extent possible within the requirements of security; and

  (c) ASIO must give the PJCIS a copy of all policies made under paragraph [4.3] of the Guidelines, including any amendments.

Public release of the ASIO Guidelines

96. The evidence given by Commonwealth officials to a public hearing of the PJCIS on 7 August 2020 indicates that there appears to have been a delay of at least seven days between the revised ASIO Guidelines being issued (and, presumably, their commencement) and their public release, via their out-of-session tabling in the Senate on 13 August 2020.[44]

97. The Law Council notes that subsection 8A(3) of the ASIO Act requires the ASIO Guidelines to be tabled in Parliament within 15 sitting days of being given to the Director-General of Security. Subsection 8A(3) of the ASIO Act does not prohibit the public release of the ASIO Guidelines prior to their tabling.

98. The matter is not governed by legal rules or prohibitions, but rather by practical considerations.[45] The Law Council can see no credible reason that such practices could not be adapted to meet the important public interests in transparency and accountability (including in circumstances in which Parliamentary sittings and

[43] PJCIS, *Advisory report on the National Security Legislation Amendment Bill (No 1) 2014*, (September 2014), 45 at [3.48]-[3.50] and recommendation 4; and PJCIS, *Advisory Report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014*, (February 2015), 259-262 at [6.217]-[6.225] and recommendation 28.

[44] See, for example, the Hon Margaret Stone AO, IGIS, *Proof Committee Hansard*, Parliamentary Joint Committee on Intelligence and Security, 7 August 2020, Canberra, 10. See further, Mr Andrew Warnes, Assistant Secretary, Department of Home Affairs, *Proof Committee Hansard,* Parliamentary Joint Committee on Intelligence and Security, 7 August 2020, Canberra, 40.

[45] Department of the Prime Minister and Cabinet, *Tabling Guidelines*, (June 2019), 2; and D.R Elder (ed), *House of Representatives Practice*, (7th edition, June 2018), 612.

scheduling for the tabling of documents out-of-sitting are disrupted, as has occurred with the COVID-19 pandemic).

99. Given the importance of the ASIO Guidelines in prescribing requirements about the way in which ASIO must perform its functions (which impact significantly on individual rights and liberties) the Law Council calls on the Government to adopt a practice of immediately publishing all future revisions of the ASIO Guidelines once they are issued to the Director-General of Security. Formal parliamentary tabling, within the statutory timeframe of 15 sitting days, could then follow, in satisfaction of the requirement in subsection 8A(3) of the ASIO Act.

100. In contrast, if the ASIO Guidelines were a legislative instrument (as is the case for other guidance material, such as the Statement of Procedures for ASIO's questioning warrants, issued under section 34C of the ASIO Act)[46] then there would be no delay between the making and commencement of the Guidelines and their public release.

101. This is because the requirements of the *Legislation Act 2003* (Cth) would apply, so that the ASIO Guidelines would be taken to commence when they are registered (that is, published) on the Federal Register of Legislation (**FRL**)[47] and would be publicly accessible at this time (noting the FRL is published at www.legislation.gov.au). The ASIO Guidelines would then have to be tabled in Parliament within six sitting days of their registration on the FRL.[48]

102. Accordingly, the Law Council recommends that consideration is given to amending section 8A of the ASIO Act to provide that the ASIO Guidelines are a legislative instrument (potentially a non-disallowable legislative instrument); or at least a notifiable instrument under the Legislation Act, so that the registration and commencement requirements in that Act would apply.

Recommendation 17—immediate publication of revised ASIO Guidelines

- **Given the importance of the ASIO Guidelines and the considerable public interest in timely access, the Government should adopt a practice of immediately publishing future versions of ASIO Guidelines, after they have been issued to the Director-General of Security.**
- **Public release of the ASIO Guidelines should not be delayed until their parliamentary tabling under subsection 8A(3) of the *Australian Security Intelligence Organisation Act 1979* (Cth), noting that nothing in this provision would prohibit the publication of the ASIO Guidelines prior to their being tabled in Parliament.**
- **Further consideration should be given to amending section 8A of the ASIO Act to provide that the ASIO Guidelines are either a legislative instrument or a notifiable instrument within the meaning of the *Legislation Act 2003* (Cth) so that the registration and commencement requirements of that Act apply.**

[46] ASIO Act, subsection 34C(5).

[47] *Legislation Act 2003* (Cth), section 12.

[48] Ibid, section 38.