PARLIAMENT OF THE COMMONWEALTH OF AUSTRALIA

# Review of the amendments made by the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018

Parliamentary Joint Committee on Intelligence and Security

December 2021
CANBERRA

ISBN 978-1-76092-164-4 (Printed Version)

ISBN 978-1-76092-165-1 (HTML Version)

# Contents

# Abbreviations

| | |
|---|---|
| AAT | Administrative Appeals Tribunal |
| ABF | Australian Border Force |
| ACIC | Australian Criminal Intelligence Commission |
| ACSC | Australian Cyber Security Centre |
| AFP | Australian Federal Police |
| ASD | Australian Signals Directorate |
| ASIO | Australian Security and Intelligence Organisation |
| ASIO Act | *Australian Security Intelligence Organisation Act 1979* |
| ASIS | Australian Secret Intelligence Organisation |
| CLOUD Act | *Clarifying Lawful Use of Overseas Data Act* (US) |
| CSIRO | Commonwealth Scientific and Industrial Research Organisation |
| DCP | Designated Communications Provider |
| DRIPA | *Data Retention and Investigatory Powers Act* (UK) |
| IGIS | Inspector-General of Intelligence and Security |
| INSLM | Independent National Security Legislation Monitor |
| INSLM Act | *Independent National Security Legislation Monitor Act 2010* |
| IPCO | Investigatory Powers Commissioner's Office |
| IPO Bill | Telecommunications Legislation Amendment (International Production Orders) Bill 2020 |
| LECC | Law Enforcement Conduct Commission |
| MEAA | Media Entertainment and Arts Alliance |

| | |
|---|---|
| OAIC | Office of the Australian Information Commissioner |
| OVIC | Office of the Victorian Information Commissioner |
| SD Act | *Surveillance Devices Act 2004* |
| TAN | Technical Assistance Notice |
| TAR | Technical Assistance Request |
| TCN | Technical Capability Notice |
| TIA Act | *Telecommunications (Interception and Access) Act 1979* |
| TOLA Act | *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* |
| TOLA Bill | Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 |
| UK | United Kingdom |
| UN | United Nations |
| US | United States of America |
| VoIP | Voice over Internet Protocol |

# Membership of the Committee

***Chair***

Mr Andrew Hastie MP (until 22/12/2020)
Senator James Paterson (from 04/02/2021)

***Deputy Chair***

Hon Anthony Byrne MP (until 14/10/2021)
Senator Jenny McAllister (Deputy Chair from 19/10/2021)

***Members***

Hon Mark Dreyfus QC, MP
Hon Dr Mike Kelly AM, MP (until 30/04/2020)
Mr Julian Leeser MP
Mr Tim Wilson MP (until 08/10/2021)
Dr Anne Aly MP (from 03/09/2020)
Ms Celia Hammond MP (from 03/02/2021)
Senator the Hon Eric Abetz
Senator the Hon David Fawcett
Senator the Hon Kristina Keneally
Senator Amanda Stoker (until 22/12/2020)
Mr Peter Khalil MP (from 28/10/2021)
Mr Andrew Wallace MP (from 28/10/2021 until 23/11/2021)
Hon Kevin Andrews MP (from 02/12/2021)

# Terms of Reference

The Committee is required under Section 187N of the *Telecommunications (Interception and Access) Act 1979* to review amendments made to Commonwealth legislation by the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* and to complete its review by 30 September 2020.

As part of its adoption of the review, the Committee resolved to focus on the following aspects of the legislation for the purposes of the review:

- the threshold, scope and proportionality of powers provided for by the Act;
- authorisation processes and decision-making criteria;
- the scope of enforcement provisions and the grant of immunities;
- interaction with intelligence agencies other powers;
- interaction with foreign laws, including the United States' *Clarifying Lawful Overseas Use of Data Act*;
- impact on industry and competitiveness; and
- reporting obligations and oversight measures.

# List of Recommendations

## Recommendation 1

4.75 The Committee recommends that the Government implement a periodic survey, starting in three years from the presentation of this report, to ascertain ongoing economic impacts of the TOLA Act legislation on Australia's ICT industry and the results should be made publicly available.

## Recommendation 2

4.78 The Committee recommends the Government, in consultation with relevant stakeholders, develop a prescribed set of requirements for information that must be included in technical assistance requests.

## Recommendation 3

4.82 The Committee recommends that s317C of the *Telecommunications Act 1997* be amended to clarify that a designated communications provider does not include a natural person, where that natural person is an employee of a designated communications provider, but will only apply to natural persons insofar as required to include sole traders.

## Recommendation 4

4.85 The Committee recommends that Part 15 of the *Telecommunications Act 1997* be amended to remove references to 'systemic vulnerability'.

## Recommendation 5

4.87 The Committee recommends that s 317ZG of the *Telecommunications Act 1997* be amended to describe the 'prohibited effects' of a technical assistance request, a technical assistance notice or a technical capability notice.

Such an amendment could take the form of the words put forward by the Independent National Security Legislation Monitor in his recommendations 9 and 10, and the government may consider incorporation of additional definitions in s317B of the *Telecommunications Act 1997* arising from the proposed amendment.

## Recommendation 6

4.90 The Committee recommends that the Department of Home Affairs develop, maintain, and publish non-exhaustive guidance documents that set out non-binding examples of what may constitute a 'whole class of technology' for the purposes of defining a systemic weakness.

## Recommendation 7

4.93 The Committee recommends the Government commission a review of Commonwealth legislation to determine whether the concept of 'serious offence', 'relevant offence', and other similar concepts:

- should be made consistent across different Acts of Parliament; and
- whether the threshold for the concept of 'serious offence' in all Commonwealth legislation should be – at a minimum – an indictable offence punishable by a maximum penalty of seven years' imprisonment or more, with a limited number of exceptions.

This body of work should inform, or occur as part of, the eventual electronic surveillance bill being considered by the Department of Home Affairs and other departments.

## Recommendation 8

5.55 The Committee recommends that the relevant provisions of the *Australian Security Intelligence Organisation Act 1979* and the *Surveillance Devices Act 2004* be amended to require the Australian Security Intelligence Organisation and law enforcement agencies to seek external authorisation from the Attorney-General or issuing authority to carry out concealment activities in relation to the execution of computer access warrants following the initial 28 day window provided in the respective acts.

The Committee recommends that such an application should allow the Australian Security Intelligence Organisation or law enforcement agencies to carry out concealment activities within a window of time not exceeding six months from the expiry of the initial 28 day window, with the option to seek additional external authorisation for a further six months if required.

## Recommendation 9

5.62 The Committee recommends that the Government make clear that no mandatory assistance order, including those defined in section 3LA of the *Crimes Act 1914* and section 201A of the *Customs Act 1901*, can be executed in a manner that amounts to the detention of a person where that agency does not otherwise have any lawful basis to detain the person.

## Recommendation 10

6.46 The Committee recommends that s21A of the *Australian Security Intelligence Organisation Act 1979* be amended to limit authorisation of activities under voluntary assistance provisions to the Director-General of Security and Deputy Directors-General of the Australian Security Intelligence Organisation.

## Recommendation 11

6.49 The Committee recommends that s 21A(1)(e) and s 21A(5)(e) of the *Australian Security Intelligence Organisation Act 1979* be amended to confine the scope of the immunity from civil liability offered under the Act to 'conduct that does not result in serious personal injury or death to any person or significant loss of, or serious damage to, property'.

## Recommendation 12

6.53 The Committee recommends that s21A of the *Australian Security Intelligence Organisation Act 1979* be amended to require the Director-General of Security to be satisfied of the reasonableness and proportionality of the conduct of a voluntary assistance request prior to issuance.

## Recommendation 13

6.55 The Committee recommends that s21A of the *Australian Security Intelligence Organisation Act 1979* be amended to require the Australian Security Intelligence Organisation to retain written reasons underpinning a voluntary assistance request.

## Recommendation 14

6.57 The Committee recommends that s21A and s34AAD of the *Australian Security Intelligence Organisation Act 1979* be amended to state that nothing in either section authorises the Director-General of Security to make a request of a person that is properly the subject of a technical assistance request as set out by s317G of the *Telecommunications Act 1997*.

## Recommendation 15

6.61 The Committee recommends that the Government make clear, for the avoidance of doubt, that the compulsory assistance order power in s34AAD of the *Australian Security Intelligence Organisation Act 1979* does not authorise the detention of person to whom the order applies where the Australian Security Intelligence Organisation does not otherwise have any lawful basis to detain the person.

## Recommendation 16

6.64 The Committee recommends that s34AAD of the *Australian Security Intelligence Organisation Act 1979* be amended to state that the requirement to comply with a compulsory assistance order is only enlivened once the specified individual has been provided with a written notice that outlines what they must do to ensure compliance with the order. This notice should also clarify the consequences of failing to comply.

## Recommendation 17

6.66 The Committee recommends that s34AAD of the *Australian Security Intelligence Organisation Act 1979* be amended to require the Australian Security Intelligence Organisation to advise the individual subject to a compulsory assistance order the conditions associated with that order at the time the written notice is provided or at such time as the conditions are known.

## Recommendation 18

7.85 The Committee recommends that the Government amend the *Inspector-General of Intelligence and Security Act 1986* to expand the jurisdiction of the IGIS to oversee the intelligence functions of the Australian Federal Police.

## Recommendation 19

7.88 The Committee recommends that the Government amend the *Intelligence Services Act 2001* to provide the Parliamentary Joint Committee on Intelligence and Security with the ability oversee to the intelligence functions of the Australian Criminal Intelligence Commission.

## Recommendation 20

7.93 The Committee recommends the Government give further consideration to the proposal from the INSLM for an Investigatory Powers Division within the Administrative Appeals Tribunal and provide a response on the proposed model or any recommended alternatives by September 2022.

## Recommendation 21

7.96 The Committee recommends the Government consider the proposal for an Investigatory Powers Commissioner, as recommended by the INSLM, and provide a response on the proposed model or any recommended alternative models by September 2022.

## Recommendation 22

7.98 The Committee recommends that the Government expressly clarify that the Commonwealth Ombudsman must consult with relevant agencies to identify operationally sensitive material that should be removed or amended before publication of a report. Section 317ZRB(7) of the *Telecommunications Act 1997* should then subsequently be repealed.

## Recommendation 23

7.100 The Committee recommends that s317LA of the *Telecommunications Act 1997* be repealed so that State and Territory police are not required to seek the approval of the Australian Federal Police for a technical assistance notice.

## Recommendation 24

7.104 The Committee recommends that s 34 of the *Australian Security Intelligence Organisation Act 1979* be amended to require the Australian Security Intelligence Organisation to report to the Attorney-General when a device is removed from premises in the execution of a computer access warrant and the duration of the removal.

## Recommendation 25

7.108 The Committee recommends that:

- the Australian Security Intelligence Organisation provide annually to the Parliamentary Joint Committee on Intelligence and Security (PJCIS) a copy of its annual report appendix in relation to Telecommunications and Other Legislation Amendment (TOLA) authorisations, consistent with current practice for telecommunications data access authorisations; and

- the *Intelligence Services Act 2001* be amended, as required, to provide that the PJCIS may review matters in relation to TOLA authorisations of the Australian Security Intelligence Organisation.

## Recommendation 26

7.110 The Committee recommends that the Australian Security Intelligence Organisation brief the Parliamentary Joint Committee on Intelligence and Security on the acts or things implemented as part of a compulsory assistance order to facilitate and assist the ongoing review and oversight of the legislation.

## Recommendation 27

7.113 The Committee recommends that s 3LA of the *Crimes Act 1914* and s 201A of the *Customs Act 1901* be amended to require agencies to report to inspection bodies on the execution of assistance orders and publish those figures in their respective annual reports.

## Recommendation 28

7.118 The Committee recommends the definition in s 4 of the *Independent National Security Legislation Monitor Act 2010* be amended to allow the Independent National Security Legislation Monitor to review the amendments made by the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* of its own motion.

## Recommendation 29

7.121 The Committee recommends s 29 of the *Intelligence Services Act 2001* be amended to require the Parliamentary Joint Committee on Intelligence and Security to commence a review within three years once the Committee becomes aware through existing annual reporting requirements that the technical assistance notices or technical capability notices provided by Schedule 1 of the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* have been used.

# 1. Introduction

1.1 Section 187N of the *Telecommunications (Interception and Access) Act 1979* requires the Parliamentary Joint Committee on Intelligence and Security (the Committee) to review the amendments made to Commonwealth legislation by the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 (TOLA Act) and to complete its review by 30 September 2020.

1.2 An overview of the legislation and discussion of the history of the inquiries related to the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 and the TOLA Act is contained in Chapters 2 and 3 of this report.

## Overview of the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018*

1.3 The *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* amended a range of Commonwealth legislation including:

- *Telecommunications Act 1997;*
- *Telecommunications (Interception and Access) Act 1979;*
- *Surveillance Devices Act 2004;*
- *Crimes Act 1914;*
- *Mutual Assistance in Criminal Matters Act 1987;*
- *Australia Security Intelligence Organisation Act 1979; and*
- *Customs Act 1901*

for the stated purpose to 'introduce measures to better deal with the challenges posed by ubiquitous encryption'.[1]

1.4 The amending Act contains five schedules. **Schedule 1** contains amendments to provide a series of 'industry assistance measures' to both lawfully request and compel industry to provide technical assistance to security agencies in response to the challenges of ubiquitous encryption.

1.5 **Schedule 2** establishes powers which enable federal, state and territory law enforcement agencies to obtain covert computer access warrants when investigating certain federal offences.

1.6 **Schedules 3 and 4** amends the search warrant framework under the Crimes Act and the Customs Act to expand the ability of criminal law enforcement agencies to collect evidence from electronic devices.

1.7 **Schedule 5** clarifies that where a person voluntarily provides assistance to ASIO, that person can be conferred immunity from civil liability. It provides for new powers which enable ASIO to compel a person to provide assistance in accessing data held on a device.[2]

1.8 The details of the schedules contained in the TOLA Act will be discussed in detail in subsequent chapters.

# Conduct of the Inquiry

1.9 The Committee announced its inquiry by media release on Thursday, 4 April 2019, just prior to the dissolution of Parliament for the 2019 Federal election, and invited submissions from interested members of the public. This action allowed submitters the time during the election break to provide submissions on the review's terms of reference.

1.10 The Committee resolved to focus on:

- the threshold, scope and proportionality of powers provided for by the Act;
- authorisation processes and decision-making criteria;
- the scope of enforcement provisions and the grant of immunities;
- interaction with intelligence agencies other powers;

---

1 Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (TOLA Bill), Explanatory Memorandum, p. 2.

2 TOLA Bill, Explanatory Memorandum, pp. 2–6.

- interaction with foreign laws, including the United States' *Clarifying Lawful Overseas Use of Data Act*;
- impact on industry and competitiveness; and
- reporting obligations and oversight measures.

1.11 Following the Australian Federal election on 18 May 2019, the Committee of the 46th Parliament again formally adopted the review and received 35 submissions and 13 supplementary submissions from industry, government, academia and civil society which are listed at Appendix A.

1.12 The Committee held public hearings on Monday, 27 July 2020 and Friday, 7 August 2020 and received a private briefing on Thursday, 18 June 2020. A list of witnesses who appeared before the Committee at public hearings is included at Appendix B.

1.13 Copies of the submissions, the transcripts from the public hearing and links to additional supporting documents can be accessed at the Committee's website.[3]

# Report structure

1.14 This report comprises seven chapters:

- This chapter, **Chapter 1**, introduces the relevant legislative provisions enabling the Committee to undertake its inquiry as well as information regarding the conduct of the inquiry.
- **Chapter 2** provides a background on the previous inquiries conducted by the Committee into the Bill and the Act, as well as an overview of the inquiry conducted by the Independent National Security Legislation Monitor (INSLM), and associated report.
- **Chapter 3** provides an overview of the current technological landscape leading to the introduction of the Act, and examines the Act's compatibility with the US *Clarifying Lawful Use of Overseas Data Act* and other international obligations.
- **Chapter 4** examines remaining concerns regarding the Schedule 1 industry assistance framework, while providing policy, law enforcement and intelligence perspectives of the provisions.
- **Chapter 5** considers Schedules 2 to 4, and remaining issues raised by the Inspector-General of Intelligence and Security (IGIS) and industry organisations. The chapter discusses some ambiguity within the

[3] www.aph.gov.au/pjcis

provisions and seeks to recommend clarifications, while asserting the necessity of agencies maintaining the ability to conduct limited telecommunications interception to carryout computer access warrants.

- **Chapter 6** considers the two new powers provided under Schedule 5 of the Act to the Australian Security and Intelligence Organisation (ASIO). The powers relate to the provision of assistance to ASIO in either a voluntary or compelled manner. The chapter also examines the conferred immunity from civil liability on persons aiding ASIO.
- **Chapter 7** provides an overview of the reporting and oversight obligations and considers whether the role of the IGIS and the Committee ought to be extended to other national intelligence agencies.

# 2. Background and previous inquiries

2.1 This chapter discusses the background leading to the inquiry, and briefly summarises the actions of the Committee's previous reviews on the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (TOLA Act), as well as the review undertaken by the Independent National Security Legislation Monitor (INSLM).

## Previous inquiries into the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018*

2.2 The Committee has completed two previous inquiries regarding the TOLA Act; first into the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (TOLA Bill), and a subsequent inquiry into the resultant TOLA Act in the year after it was passed.

### Advisory Report on the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018

2.3 On 20 September 2018 the TOLA Bill was introduced into the House of Representatives by the Minister for Home Affairs, the Hon. Peter Dutton MP, and the Bill was subsequently referred by the Attorney-General, the Hon. Christian Porter MP, to the Committee for inquiry and report.

2.4 The Committee had significant engagement with industry, government agencies and civil society, receiving a total of 105 submissions and numerous

supplementary submissions to the inquiry. The Committee also held five public hearings on the TOLA Bill in October and November 2018.

2.5 On 22 November 2018, the Committee received advice in correspondence from the Minister for Home Affairs that there was an immediate need to provide agencies with additional powers and to pass the TOLA Bill in the last sitting week of 2018. The Minister for Home Affairs, the Hon. Peter Dutton, said:

> The situation has become more urgent in light of the recent fatal terrorist attack in Melbourne and the subsequent disruption of alleged planning for a mass casualty attack by three individuals …
>
> I am gravely concerned that our agencies cannot rule out the possibility that others may also have been inspired by events in Melbourne to plan and execute attacks … This is particularly concerning as we approach Christmas and the New Year, which we know have been targeted previously by terrorists planning attacks against Australians gathered to enjoy the festive season …
>
> For these reasons I ask that the committee accelerate its consideration of this vital piece of legislation to enable its passage by the parliament before it rises for the Christmas break.[1]

2.6 In response to this advice, the Committee sought short-timeframe private briefings from a number of organisations including:

- Australian Security Intelligence Organisation (ASIO)
- Australian Signals Directorate (ASD)
- Department of Home Affairs
- Australian Federal Police (AFP)
- Victoria Police
- Inspector-General of Intelligence and Security (IGIS)

2.7 Following the briefings the Committee accepted that there was a 'genuine and immediate' need for agencies to have tools to respond to the challenges of encrypted communications.

2.8 To address the immediate concerns arising out of the TOLA Bill, the Committee made 17 recommendations for amendment or action, primarily

---

1 Submission 89 to the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 inquiry, as referenced in Parliamentary Joint Committee on Intelligence and Security, *Advisory Report on the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018*, December 2018, p. 2.

aimed at improving the efficacy or oversight of the industry assistance measures in Schedule 1 of the TOLA Bill.

2.9 In response to the Committee's report and expanding on the original Bill, 173 amendments to the TOLA Bill were introduced and passed by the Parliament on 6 December 2018, the final sitting day for 2018.

2.10 These amendments came only one day after the Committee had delivered its Bill review report on 5 December 2019. Some members of the Committee and other interested parties expressed concerns about whether the amendments had fully addressed the Committee's recommendations or what their effect may be, but the inclusion of an immediate review of the Act by the Committee as one of those amendments was accepted as a mechanism to expedite analysis of any such concerns.

2.11 Additionally, though the TOLA Bill was passed by Parliament by the end of 2018, the compressed timeframe meant that the Committee was unable to fully expand or articulate its response to the concerns raised by submitters or explain the rationale leading to the recommendations in its Bill review report. Additionally, the Committee's TOLA Bill review report was limited to recommendations regarding only one of five schedules of amendments brought forward under the TOLA Bill.

2.12 Therefore, amendments made to the TOLA Bill referring the TOLA Act to the Committee to inquire and report in 2019 were welcomed by the Committee.

## Review of the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018*

2.13 The Committee commenced the 2019 TOLA Act review on 17 December 2018. The intent of the inquiry was to clarify the intent of the recommendations made in the TOLA Bill inquiry and to advise Parliament on the extent to which the recommendations made by the Committee in its advisory report were addressed.

2.14 The Committee received 71 submissions and 7 supplementary submissions, and held classified briefings with the ASIO, AFP and the IGIS in February 2019.

2.15 Mr Andrew Hastie MP, Chair of the Committee, and the Hon. Mark Dreyfus QC, MP made statements in the House of Representatives on Tuesday 12 February 2019, updating the Parliament on

the progress of the Inquiry and expressed the Committee's unanimous support for two amendments of the Act to:

- bring forward the timeframe of the INSLM's review of the Act; and
- extend industry assistance powers provided for in the Act to Commonwealth, State and Territory anti-corruption bodies.[2]

2.16 On 13 February 2019, the Government introduced the *Telecommunications and Other Legislation Amendment (Miscellaneous Amendments) Bill 2019* to give effect to these suggested amendments. This Bill lapsed due to the 2019 Federal election and has not been reintroduced.

2.17 On 3 April 2019 the Committee tabled its report into the TOLA Act, with three recommendations. The recommendation provided for a further statutory review by the Committee into the TOLA Act, with a reporting deadline of June 2020, to enable the INSLM to undertake a review of the TOLA Act by 1 March 2020, to ensure resourcing be made available to the INSLM to conduct his review, and to recommend that the Commonwealth oversight bodies – the Commonwealth Ombudsman and the IGIS – be provided adequate resources to oversee compliance with the requirements of the legislation.

2.18 On 12 December 2019 the *Telecommunications (Interception and Access) Amendment (Assistance and Access Amendments Review) Act 2019* received assent and extended the Committee's review deadline to 30 September 2020.

## The Report of the Independent National Security Legislation Monitor into the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018*

2.19 Noting the timing of the 2019 Federal election, the Committee exercised its powers under s7A of the *Independent National Security Legislation Monitor Act 2010* (INSLM Act) to refer the TOLA Act to the INSLM for review, with a report to be provided to the Committee to inform this statutory review.[3]

2.20 Following the extension to the review deadline provided to the Committee by *Telecommunications (Interception and Access) Amendment (Assistance and Access Amendments Review) Act 2019*, the Committee resolved to extend the deadline for the INSLM to review and provide a report by 30 June 2020.

---

2 Mr Andrew Hastie MP, *House of Representatives Hansard*, 12 February 2019, p. 112.

3 Independent National Security Legislation Monitor (INSLM), *Trust but Verify: A report concerning the* Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 *and related matters* ('TOLA Act Report'), pp. 56-57.

2.21 The terms of reference for the inquiry requested the INSLM to consider the safeguards, proportionality and ongoing necessity of the legislation:

> …the operation, effectiveness and implementation of amendments made by the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* and whether the Act: (i) contains appropriate safeguards for protecting the rights of individuals; and (ii) remains proportionate to any threat of terrorism or threat to national security, or both; and (iii) remains necessary.[4]

2.22 The INSLM consulted extensively in Australia, the United Kingdom (UK) and the United States (US) with public and private hearings, stating:

> This travel gave me confidence that the recommendations I now make are based on a full understanding of the operation of the US Clarifying Lawful Overseas Use of Data Act 2018 (CLOUD Act) and the crucial importance of IPCO, both in raising public trust in the exercise of powers similar to those in TOLA and, in the UK, obtaining an agreement with the US Government in relation to the CLOUD Act.
>
> More generally, the consultation and submissions referred to in this chapter, the appendices and elsewhere in this report, have been vital in the conduct of this review and the recommendations I have come to. I thank all concerned for their contributions.[5]

2.23 The INSLM provided his report to the Committee on 30 June 2020.

2.24 The INSLM's report satisfied the statutory requirement of the INSLM Act to review the operation, effectiveness and implications of the TOLA Act within 18-months of Royal Assent.[6]

2.25 The INSLM's report contained 33 recommendations on all aspects of the amendments made by the TOLA Act, as well as the recommending amendments to the INSLM Act to enable own-motion reviews of aspects of the TOLA Act, and recommendations regarding improvements in reporting, disclosure and oversight of the powers granted by the TOLA Act amendments.[7]

---

4 INSLM, TOLA Act Report, p. 259

5 INSLM, TOLA Act Report, pp. 56–57.

6 *Independent National Security Legislation Monitor Act 2010*, s6(1D).

7 A list of the INSLM's recommendations can be found at pages 42-48 of the INSLM's TOLA Act Report.

2.26 This Committee report makes reference to the INSLM's findings and recommendations in subsequent chapters.

## Comprehensive Review of the Legal Framework of the National Intelligence Community (Richardson Review)

2.27 On 30 May 2018 the Attorney-General announced the comprehensive review of the National Intelligence Community's legal framework to be undertaken by Mr Dennis Richardson AC.[8]

2.28 The review was an outcome of the 2017 Independent Intelligence Review to 'consider options for harmonising and modernising the legislative framework that governs the activities of our intelligence agencies to ensure they operate with clear coherent and consistent powers, protections and oversight'.[9]

2.29 The Government released the unclassified version of the Comprehensive Review into Intelligence Legislation as well as the Government response to the review in December 2020.[10]

2.30 The Richardson Review considered that the current authorisation framework was adequate and a 'double-lock' for warrant authorisation was not required.[11]

2.31 The Richardson Review recommended the establishment of a new electronic surveillance Act that would consolidate a number of telecommunications related powers, largely as they relate to the interception of information.

2.32 However, one aspect of the proposed electronic surveillance Act directly related to the performance of functions under the *Telecommunications Act*

---

8 Attorney-General of Australia, *Review of national intelligence legislation*, Media Release, 30 May 2018 <https://www.attorneygeneral.gov.au/media/media-releases/review-national-intelligence-legislation-30-may-2018> viewed 30 September 2020.

9 Attorney-General of Australia, *Review of national intelligence legislation*, Media Release, 30 May 2018 <https://www.attorneygeneral.gov.au/media/media-releases/review-national-intelligence-legislation-30-may-2018> viewed 30 September 2020.

10 Attorney-General of Australia, *Government response to the Comprehensive Review into Intelligence Legislation (Richardson Review)*, Media Release, 4 December 2020 <https://www.attorneygeneral.gov.au/media/media-releases/government-response-richardson-review-4-december-2020> viewed 4 December 2020.

11 Attorney-General's Department, *Report of the Comprehensive Review of the Legal Framework of the National Intelligence Community*, 4 December 2020, p. 61.

*1997* is the current prohibition on requiring a designated communications provider (DCP) to develop a capability to intercept communications.[12] The Richardson Review proposes to remove this prohibition to allow law enforcement and intelligence agencies to engage with DCPs to develop and maintain interception capabilities. The Richardson Review did not consider that this would constitute an expansion of powers, but rather to 'enable agencies to work with industry to develop more targeted and effective interception capabilities, to address particular security and law enforcement challenges'.[13]

2.33 On 9 December 2020 the Attorney-General of Australia, the Hon. Christian Porter MP, introduced the Intelligence Oversight and Other Legislation Amendment (Integrity Measures) Bill 2020 to the House of Representatives to introduce some of the amendments from the Richardson Review. The Bill proposes to expand the oversight functions of the IGIS and the PJCIS, as well as to incorporate some definitional amendments.[14] The PJCIS is considering these matters in its review of the Bill.

# Committee Comment

2.34 The Committee extends its appreciation to the former Independent National Security Legislation Monitor, Dr James Renwick CSC SC, and his office for their efforts in producing the report into the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* which greatly assisted the Committee in its inquiry.

2.35 The Committee also extends its appreciation to industry, departments and civil society for its continued engagement in the Committee's consideration of the TOLA Act, noting that several organisations have submitted to each of the Committee's inquiries. These submissions and engagement in public hearings have also greatly assisted the Committee in its inquiry.

2.36 The Committee notes that the recommendations contained in the Richardson Review report has potential implications for the Committee's consideration and recommendations in this inquiry, especially the recommended implementation of a new electronic surveillance Act. The Committee

---

12 *Telecommunications Act 1997*, s 317GA

13 Attorney-General's Department, *Report of the Comprehensive Review of the Legal Framework of the National Intelligence Community*, 4 December 2020, p. 379.

14 Intelligence Oversight and Other Legislation Amendment (Integrity Measures) Bill 2020, Explanatory Memorandum, p. 8.

considers that the recommendations in the following chapters can be implemented in the immediate term while the broader reforms set out as part of the Richardson Review are considered.

2.37 The Committee acknowledges the circumstances that have influenced the Committee's historical consideration of this legislation, and that the threat of terrorism and other serious crime can require urgency in addressing the needs of law enforcement and intelligence agencies to thwart attempts to cause significant harm.

2.38 The Committee also notes that the circumstances around the TOLA Bill were exceptional and considers that appropriate parliamentary scrutiny is an essential part of the consideration of new powers affecting Australia, its industry and its people. The unprecedented complexity of the Bill, the rapid timeframe for its amendment and passage have ultimately resulted in an effective framework of changes that have enhanced law enforcement and intelligence powers. However, the Committee has undertaken this review with a mind to giving careful consideration to the issues raised in the earlier reviews that could not be addressed then, or that have come to light since.

2.39 Noting the intrusiveness of the powers contained in this legislation, the Committee has given careful consideration to the ongoing appropriateness, effectiveness and necessity of the powers conferred by the TOLA Act.

# 3. International context and obligations

3.1 This chapter discusses the global and domestic threat environment, Australia's international law obligations, and the compatibility of the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (TOLA Act) with the requirements of the CLOUD Act.

## Current and emerging technological landscape

3.2 Digital innovation has occurred in waves since the 1980's, first with the development and adoption of personal computers and then with the introduction of mobile and wireless technology that has greatly expanded the internet.[1] It is estimated that digital industries account for around 11 per cent of GDP in advanced economies and this figure is predicted to grow.[2]

3.3 The Independent National Security Legislation Monitor (INSLM) said that Australia relies on technology and is among the fastest adopters of new communication technologies:

> Day-to-day communication in Australia relies almost wholly on technology that is complex and constantly evolving. Australians have been among the fastest adopters of new communication technologies in the world. We have become almost entirely dependent on these technologies for everyday activities: business operations, financial transactions, economic development, social interactions and public engagement.

---

1 Commonwealth Scientific and Industrial Research Organisation (CSIRO), *Digital Innovation Report*, Report, September 2018, p. 8.

2 CSIRO, *Digital Innovation Report*, Report, September 2018, p. 8.

> Indeed, new and emerging technologies have been at the forefront of burgeoning industries, and enabled the growth and vitality of others, in Australia and around the world. It is believed that in future technologies will be developed that have business, private, military and intelligence applications – for example, neuromorphic hardware, artificial general intelligence, fully autonomous vehicles and robots, and nanotube electronics.[3]

3.4 To allow for innovation and growth, Amazon said that trust in the security of data is an integral part of the uptake of new technology:

> Trust in the security of information is fundamental to business innovation and economic growth – it is crucial in a digital economy. Information security tools, processes and protocols are deployed to protect the personal data of Australian citizens, and the commercial or sensitive information of businesses and governments.[4]

3.5 Encryption is one way that service providers on the internet secure information and build trust with their consumers. Internet Australia said encryption is the foundation of trust on the internet:

> Encryption is a technical foundation for trust on the Internet. It promotes freedom of expression, commerce, privacy, user trust, and helps protect data from bad actors. Encryption and related techniques are also used to build increased security for financial transactions and to protect the private communications of end users. Examples include establishing whether data has been tampered with (data integrity), increasing users' confidence that they are communicating with the intended receivers (authentication), and forming part of the protocols that provide the evidence that messages were sent and received (nonrepudiation).[5]

3.6 However, while increasing encryption ensures consumer confidence in new and emerging forms of technology, it is also an ongoing challenge for national security and intelligence agencies in investigating and prosecuting serious crimes.[6]

---

3 Independent National Security Monitor (INSLM), *Trust but verify: A report concerning the* Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 *and related matters* (TOLA Act Report), p. 98.

4 Amazon, *Submission 17*, p. 2.

5 Internet Australia, *Submission 27*, p. 5.

6 Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (TOLA Bill), Explanatory Memorandum, p. 2.

3.7 At the time the Bill was introduced approximately 90% of telecommunications information lawfully intercepted by the Australian Federal Police used some form on encryption, such as through security messaging applications, social media and Voice over Internet Protocol (VoIP) services.[7]

3.8 When law enforcement and intelligence agencies successfully disrupt criminal activities, users are driven to the 'dark web' which stifles the ability of law enforcement agencies to investigate and prosecute crime:

> The dark web is the part of the internet that allows its users to remain anonymous. It is not easily accessible. The dark web facilitates illegal activity such as child sexual abuse, identity theft, drug and firearm trafficking and the planning of terror attacks.
>
> The use of anonymising technologies has made it easier to commit serious crimes at volume and across jurisdictions. It allows criminals and other malicious actors to operate outside the visibility of law enforcement.[8]

3.9 Several pieces of domestic legislation provide powers to law enforcement and intelligence agencies to intercept and access communications,[9] to use surveillance devices,[10] and allow communications providers to disclose communications when permitted under law.[11]

3.10 Despite this, the Department of Home Affairs said that the utility of the full range of investigatory tools has been undermined by new technology and legislation like the TOLA Act allows agencies to keep pace with the volume of change:

> The utility of the interception framework has been undermined by new technology and the evolving communications environment. While the growth of technologies such as encryption is overwhelmingly positive, it has severely undermined the powers previously granted to law enforcement, national security and intelligence agencies to fulfil their functions. To combat this, successive Governments have reformed the law to ensure these important investigatory powers are adapted to the realities of modern communications.

---

7 TOLA Bill, Explanatory Memorandum, p. 2

8 Department of Home Affairs, *Australia's Cyber Security Strategy 2020*, p. 14.

9 See the provisions of the *Telecommunications (Interception and Access) Act 1979*.

10 See the *Surveillance Devices Act 2004*

11 See the provisions of the *Telecommunications Act 1997*

…

> The passage of this legislation was a further step in modernising the capacity of Australia's law enforcement, national security and intelligence agencies to operate in the rapidly evolving communications environment. Agencies now have access to additional tools and investigatory powers to help them adapt to the pace and scale of technological innovation, and the increasing digital sophistication of those who commit serious crimes or seek to harm our national security.[12]

3.11 In the INSLM's report into the TOLA Act, the threat of terrorism, foreign interference and other serious crimes supported the necessity of a legislative response to the ongoing challenges of encryption.[13] Discussion on the nature of these threats follows.

## Terrorism

3.12 The Committee's consideration of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 was hastened by correspondence from the Minister for Home Affairs indicating the potential for terrorist activity at the end of 2018.[14] The circumstances underpinning the Committee's consideration of the Bill at that time will be discussed further in Chapter 3.

3.13 The Australian Security Intelligence Organisation (ASIO) summarised the current terrorism threat to Australia in its annual report:

> Australia's threat environment is complex, challenging and changing.
>
> Based on current trends, we anticipate that espionage and foreign interference will supplant terrorism as Australia's principal security concern over the next five years. This is not to downplay the threat of terrorism, which represents an ongoing and evolving challenge. Countering threats to life will always be a priority for ASIO. …

---

12 Department of Home Affairs, *Submission 16*, p. 5.

13 INSLM, TOLA Act Report, p. 66.

14 Submission 89 to the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 inquiry, as referenced in Parliamentary Joint Committee on Intelligence and Security, *Advisory Report on the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018*, December 2018, pp. [1]–[2].

> Australia's national terrorism threat level remains at PROBABLE. This means we have credible intelligence that there are individuals in Australia with the intent and capability to conduct an act of terrorism.
>
> Religiously motivated violent extremists want to kill Australians. Groups such as the Islamic State of Iraq and the Levant (ISIL) continue to urge attacks, 24 convicted terrorism offenders are eligible for release over the next 10 years, and some battle-hardened foreign fighters may yet return to Australia.
>
> At the same time, our investigations into ideologically motivated violent extremists, such as racist and nationalist violent extremists, have grown. During 2020–21, these investigations approached 50 per cent of our onshore priority counter-terrorism caseload. …
>
> At the same time, espionage and foreign interference attempts by multiple countries remain unacceptably high.
>
> These attempts occur on a daily basis. They are sophisticated and wide-ranging. They are enabled and accelerated by technology. And they take place in every state and territory, targeting all levels of government, as well as industry and academia. …
>
> I remain concerned about the potential for Australia's adversaries to pre-position malicious code in critical infrastructure, particularly in areas such as telecommunications and energy. Such cyber enabled activities could be used to damage critical networks in the future.[15]

3.14 Dr Isaac Kfir of the Australian Strategic Policy Institute said that there is evidence that those engaging in online violent extremism have moved to online niche communication platforms:

> There is evidence that those engaging in online violent extremism have largely left mainstream social media, opting instead to use niche social media platforms and messaging applications such as Telegram, 4chan, 8chan, Viber, Kik, Ask.fm, etc.[16]

3.15 Mr Mike Burgess, Director-General of ASIO, said that 'encrypted communications damage intelligence collection and coverage in nine out of 10 priority counterterrorism cases'[17] and in its submission to the INSLM's

---

15 Australian Security Intelligence Organisation (ASIO), *Annual Report 2020-21*, pp.4-5.

16 Dr Isaac Kfir, Australian Strategic Policy Institute (ASPI), *Submission 5*, p. 3.

17 Mr Mike Burgess, Director-General, ASIO, *Committee Hansard*, Canberra, 7 August 2020, p. 26.

TOLA Act inquiry ASIO said that 'over 95 per cent of ASIO's most dangerous counter terrorism targets use encrypted communications'.[18]

3.16 The Australian Federal Police (AFP) said they have accessed computer access warrants as provided by Schedule 2 of the TOLA Act on 11 occasions in relation to counter-terrorism matters, with the first issued in April 2019 following the passage of the legislation.[19] The AFP Commissioner said that during the COVID-19 pandemic, the operational tempo of counterterrorism activities undertaken by federal and state police remained high:

> Since September 2014, when the national terrorism threat level was raised, there have been seven attacks, however, nationally, there have been 18 major counter-terrorism disruption operations in response to potential or imminent attacks.
>
> There have been 110 people charged as a result of 51 counter-terrorism-related operations in Australia.
>
> And just since December last year, joint AFP and state police operations have conducted two major counter-terrorism disruptions into potential domestic attacks.
>
> Our operational tempo has remained high during the pandemic.[20]

3.17 At the time of this inquiry Australia's national terrorism threat level is PROBABLE.[21]

## Protecting Australia's interests

3.18 While technology can be used as part of the commission of an otherwise non-technology related offence, technology is increasingly used in the commission of cybercrime.[22]

---

18 INSLM, TOLA Act Report, p. 65.

19 Australian Federal Police (AFP), *Submission 33.2*, p. 8.

20 Commissioner Reece Kershaw, AFP Commissioner, 'National Press Club Address – 22 July 2020', 22 July 2020, <https://www.afp.gov.au/news-media/national-speeches/national-press-club-address-22-july-2020> viewed 30 September 2020.

21 Department of Home Affairs, 'National Terrorism Threat Advisory System', <https://www.nationalsecurity.gov.au/Securityandyourcommunity/Pages/National-Terrorism-Threat-Advisory-System.aspx> viewed 22 October 2021.

22 Australian Signals Directorate (ASD), *ASD Annual Report 2018-19*, p. 14

3.19 During the 2019-20 financial year the Australian Cyber Security Centre (ACSC) responded to more than two thousand cyber security incidents[23] and the most common type of cyber security incident was malicious email.[24]

3.20 The Department of Home Affairs said these types of incidents can involve nation-states and state-sponsored actors targeting governments and infrastructure providers:

> Highly sophisticated nation states and state-sponsored actors continue to target governments and critical infrastructure providers. Australian Government or state and territory government entities were targeted in 35.4% of the incidents the ACSC responded to in the year to 30 June 2020... Around 35% of incidents impacted critical infrastructure providers that deliver essential services including healthcare, education, banking, water, communications, transport and energy.[25]

3.21 ASIO said that Australia remains an attractive target for foreign espionage and interference, and cyber espionage is a scalable and cost-effective mechanism for hostile foreign actors to seek information:

> Foreign states continue to undertake acts of cyber espionage targeting Australian Government, academic, industrial and economic information technology networks and individuals, to gain access to sensitive and commercially valuable information—these threats to Australia's security continue to increase in scale and sophistication. Cyber espionage is a relatively low-risk and scalable means of obtaining privileged information, which adds another potent method to the array of espionage techniques through which foreign intelligence agencies and other hostile actors can target Australians and Australian interests.[26]

## Serious criminal offences

3.22 Technology continues to be a valuable tool in the commission of serious offences for a number of reasons, summarised by the Australian Criminal Intelligence Commission (ACIC) in a 2017 report:

> Technology is attractive to criminals as it can provide anonymity, obfuscate activities and locations, and increase their global reach by connecting them to

---

23 Australian Cyber Security Centre (ACSC), *ACSC Annual Cyber Threat Report: June 2019 to June 2020*, 2020, p. 6.

24 ACSC, *ACSC Annual Cyber Threat Report: June 2019 to June 2020*, 2020, p. 8.

25 Department of Home Affairs, *Australia's Cyber Security Strategy 2020*, August 2020, p. 13.

26 ASIO, *2018-19 ASIO Annual Report*, p. 27.

> potential victims and information around the world. Using technology to commit crime is also significantly more efficient and less resource intensive than traditional methods of perpetrating crime.[27]

3.23 The ACIC also said that encryption was a key tool used by serious and organised crimes groups to impede law enforcement:

> High-end encrypted smartphones continue to be preferred by serious and organised crime groups to reduce visibility of their activities to law enforcement. Multiple OMCGs and other serious and organised crime groups use encrypted communication devices and software applications such as Phantom Secure BlackBerry and Wickr as their primary means of communication, due to the content protection features available on these devices and applications.
>
> Increased availability and ongoing advancement of technology will continue to provide criminals with a diverse range of resources to conduct criminal activity and impede law enforcement investigations.[28]

3.24 The AFP Commissioner said that end-to-end encryption will impact the ability to investigate and prosecute child sex exploitation:

> Between July 2019 to May 2020 - just 10 months - the AFP has laid 1078 Commonwealth Child Exploitation charges against 144 people.
>
> It compares to 74 summons and arrests; and 372 charges laid in the previous financial year.
>
> This crime type is getting worse. The average number of images seized when an offender is arrested has been steadily increasing. In the early-to-mid 2000s, a child sex predator had about 1000 images, now it's between 10,000 to 80,000 images and videos.
>
> …
>
> As a country we need to be more outraged about those who produce and distribute child exploitation material, and we need to be better engaged when the inevitable debate arises with Facebook and other platforms when they move to end- to-end encryption.
>
> To put it simply, when these platforms move to end-to-end encryption, the job becomes harder for police to catch predators. We are very worried about when

---

27 Australian Criminal Intelligence Commission (ACIC), *Organised Crime in Australia 2017*, p. 12.

28 ACIC, *Organised Crime in Australia 2017*, 2017, p. 12.

> that day comes, while on the other hand, paedophiles are counting down the days because they cannot wait.[29]

3.25 The AFP said the TOLA Act framework is essential to their efforts to disrupt criminal activities:

> As noted in our previous submissions and appearances before this Committee, and in the INSLM review of TOLA, the tempo and complexity of the criminal threat environment is ever evolving with increasing use of technology by criminal groups and their networks, to facilitate and obfuscate criminal conduct. TOLA provides an essential framework to strengthen the AFP's ability to overcome technological impediments to lawful access to digital content, where necessary and appropriate.[30]

3.26 In 2018-19 the AFP and the NSW Police reported using Technical Assistance Request powers provided under TOLA for serious criminal offences such as homicide (2), drugs (1), organised offences (2), theft (1), as well as telecommunications and cybercrime offences (11).[31] In 2019-20 the ACIC, the AFP and the NSW Police used Technical Assistance Request powers for cybercrime offences (1), drugs (7), and robbery (1).[32]

# International developments

3.27 The global nature of the telecommunications environment requires a high degree of cooperation between international law enforcement organisations. For member parties, cooperation is facilitated through international treaties such as the United Nations (UN)' *Convention against Transnational Organised Crime*[33] and the Council of Europe's *Convention on Cybercrime*.[34]

---

29 Commissioner Reece Kershaw, AFP Commissioner, 'National Press Club Address – 22 July 2020', 22 July 2020, <https://www.afp.gov.au/news-media/national-speeches/national-press-club-address-22-july-2020> viewed 30 September 2020.

30 AFP, *Submission 33*, p. 3.

31 Department of Home Affairs, *Telecommunications (Interception and Access) Act 1979 Annual Report 2018-19*, 2019, p. 77.

32 Department of Home Affairs, *Telecommunications (Interception and Access) Act 1979 Annual Report 2019-20*, p. 79.

33 *United Nations Convention against Transnational Organised Crime and the Protocols thereto,* opened for signature 12 December 2000, A/RES/55/25 (entered into force 29 September 2003).

34 *Council of Europe Convention on Cybercrime*, opened for signature 23 November 2001, E.T.S 185 (entered into force 1 July 2004).

3.28 These treaties encourage international cooperation and provide for mutual legal assistance processes that allow parties to approach countries that hold information and legally obtain information to assist with the investigation and prosecution of serious offences.[35]

3.29 Under the UN *Convention against Transnational Organised Crime*, countries have the ability to negotiate agreements to clarify or expedite parts of the process. At the time of this report, Australia had 30 bilateral mutual assistance relationships in place.[36] The Council of Europe's *Convention on Cybercrime* does not invite a Party to make alternative procedures or arrangements, but does not prohibit such arrangements.[37]

## UK Investigatory Powers Act 2016

3.30 In 2014 the European Court of Justice declared the precursor to the Investigatory Powers Act – the Data Retention (EC Directive) Regulations 2009 – invalid. The outcome led the United Kingdom (UK) to develop and pass the *Data Retention and Investigatory Powers (DRIPA) Act 2014* (UK).[38]

3.31 In 2015, the UK equivalent to Australia's INSLM presented a report that recommended the establishment of the *Investigatory Powers Act 2016* (UK) and introduced the Investigatory Powers Commissioner's Office (IPCO). The INSLM's TOLA Act report summarises:

> Among other matters, it led to the enactment of the *Investigatory Powers Act 2016* (UK). It also led to the creation of the Investigatory Powers Commissioner's Office (IPCO). For warrants authorising intrusive powers of access equivalent to those conferred by Schedules 1 and 2 of TOLA, in addition to administrative or ministerial approval, there is a 'double-lock' so that retired judges, with access to high level technical advisers, must also approve the exercise of the powers by reference to those judges' assessments of the lawfulness, proportionality and intrusiveness of the proposed warrant.

---

35 See art. 18 of the *United Nations Convention against Transnational Organised Crime and the Protocols thereto*, opened for signature 12 December 2000, A/Res/55/25 (entered into force 29 September 2003), and ch. 3 of the *Council of Europe Convention on Cybercrime,* opened for signature 23 November 2001, E.T.S 185 (entered into force 1 July 2004).

36 Attorney-General's Department, *Australia's bilateral mutual assistance relationships*, <https://www.ag.gov.au/Internationalrelations/Internationalcrimecooperationarrangements/Documents/bilateral-treaties-on-mutual-assistance-in-criminal-matters.pdf> viewed 22 October 2021.

37 INSLM, TOLA Act Report, p. 144.

38 *Investigatory Powers Act 2016*, Explanatory Notes, <https://www.legislation.gov.uk/ukpga/2016/25/pdfs/ukpgaen_20160025_en.pdf> viewed 30 September 2020, p. 9.

> IPCO also performs the complaint and audit functions undertaken in Australia by the Inspector-General of Intelligence and Security (IGIS), the Hon Margaret Stone AO FAAL, and the Commonwealth Ombudsman, Michael Manthorpe PSM.[39]

3.32 The IPCO model and the INSLM's recommendations regarding authorisation processes are discussed further in Chapter 7.

3.33 In 2018, the UN Rapporteur on the promotion and protection of the right to freedom of opinion and expression stated concerns with the technical capability notices provided for under the *Investigatory Powers Act 2016* (UK) and the potential to affect encryption.[40]

3.34 However, in the same year the UN Special Rapporteur on the right to privacy praised the *Investigatory Powers Act 2016* (UK) in its development and implementation of a double-lock system for warrant authorisation and in providing better resourcing for the IPCO.[41]

## US CLOUD Act

3.35 The terms of reference for the inquiry require consideration of whether the provisions of the TOLA Act are compatible with the United States of America (US) *Clarifying Lawful Overseas Use of Data Act* (CLOUD Act). In considering this aspect of the terms of reference, the Committee refers to its September 2021 report on its review of the Telecommunications Legislation Amendment (International Production Orders) Bill 2020 and the passage of the legislation through the parliament which will facilitate Australia's cooperation with the US on cross-border data sharing.

3.36 The US CLOUD Act was introduced in March 2018, stating that a company within US jurisdiction can be required to produce electronic data regardless of where it is stored at the time,[42] and allowing the US to enter into executive agreements with other countries when certain criteria are met:

---

39 INSLM, TOLA Act Report, p. 55.

40 International Civil Liberties and Technology Coalition, *Submission 19*, p. 3.

41 United Nations Human Rights: Office of the High Commissioner, 'UK jointly leads Europe and world on privacy after big improvements, says UN rights expert', 29 June 2018, https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=23297&LangID=E viewed 29 September 2020.

42 United States (US) Department of Justice, *Promoting Public Safety, Privacy and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act,* April 2019, <https://www.justice.gov/opa/press-release/file/1153446/download> viewed 29 September 2020, p. 3.

> The CLOUD Act provides that the United States may enter into CLOUD Act agreements only with rights-respecting countries that abide by the rule of law. In particular, before the United States can enter into an executive agreement anticipated by the CLOUD Act, the CLOUD Act requires that the U.S. Attorney General certify to the U.S. Congress that the partner country has in its laws, and implements in practice, robust substantive and procedural protections for privacy and civil liberties, based on factors such as:
>
> - adequate substantive and procedural laws on cybercrime and electronic evidence, such as those enumerated in the Budapest Convention;
> - respect for the rule of law and principles of non-discrimination;
> - adherence to applicable international human rights obligations;
> - clear legal mandates and procedures governing the collection, retention, use and sharing of electronic data;
> - mechanisms for accountability and transparency regarding the collection and use of electronic data; and
> - a demonstrated commitment to the free flow of information and a global Internet.[43]

3.37 In July 2020 a data-sharing bilateral agreement provided for by the CLOUD Act between the US and the UK came into force, and allows either country to approach a provider to seek stored or live communications through each party's Designated Authority, or approach a communications provider directly for subscriber information.[44]

3.38 Some submitters to the inquiry raised concerns about the compatibility of Australian law with the provisions of the CLOUD Act. The Law Council of Australia said that Australia's laws will be insufficient to allow for an executive agreement to be made under the CLOUD Act:

> The Law Council considers that the current law in Australia as it relates to storing and accessing telecommunications data will be insufficient to allow Australia to qualify for entry into an 'executive agreement' with the US. This means that law enforcement agencies in Australia will be restricted to seeking

---

43 US Department of Justice, *Promoting Public Safety, Privacy and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act*, April 2019, <https://www.justice.gov/opa/press-release/file/1153446/download> viewed 29 September 2020, p. 11.

44 See *Agreement between the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the United States of America on Access to Electronic Data for the Purpose of Countering Serious Crime*, United Kingdom-United States of America, signed 3 October 2019, art. 10 and art. 1.

> access to data held by a service provider in the US through the existing and time consuming MLAT process.[45]

3.39 BSA | The Software Alliance said that the current TAN and TCN process does not provide for merit review and may be considered an arbitrary incursion on individual privacy which does not accord with CLOUD Act requirements:

> In particular, the Assistance and Access Act authorizes the Australian government to issue technical assistance notices (TANs) and technical capability notices (TCNs) to compel private companies to build or implement certain surveillance capabilities, without any recourse to a merits review by an independent judicial authority before or after a TAN or TCN is issued, and limited recourse to judicial review of the administrative decision to issue the TAN or TCN after the fact. Further, while TCNs can only be issued by the Attorney-General with prior approval from the Minister of Communications (and Cybersafety), no such safeguard exists in respect of TANs, which can be issued by the heads of the relevant enforcement agencies with no pre-issuance review by any independent authority.
>
> …
>
> The above shortfalls in the overall TAN/TCN regime (among others) could result in the potentially arbitrary and non-transparent issuance of TANs and TCNs, in turn resulting in an arbitrary impact on privacy and liberties. This, coupled with the general lack of review or oversight by independent authorities in the TAN/TCN issuance process, would pose serious concerns as to whether the pre-conditions for entering into an executive agreement under the CLOUD Act are met.[46]

3.40 In addition, the Law Council of Australia said that the terms of the TOLA Act were incompatible with the *Communications Assistance for Law Enforcement Act 1994* (US) which allows a carrier to deploy an encrypted service that it is not capable of decrypting:

> This Act does not preclude a carrier from deploying an encryption service for which it does not retain the capacity to decrypt if and when requested by lawenforcement to do so. That is, it does not 'mandate that US providers of encrypted communications, devices, and storage services be able to decrypt communications for law enforcement access'. In these circumstances, as

---

45 Law Council of Australia, *Submission 24*, p. 8.

46 BSA | The Software Alliance, *Submission 6*, p. 3. See also International Civil Liberties and Technology Coalition, *Submission 19*, pp. 8-9.

> argued by Riana Pfefferkorn, Associate Director of Surveillance and Cybersecurity at the Stanford Centre for Internet and Society in the United States, citing §2523(b)(3) of the US Code: 'Any executive agreement with Australia is flatly barred from "creating any obligation that providers be capable of decrypting data"'.[47]

3.41 In April 2020, the Committee received correspondence from the US Department of Justice that explained the US position on encryption and indicated that there was nothing in the TOLA Act that would preclude an agreement being made:

> As I discussed at the February meeting, the CLOUD Act requires that the agreements it authorizes be "encryption neutral." The statute provides that CLOUD Act agreements "shall not create any obligation that providers be capable of decrypting data or limitation that prevents providers from decrypting data." 18 U.S.C. 2523(b)(3). This means that CLOUD Act agreements may not create any new requirement on service providers to decrypt communications, nor may CLOUD Act agreements prevent or limit service providers from assisting in decryption. In short, CLOUD Act agreements may not prevent partner countries from addressing encryption requirements in their own domestic laws.
>
> This neutrality allows for encryption issues to be discussed and addressed separately among governments, companies, and other stakeholders pursuant to domestic law and policy, and addressing such requirements in domestic law does not affect a country's eligibility for a CLOUD Act agreement. Accordingly, it is the view of the U.S. Department of Justice that there is nothing in Australia's Assistance and Access Act that would preclude or prevent the conclusion of a CLOUD Act agreement between our governments.[48]

# Committee Comment

3.42 The Committee would like to extend its thanks to the Deputy Assistant Attorney General of the US Department of Justice, Mr Richard Downing, for meeting with the Committee to discuss the compatibility of the TOLA Act with the CLOUD Act.

3.43 While the Committee notes the concerns of submitters regarding the compatibility of the TOLA Act with the provisions of the CLOUD Act, the

---

47 Law Council of Australia, *Submission 24*, p. 9.

48 US Department of Justice, *Submission 30*, p. 1.

Committee must give appropriate weight to the evidence provided by the US Department of Justice that there is nothing within the provisions of the TOLA Act that would preclude the making of an agreement under the CLOUD Act between the US and Australia.

3.44 The Committee accepts the important role of technology in Australia's economy. While the constantly evolving nature of technology and communication allows for growth and innovation, the Committee is sympathetic to the difficulties faced by law enforcement and intelligence agencies in Australia and across the world in combatting serious crime in the face of technological innovation.

3.45 The Committee notes the current terrorism threat levels, and ASIO's and the AFP's assessment of the terrorist threats Australia continues to face. The Committee also notes the evidence of growing serious and organised crime, child exploitation as well as drugs and firearms offences that the powers within the TOLA Act have been used to combat.

3.46 Likewise, the Committee notes that foreign interference and espionage is an ongoing threat to Australia's defence, businesses and individuals, where hostile foreign actors seek to obtain information at the expense of Australia's interests. The Committee is examining this issue further in its inquiry into national security risks affecting the Australian higher education and research sector.

3.47 The Committee acknowledges that Australia's law enforcement and intelligence agencies need a range of tools to combat the likelihood of criminal offenders 'going dark', and agrees with the INSLM that the challenges faced by these agencies warrants a legislative response.

3.48 Additionally, the Committee agrees that trust in the communication and storage of data on the internet is foundational, and appropriate protections should be in place to ensure that the access of this information is reasonable and proportionate to the threat posed by criminal offenders.

3.49 The recommendations made by the Committee in this report attempt to more fully balance the concerns of industry with Australia's national security interests.

# 4. Schedule 1: The Industry Assistance Framework

4.1 This chapter provides an overview of the powers under Schedule 1 of the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (TOLA Act) and examines the remaining concerns of stakeholders in relation to the provisions.

## Overview of Schedule 1 powers

4.2 Schedule 1 of the TOLA Act amended the *Telecommunications Act 1997* as well as additional amendments to the *Australian Security Intelligence Organisation Act 1979* (ASIO Act), the *Criminal Code 1995* and the *Telecommunications (Interception and Access) Act 1979* (TIA Act) to establish the industry assistance framework.

4.3 The industry assistance framework is an attempt to modernise an existing provision of the *Telecommunications Act* 1997 which required Australian telecommunications providers to provide reasonably necessary assistance to Australian authorities.[1] As discussed in Chapter 3, advancement in communications platforms and the global nature of the internet means that the ability of law enforcement to gather information to assist in the investigation and prosecution of serious offences has been tangibly hampered by this historical construct.

4.4 Schedule 1 of the TOLA Act introduces a broader definition of a designated communications provider (DCP) which includes carriers or carriage service providers, as well as a company whose electronic product or service is used

[1] *Telecommunications Act 1997*, s. 313.

by one or more end-users in Australia. Section 317C of the *Telecommunications Act* 1997 provides an extensive list of a designated communications provider and the eligible activities of the person that incur an obligation.

4.5 When the requirements of s317C are met, law enforcement, national security or intelligence agencies may enter into an agreement with a DCP under a technical assistance request (TAR), or these parties may seek a technical assistance notices (TAN) or a technical capability notice (TCN) which requires providers to give assistance.

4.6 Such a request may only be made for an authorised reason. For applications made by ASIO, this must be for the purposes of safeguarding Australia's national security. For applications made by other law enforcement and intelligence agencies, assistance may only be sought for the enforcement of criminal law in the investigation or prosecution of a serious offence incurring a penalty of 3 years or more of imprisonment. These provisions also empower law enforcement agencies to cooperate with mutual legal assistance requests as provided for by the *Mutual Assistance in Criminal Matters Act 1987*.

4.7 Since the commencement of the TOLA Act in December 2018, the only assistance instrument used by law enforcement was a TAR.[2] In general terms, TARs are negotiated between the relevant agency and DCP using a present capability or by building a new capability. The agreement takes the form of a contracting arrangements between parties on matters such as the terms of assistance to be provided, or financial arrangements. In making an agreement under a TAR, a DCP receives immunity from civil liability and computer related offences contained in the *Criminal Code 1995* for conduct undertaken in accordance with the TAR.[3]

4.8 Where an agreement is not reached through the voluntary process, law enforcement or intelligence agencies may seek to access assistance through an existing capability – through a TAN – or require the DCP to establish a new capability through a TCN.

---

[2] Department of Home Affairs, *Supplementary Submission 16.1*, pp. 3–4.

[3] Department of Home Affairs, *Industry assistance under Part 15 of the Telecommunications Act 1997 (Cth): Administrative guidance for agency engagement with designated communications providers*, Document <https://www.homeaffairs.gov.au/nat-security/files/assistance-access-administrative-guidance.pdf> viewed 22 October 2021.

4.9 Chief Officers or their delegates[4] have the ability to issue a TAN, however, prior to State or Territory police forces issuing a TAN they must have their application approved by the Commissioner of the AFP. Prior to issuing a TAN, the chief officer or their delegate must be satisfied that the assistance sought is reasonable and proportionate and also that the notice is practicable and technically feasible.

4.10 A TCN requires the approval of the Minister for Communications and is issued by the Attorney-General on behalf of law enforcement and intelligence agencies. As above, prior to issuing a TAN the Attorney-General must be satisfied that the capability is reasonable and proportionate and also that the assistance is practicable and technically feasible. Further discussion on the appropriateness of the approval process is contained in Chapter 7.

4.11 The Department of Home Affairs explains that an assessment of practicability and technical feasibility considers resourcing and the required technical procedures:

> An assistance instrument is technically feasible when the assistance sought relates to an existing capability that is within the provider's power to utilise or, in the case of TCNs and TARs, where the new capability that is sought is one that the provider is able to build. Conversely, an assistance instrument may not be technically feasible if it is unclear what technical procedure would need to occur in order to provide the assistance or produce the outcome sought or if no technical procedure exists that could produce the outcome that is sought from the assistance.
>
> The assessment of technical feasibility also denotes an assessment of what is technically feasible within the bounds of the legal safeguards in the legislation. For example, consider a situation where it is feasible to enable access to a targeted user's encrypted data carried over an end-to-end encrypted service, however doing so would create a material risk that unauthorised parties could access the data of another, non-targeted user. This activity **would no**t be technically feasible, in a legal sense, within the parameters of the legislation because it would contravene the prohibition against systemic weaknesses.[5]

---

[4] The definition of 'chief officer' is set out in s. 317ZM of the TOLA Act as the Commissioner of the AFP, the Chief Executive Officer of the Australian Crime Commission, and the Commissioner of Police (however designated) of the relevant State or Territory.

[5] Department of Home Affairs, *Industry assistance under Part 15 of the Telecommunications Act 1997 (Cth): Administrative guidance for agency engagement with designated communications providers*, Document <https://www.homeaffairs.gov.au/nat-security/files/assistance-access-administrative-guidance.pdf> viewed 22 October 2021, p. 6

4.12 While the TOLA Act provides a certain degree of flexibility in relation to the types of assistance and capabilities that can be sought, there are limits in place which prevent the introduction of anything that would create a systemic weakness or systemic vulnerability in a whole class of technology. In addition, the TOLA Act also provides that assistance must not have the effect of weakening the information security of a third party.

4.13 In its administrative guidance to industry the Department of Home Affairs says that this protection is broad:

> Put simply, the law treats anything that would jeopardise the integrity and security of data, services and products used by any natural or legal persons, the general public and the business community as a systemic weakness.[6]

4.14 The relevant agency requesting either a TAN or a TCN must consult with a DCP prior to issuing a notice. In addition, for TCNs a DCP may write to the Attorney-General within the consultation period to request that an assessment of the proposed TCN be conducted. Upon receiving such a request, the Attorney-General must appoint two assessors one of whom must have the technical knowledge to determine whether the capability would have the potential to establish a systemic weakness and must have the appropriate level of security clearance, and the other must be a judge of the High Court of Australia, the Federal Court of Australia, the Supreme Court of a State or Territory, or a District Court of a State of Territory who served for a period of at least five years and is now retired.

4.15 The assessors must make a determination in relation to the following issues:

- whether the proposed technical capability notice would contravene section 317ZG
- whether the requirements imposed by the proposed technical capability notice are reasonable and proportionate
- whether compliance with the proposed technical capability notice is practicable
- whether compliance with the proposed technical capability notice is technically feasible, and

---

[6] Department of Home Affairs, *Industry assistance under Part 15 of the Telecommunications Act 1997 (Cth): Administrative guidance for agency engagement with designated communications providers*, Document <https://www.homeaffairs.gov.au/nat-security/files/assistance-access-administrative-guidance.pdf> viewed 22 October 2021, p. 4.

- whether the proposed technical capability notice is the least intrusive measure that would be effective in achieving the legitimate objective of the proposed technical capability notice.[7]

# Impact of implementation on industry bodies

4.16 Submitters considered that the implementation of the TOLA Act had an impact on the economic and business prospects of Australian industry as well as impacts, more generally, on human rights.

## Economic and business impacts of the TOLA Act

4.17 As discussed in Chapter 2, consideration of the TOLA Bill was expedited due to reported imminent terrorism threats. Mary Greene said that the expedited consideration did not give 'due consideration of [its] ramifications in terms of the privacy of all persons in the community regardless of who they are'.[8]

4.18 Additionally, the Australian Civil Society Coalition said that the expedited consideration did not allow for parliamentarians to appropriately indicate concerns as part of the process.[9]

4.19 Several submitters described the negative impact that the implementation of the TOLA Act had or could have on the Australian technology sector.[10]

4.20 Riana Pfefferkorn said that the TOLA Act is affecting Australia's competitiveness in the global market:

> In short, the Act is hurting Australian companies, spooking both current and potential customers, and making other countries look like more attractive options for doing business. If the Government wants to help Australia's young cybersecurity sector become a global leader by closing the gaps in innovation,

---

7 Department of Home Affairs, *Industry assistance under Part 15 of the Telecommunications Act 1997 (Cth): Administrative guidance for agency engagement with designated communications providers*, Document <https://www.homeaffairs.gov.au/nat-security/files/assistance-access-administrative-guidance.pdf> viewed 22 October 2021, p. 20.

8 Mary Greene, *Submission 9*, p. [1].

9 Australian Civil Society Coalition, *Submission 13*, p. [2].

10 Mr David Gates, *Submission* 1, p. [2]; Australian Information Industry Association, *Submission* 7, p. 2; StartupAUS, *Submission 8,* p. [3]; Mr Peter Jardine, *Submission* 10, p. 5; Vault, *Submission* 11, pp. [1]–[2]; Koji Payne, *Submission 18*, p. 3; International Civil Liberties and Technology Coalition, *Submission 19*, p. 4; Access Now, *Submission* 21, p. 1; Communications Alliance, *Supplementary Submission 23*.2, p. 3; Internet Australia, *Submission 27*, p. 5; Altassian; *Submission 31*, p. [1];

> exports, and skills training, it can ill afford to give with one hand while taking away with the other.[11]

4.21 Communications Alliance said that anti-competitiveness is already being observed in Australia's largest ICT providers:

> The geopolitical impact of the Act must be further interrogated, and particular attention should also be focused on the legal and economic implications of the application of the law on Australian Industry. This issue and the already visible anti-competitive consequences of the Act have also been raised by some of Australia's largest ICT businesses and leading software and encryption services providers – it must not be underestimated.[12]

4.22 However, the Department of Communications and the Arts considered that it is not yet possible to ascertain the broader impacts of the TOLA Act:

> While the impacts of assistance requests can be considered on a case-by-case basis, the Department recognises it is difficult to ascertain the broader impacts of the legislation at this stage. This is largely in part due to the infancy of the framework with some processes yet to be bedded down, and the need to protect information about assistance requests and notices.[13]

4.23 Telstra said that since the TOLA Act came into effect, it has been working with the Department of Home Affairs to develop administrative guidance:

> Since passage of the Act, we have been working with the agencies and the Department of Home Affairs to develop administrative guidance on the operation of the assistance and access framework. While we have generally found the operation of the assistance and access framework to represent a workable expansion of the 'reasonable assistance' requirements of the Telecommunications Act 1997, the ability of agencies to request (or require) the development of new capabilities represents a more fundamental change to the way they engage with carriers (or other Designated Communications Providers (DCPs)).[14]

4.24 The Department of Home Affairs has developed administrative guidance for agencies' engagement with DCPs,[15] a factsheet for industry[16] and a factsheet

---

11 Riana Pfefferkorn, *Submission 4*, p. 6.

12 Communications Alliance, *Submission 23*, p. 3.

13 Department of Communications and the Arts, *Submission 25*, p. 3.

14 Telstra, *Submission 22*, p. 2.

15 Department of Home Affairs, *Industry assistance under Part 15 of the Telecommunications Act 1997 (Cth): Administrative guidance for agency engagement with designated communications providers*

for investors,[17] a set of frequently asked questions,[18] and a scenarios factsheet.[19]

4.25 Communications Alliance conducted a survey in December 2019 following the introduction of the TOLA Act. In the survey, 95% of participants assessed that the TOLA Act had a negative impact[20] on the reputation of Australian tech companies in global markets, and 61% of respondents indicated that international or domestic customers expressed concerns about the impact of the TOLA Act on their organisation's products and services.[21]

## Human rights considerations

4.26 A number of submitters considered that the TOLA Act did not appropriately balance the need to uphold Australia's national security with broader human rights considerations.[22]

4.27 As a party to the International Covenant on Civil and Political Rights,[23] Australia has an obligation to, among other obligations, protect the right to

---

<https://www.homeaffairs.gov.au/nat-security/files/assistance-access-administrative-guidance.pdf> viewed 22 October 2021.

16 Department of Home Affairs, *The Assistance and Access Act: what does the industry assistance framework mean for domestic and international companies?*, Factsheet <https://www.homeaffairs.gov.au/nat-security/files/assistance-access-act-information-industry.pdf> viewed 22 October 2021.

17 Department of Home Affairs, *The Assistance and Access Act: what does the industry assistance framework mean for investors?*, Factsheet <https://www.homeaffairs.gov.au/nat-security/files/assistance-access-act-information-investors.pdf> viewed 22 October 2021.

18 Department of Homes Affairs, *Industry assistance under Part 15 of the Telecommunications Act 1997 – Frequently Asked Questions*, Factsheet <https://www.homeaffairs.gov.au/nat-security/files/assistance-access-act-faq.pdf> viewed 22 October 2021.

19 Department of Home Affairs, *Scenarios – industry assistance to law enforcement and national security agencies*, Factsheet <https://www.homeaffairs.gov.au/nat-security/files/assistance-access-act-scenarios.pdf> viewed 22 October 2021.

20 Figure comprised of responses of either 'very negative' (51%) or 'somewhat negative' (44%).

21 Communications Alliance, *Supplementary Submission 23.2*, p. 3.

22 Riana Pfefferkorn, *Submission 4*, p. 3; Australian Information Industry Association, *Submission 7*, p. 8; StartupAUS, *Submission 8*, p. 3; Mary Greene, *Submission 9*, p. 1; Australian Civil Society Coalition, *Submission 13*, p. 1; Koji Payne, *Submission 18*, p. 4; International Civil Liberties and Technology Coalition, *Submission 19*, p. 1; Access Now, *Submission 21*, p. 6; Australian Information Industry Association and BSA | The Software Alliance, *Submission 32*, pp. 1–2.

23 International Covenant on Civil and Political Rights, opened for signature 19 December 1996, 999 UNTS 171 (entered into force 23 March 1976)

privacy[24] and the right to freedom of expression.[25] These specific rights may be limited where the limitation is reasonable, necessary and proportionate to achieving a legitimate aim; such as for the purposes of national security, public order, public health, public morals, and rights and freedoms of others.[26]

4.28 The INSLM considered the interplay of Australia's human rights obligations with the various provisions of the TOLA Act, and said that the High Commission for Human Rights had considered 'legitimate aims' in the context of preventing terrorism and upholding national security:

> The High Commissioner for Human Rights has stated that surveillance on the grounds of national security or for the prevention of terrorism or other crime may be a measure that serves a 'legitimate aim'. However, the degree of interference must be assessed against the necessity of the measure to achieve that aim and the actual benefit it produces towards such a purpose.[27]

4.29 In relation to the Schedule 1 powers, the INSLM referred to the conclusion reached by the Parliamentary Joint Committee on Human Rights (PJCHR) that the TOLA Act may be incompatible with Australia's human rights obligations:

> The PJCHR concluded that, while TARs, TANs and TCNs pursue a legitimate objective and are likely to be rationally connected to that objective, the current regime is unlikely to constitute a proportionate limitation on the rights to privacy and freedom of expression and is therefore likely to be incompatible with those rights.

4.30 Access Now said that the lack of judicial authorisation, discussed in Chapter 7, inappropriately impinged on individual human rights.[28] The INSLM said that the Australian Human Rights Commission mirrored this concern.[29] Part of the concern raised by the parties related to the ability of an affected party

---

24 International Covenant on Civil and Political Rights, opened for signature 19 December 1996, 999 UNTS 171 (entered into force 23 March 1976), Art. 17

25 International Covenant on Civil and Political Rights, opened for signature 19 December 1996, 999 UNTS 171 (entered into force 23 March 1976), Art. 18.

26 Access Now, *Submission 21*, pp. 5–6.

27 Independent National Security Legislation Monitor (INSLM), *Trust but Verify: A report concerning the* Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 *and related matters (*'TOLA Act Report'), p. 152.

28 Access Now, *Submission 21*, pp. 3–4.

29 INSLM, TOLA Act Report, p. 159.

to seek review of a decision, especially where a party is not informed that a request or notice is issued.[30]

4.31 The INSLM identified that others expressed concerns about the potential breadth of 'acts or things' with the ability to be compelled, the current form of limitations on TARs, TANs and TCNs, as well as the definitional matters discussed further below.[31]

4.32 However, the INSLM said that this position was not necessarily supported by 'agency submitters'.[32]

4.33 The INSLM concluded that the TOLA Act was necessary[33] and that the Schedule 1 powers in the TOLA Act would meet the threshold of proportionality for the purposes of the human rights obligations if the central recommendations related to the establishment of an Investigatory Powers Commission were implemented[34] – see Chapter 7 for further discussion.

# Prescribed form for TARs, TANs and TCNs

4.34 The INSLM noted that in the course of the inquiry, a number of TARs were reviewed. Further, the INSLM noted that the form of the TARs varied depending on the issuing authority and the type of information being requested.[35]

4.35 The INSLM suggested that a prescribed form for TARs could provide a set of requirements to be fulfilled as part of the request or notice, and the rights and obligations imposed on the recipient. Additionally, the INSLM said the a prescribed form would allow for a set of standardised data that could be used for reporting purposes:

> I propose that the prescribed form would include key information as to, for instance, the 'listed acts or things' in respect of which the notice issues, the 'eligible activities' of the DCP to which it relates, and the rights and obligations of the DCP in relation to the notice. In this way, it will perhaps perform a similar function to the 'notice to occupier' that Australian Federal

30 INSLM, TOLA Act Report, p. 161.

31 INSLM, TOLA Act Report, p. 159.

32 INSLM, TOLA Act Report, p. 161.

33 INSLM, TOLA Act Report, p. 24.

34 INSLM, TOLA Act Report, p. 25.

35 INSLM, TOLA Act Report, p. 228.

> Police (AFP) members are required to serve on the occupier of premises during the execution of a Crimes Act 1914 (Cth) s 3E search warrant. The inclusion of those details in a prescribed form would also assist agencies in compiling and reporting general information as to their use.[36]

4.36 Internet Australia supported the INSLM's recommendation saying that the use of a prescribed form containing all rights, obligations and options to respond to the issue of a TAR will allow DCPs who are not familiar with TOLA requirements to respond appropriately to the requirements of a TAR.[37]

4.37 The Department of Home Affairs said that it generally supported the introduction of a prescribed form, but noted that such a form would have to provide sufficient flexibility for law enforcement, intelligence agencies and DCPs to negotiate the terms appropriately:

> The Department notes this recommendation and will consider the development of standard forms for the use of technical assistance requests and other industry assistance powers working with all agencies empowered to use the framework. The Department notes advice from agencies that overly prescriptive forms may limit agencies' ability to negotiate with industry and that different organisational requirements will require some flexibility. The Department is also conscious that some standardisation of forms could lead to improved efficiency and lower regulatory burden from an industry perspective, and welcomes comment from industry on the design of forms.[38]

4.38 The Law Council supports the intent of the INSLM's recommendation to provide information on the rights of the recipient to challenge a request or notice, and said that there should be 'consultation with industry and civil society, including the Law Council, on the suite of prescribed forms before they are finalised'.[39]

4.39 The INSLM also suggested that the recommended statutory office of the Investigatory Powers Commission in the Administrative Appeals Tribunal could have the responsibility of establishing a prescribed form for TANs and TCNs.[40]

---

36 INSLM, TOLA Act Report, p. 228. Reporting obligations are discussed further in Chapter 7.

37 Internet Australia, *Supplementary Submission 27.1*, p. 10.

38 Department of Home Affairs, *Supplementary Submission 16.2*, p. 4.

39 Law Council of Australia, *Supplementary Submission 24.1*, p. 10.

40 INSLM, TOLA Act Report, p. 221.

4.40 The Department of Home Affairs said that it had 'previously provided guidelines for the use of the industry assistance framework which are available on the Department's website'.[41]

# Definitional concerns raised by stakeholders

4.41 Stakeholders raised concerns with certain definitional aspects of the TOLA Act, including the scope of the ability to service a notice on a DCP and aspects of the definitions of systemic vulnerabilities and systemic weaknesses.

## Individuals and the definition of designated communications providers

4.42 As mentioned above, the TOLA Act contains a table defining DCPs. Each item commences with 'the person…'[42] and the revised explanatory memorandum explains that '[individuals], as well as body corporates, may be designated communications providers'.[43]

4.43 The INSLM noted that several submitters raised concerns that this construction could lead to a TAR, TAN or TCN being issued to an individual rather than appropriately directed at the relevant carrier or provider.[44] This concern was echoed by submitters to this inquiry.[45]

4.44 The Department of Home Affairs said that it was not the intention of the legislation to serve a TAR, TAN or TCN on a natural person who is an employee of a DCP:

> The intention of the legislation is that a designated communications provider not be taken to include a natural person who is an employee of that designated communications provider, and that designated communications provider only applies to natural persons who are sole traders.[46]

---

41 Department of Home Affairs, *Supplementary Submission 16.2*, p. 6.

42 *Telecommunications and Other Legislation Amendment (Assistance and Access) Act* 2018 (TOLA Act), s. 317C

43 Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018, Revised Explanatory Memorandum, p. 40

44 INSLM, TOLA Act Report, p. 230.

45 See Koji Payne, *Submission 18*, p. 4; Atlassian, *Submission 31*, p. 4.

46 Department of Home Affairs, *Supplementary Submission 16.2*, p. 9.

4.45 The INSLM acknowledged evidence by the Department of Home Affairs to this effect as part of the TOLA Act inquiry, but considered that the definition should put this issue beyond doubt.[47]

4.46 Internet Australia supported the proposal by the INSLM to clarify that the term 'persons' is not taken to 'include a natural person (where that natural person is an employee of a DCP) but only applies to natural persons where that natural person is a sole trader responsible for the relevant eligible activity.[48]

## Systemic vulnerability, systemic weakness and related definitions

4.47 Division 7 of the TOLA Act outlines the limitations on the industry assistance framework. Section 317ZG of the TOLA Act requires that a DCP not be requested or required to build a systemic weakness or systemic vulnerability. These concepts are defined earlier in the TOLA Act as follows:

> **systemic vulnerability** means a vulnerability that affects a whole class of technology, but does not include a vulnerability that is selectively introduced to one or more target technologies that are connected with a particular person. For this purpose, it is immaterial whether the person can be identified.
>
> **systemic weakness** means a weakness that affects a whole class of technology, but does not include a weakness that is selectively introduced to one or more target technologies that are connected with a particular person. For this purpose, it is immaterial whether the person can be identified.[49]

4.48 Communications Alliance said that as presently defined, the definitions of systemic weakness and systemic vulnerability are difficult to understand, ambiguous and too narrow:

> It has proved very difficult to adequately define the terms 'systemic weakness/vulnerability' and 'target technology'. As currently drafted in the Act, these definitions are difficult to understand, ambiguous and – on the basis of initial interpretation - are significantly too narrow. The limitations intended to be given to systemic vulnerability/weakness through the definition of target technology do not achieve the desired objective. Specifically, it is unclear what constitutes a 'class of technology'
>
> …

---

47 INSLM, TOLA Act Report, p. 230.

48 Internet Australia, *Supplementary Submission 27.1*, p. 5.

49 TOLA Act, s. 317B

> Assuming the definition of whole class of technology as proposed by the Department of Home Affairs creates a far too narrow characterisation of what constitutes a systemic weakness or vulnerability and provides avenues for agencies to operate outside the spirit of the legislation.[50]

4.49 In addition, Kaspersky said that the definition of systemic weakness and systemic vulnerability are identical and may contradict the definition of target technology:

> Both definitions are identical, and they do not provide differentiation between 'weakness' or 'vulnerability'. It may be reasonable to avoid duplication and leave one term. Both definitions also contradict the definition of a 'target technology'. The latter definition implies targeting a particular person: 'for the purposes of this Part, a particular carriage service, so far as the service is used, or is likely to be used (whether directly or indirectly) by a particular person, is a target technology that is connected with that person'. However, the Act adds that 'for the purposes of paragraphs (a), (b), (c), (d), (e) and (f), it is immaterial whether the person can be identified (italic - Kaspersky)'. If it is immaterial that the target person can be identified, the provision means that the TOLA would permit bulk interception/surveillance. If the person cannot be identified, he or she shall not be targeted in the first place.[51]

4.50 The INSLM recommended that any mention of systemic vulnerability be removed because it did not reflect the use of the term by law enforcement, intelligence agencies and industry:

> There seems to be little if any difference conceptually or in normal language or technical usage between a 'systemic weakness' and 'systemic vulnerability'. A 'weakness' and a 'vulnerability' are synonymous, at least in the present context. If a 'weakness' is something that is at risk of exploitation then it seems equally accurate to describe it as a 'vulnerability'. Further, none of the materials I have seen, including in response to s 24 notices I issued to police and intelligence agencies, indicated that either of the concepts had any meaning or operation that distinguished one from the other. To the extent that the terms are already used interchangeably in industry and public discourse, there should be no further need to use both in the legislation, especially where they are defined separately. Separate definitions for the same thing invites confusion.[52]

---

50 Communications Alliance, *Submission 23*, p. 5.

51 Kaspersky, *Submission 2*, p. 4.

52 INSLM, TOLA Act Report, p. 208.

4.51 The Department of Home Affairs said that the definition of a 'whole class of technology' is set out in the supplementary explanatory memorandum and is designed to capture actions that make general items of technology less secure:

> As set out in the supplementary explanatory memorandum, the term 'whole class of technology' is intended to capture actions that make general items of technology less secure; a 'class' is a category of technology that includes a product line, or a facet of a product line, or any constituent element of a particular technology that is also widely applied and available. For example, a class of technology encompasses:
>
> - a particular model of mobile phone
> - a particular type of operating system within that model of mobile phone, or
> - a particular form of encryption or authentication that secures communications with that operating system.
>
> As the above indicates, the protection has been broadly cast to be consistent with the Government's general intent to preserve electronic protection. That is, the Assistance and Access Act may not weaken or make vulnerable the services and devices that are used by the general public, business community or legitimate and specialised subsets of either. Any use of an industry assistance power that interacts with the information security of products may only impact the target person/s, or related parties.[53]

4.52 However, the INSLM said that it would be more appropriate to include the definition of 'whole class of technology' in the legislation itself rather than relying on the supplementary explanatory memorandum.[54]

4.53 Systemic weaknesses and systemic vulnerabilities are not taken to include 'target technologies' introduced to a system or device that are connected with a particular person – whether or not the person can be identified.[55]

4.54 The Department of Home Affairs says that the 'target technologies' aspect of the definition provides additional assurance on the circumstances where interaction with encryption is permitted:

> The definition of 'target technology' further reinforces the precise circumstances under which interaction with electronic protections such as encryption is permissible. This definition takes each likely item of technology,

---

53 Department of Home Affairs, *Submission 16*, p. 17.

54 INSLM, TOLA Act Report, p. 209.

55 TOLA Act, s. 317B.

> like a carriage service or electronic service, which may be supplied by a provider, and reinforces that a weakness or vulnerability may only be introduced to the particular technology that is used, or likely to be used by a particular person.
>
> For example, a single mobile device operated by a criminal, or suspected to be used by a criminal, would be classified as a target technology for the purpose of paragraph (e) of the definition. However, a particular model of mobile devices, or any devices that are not connected with the particular person, would be too broad to fall within the definition. This ensures that the services and devices enjoyed by any person other than the target of the power remain unaffected. This is an additional protection to the need to have a valid warrant or authorisation (which are already inherently targeted) in place to lawfully access personal information…[56]

4.55 The INSLM said there was evidence provided regarding the potential breadth of the application of the term 'target technology':

> At the public hearing, Mr Murray of Electronic Frontiers submitted that the term 'target technology' requires clearer guidance because it is unclear, for instance, how it would apply to the Facebook Messenger application.447 Would Facebook Messenger amount to a 'technology' if deployed on a single device? Would Facebook Messenger be classed as a 'whole class of technology' to the extent it operated as an application on all devices around the world, or the totality of a network, or something located on a server either inside or outside Australia?[57]

4.56 The International Civil Liberties and Technology Coalition recommended that the definition of systemic weakness and systemic vulnerability should be amended to specify that the definitions cover any weakness or vulnerability that extends beyond the specifically targeted device or individual:

> We renew our recommendation that these definitions should clarify that systemic vulnerabilities or weaknesses mean any vulnerability or weakness that could or would extend beyond the specifically targeted device or service that the targeted individual is using and is implemented in such a way that any other user of the same device or service, or any other device or service of the Designated Communications Provider, could or would be affected.[58]

---

56 Department of Home Affairs, *Submission 16*, p. 18.

57 INSLM, TOLA Act Report, p. 209.

58 International Civil Liberties and Technology Coalition, *Submission 19*, p. 4.

4.57 The INSLM considered the applications of the limitations placed on requests and notices in the industry assistance framework and noted that it was generally agreed by stakeholders that the legislation should not permit actions which create an unacceptable risk of compromising the security of users.[59] While the INSLM disagreed that any level of risk is unacceptable, and instead recommended an amendment to s 317ZG to articulate the prohibited effects of a systemic weakness:

> I conclude that s 317ZG(4A) should state prohibited effects as follows:
>
> (4A) In a case where a weakness is selectively introduced to one or more target technologies that are connected with a particular person, the reference in sub-s (1)(a) to implement or build a systemic weakness into a form of electronic protection means a reference to any act or thing that creates a material risk that otherwise secure information will be accessed, used, manipulated, disclosed or otherwise compromised by an unauthorised third party.
>
> I further conclude that the following definitions should be introduced:
>
> a. 'Otherwise secure information' means 'information of any person who is not the subject, or is not communicating with the subject, of an investigation'.
>
> b. 'Unauthorised third party' means 'anyone other than a party to the communication, the agency requesting the relevant technical assistance request, technical assistance notice or technical capability notice and/or integrity agencies'.[60]

4.58 Prior to the prorogation of the 45th Parliament, the Telecommunications Amendment (Repairing Assistance and Access) Bill 2020 proposed amendments to the operation of these definitions which would clarify actions that DCPs must not be requested or required to do as part of TARs, TANs or TCNs. The Bill lapsed at the conclusion of the 45th Parliament.

4.59 However, in its submission Atlassian said that the amendments proposed by the Telecommunications Amendment (Repairing Assistance and Access) Bill 2019 provided a starting point for addressing industry concerns with these definitions, but recommended that the protections afforded by the provisions of the Bill should go further:

> Atlassian would also add further protections to the prohibition, as drafted in the provisions of the Bill, to address the specific concerns that industry

---

59 INSLM, TOLA Act Report, p. 210.

60 INSLM, TOLA Act Report, p. 211.

> assistance notices should not be used to prevent improvements to a DCP's security capabilities or to create new points of access into a DCP's electronically protected systems or products that would expose otherwise secure data… With respect to the building of points of access, Atlassian's primary concern is that — once created — a point of access into a DCP's systems and products can be exploited by unauthorised parties without the knowledge of law enforcement or the DCP, and without following the legal procedures required for notices under the Act. This specific example is also helpful to clarify the bounds of the 'material risk' prohibition that already exists in the Act, which is also repeated in the proposed Bill. Given the commercially valuable data entrusted to DCPs like Atlassian and the ongoing threats of intellectual property theft by state-sponsored and private actors alike, this is an important area for clarification.[61]

4.60 The INSLM recommended that the definition of 'target technology' be amended to include examples in statute that would clarify the intention of the powers:

> I conclude that the definition of 'target technology' in s 317B should be clarified through the use of non-exhaustive statutory examples to clarify it refers to the specific instance used by the intended target. For example, whether it includes:
>
> c. the mobile phone service as provided only to one or more specified mobile phone numbers
>
> d. a particular physical device such as the mobile phone that belongs to a target?
>
> 'Class of technology' can then be defined through examples of services used by a group of users broader than the intended target – for example, all Telstra mobile phone subscribers or all subscribers in a particular location.[62]

4.61 The Department of Home Affairs suggested that the existing construction of 'target technology' limits the use of powers to a particular person, or circumstances where 'target technology' is connected to a person.[63] Further the Department said that the inclusion of the term 'electronic protection' within the definition of 'target technology' provides examples of what the term covers, rather than what it doesn't cover.[64]

---

61 Atlassian, *Submission 31*, p. 3.

62 INSLM, TOLA Act Report, p. 210.

63 Department of Home Affairs, *Supplementary Submission 16.2*, p. 9.

64 Department of Home Affairs, *Supplementary Submission 16.2*, p. 9.

4.62 The INSLM noted that submissions to the TOLA Act inquiry considered the definition of electronic protection was 'too vague to provide any useful assistance' and that the definition should also include non-exhaustive examples of what is excluded from its meaning.[65]

4.63 The Department of Home Affairs considers it would be not be practical to exhaustively define current electronic protections and also allow for future technological developments:

> It would be impractical to define all current electronic protections and allow enough flexibility to capture future technologies. For this reason, the definition must remain technologically neutral. Further, what the Monitor describes could amount to a particular interaction with electronic protection rather than a type of protection excluded from the concept of electronic protection itself and may, therefore, be of limited use for setting the boundaries of the concept.[66]

4.64 The New South Wales (NSW) Police Force said it agreed with the Department of Home Affairs, and said that it was important to achieve balance between privacy of data and the need to keep Australians safe:

> NSWPF agree with Department of Home Affairs' position that any clarification or amendment of the term 'systemic weakness' should balance the need for a DCP to keep its customer data secure against the need for law enforcement to access the data to keep Australians safe. An overly restrictive definition could make aspects of the legislation unworkable.[67]

## Serious Australian offences and serious foreign offences

4.65 The industry assistance framework can be exercised in respect of a 'serious Australian offence' or a 'serious foreign offence' which is defined in the *Telecommunications Act 1997* to mean an offence that carries a maximum term of imprisonment for three years or more, or for life.[68]

4.66 The Communications Alliance said that less serious offences than that originally contemplated by the TOLA Bill could be captured by the definition:

---

65 INSLM, TOLA Act Report, p. 230.

66 Department of Home Affairs, *Supplementary Submission 16.2*, p. 9.

67 New South Wales (NSW) Police Force, *Submission 34*, p. 1.

68 *Telecommunications Act 1997*, s. 317B

> When assessing this threshold, it becomes clear that less serious offences, compared to the crimes originally contemplated to be combatted by the legislation (terrorism, child abuse, human trafficking etc.) can be captured by this definition. For example, under the Crimes Act a prank or menacing phone call could satisfy the 3-year prison sentence criterion. Consequently, we strongly recommend raising the threshold for offences which could give rise to the powers of the Act being used.[69]

4.67 Similarly, StartupAUS said that a broad definition of serious offence erodes the exceptional intent of the TOLA Act powers and undermines Australia's reputation in the technology market:

> The result of such a broad definition of serious offence is that rather than the powers under this Act being reserved as a critical measure in times of great need, they will simply fall into regular use as part of the daily toolkit of law enforcement, at significant cost to Australian technology companies, their customers and their products.
>
> In addition, the Act specifies a similar definition for foreign crimes, which may well allow international counterparts to use Australia as a channel to exercising law enforcement power that they do not possess in their native country, further harming Australia's reputation within the technology market.
>
> The definition of 'serious crime' should be restricted only to those crimes which are the stated target of the Act, that pose a genuine and serious threat to Australia and its citizens. Further, the ability to exercise powers in furtherance of other countries' criminal laws should be withdrawn.[70]

4.68 The *Telecommunications (Interception and Access) Act 1979* (TIA Act) provides a definition of serious offence that aligns in some respects with the intent of the industry assistance framework to provide a tool that can assist with the investigation and prosecution of murder, kidnapping, terrorism and national security offences.[71] The Law Council suggested that the definition of serious offence for the purposes of the industry assistance framework should be amended to align with the definition in the TIA Act:

> The Law Council does not support the definition of 'serious Australian offences' and 'serious foreign offences' as introduced by the Government amendments. The Law Council recommends that the definition of 'serious offences' should be consistent with the TIA in so far that 'serious offences' is

---

69 Communications Alliance, *Submission 23*, p. 6.

70 StartupAUS, *Submission 8*, p. [4].

71 *Telecommunications (Interception and Access) Act 1979*, s. 5D

> defined as laws of the Commonwealth, a State or a Territory that is punishable by a maximum term of imprisonment of seven years or more, rather than three years.[72]

4.69 The INSLM noted that the Department of Home Affairs had provided in evidence that the TIA Act powers were appropriately limited because of the intrusive nature of the powers, and that the industry assistance framework does not intrude on privacy and the collection of personal data.[73] However, the INSLM noted that the evidence reviewed did not point to that outcome:

> I have reviewed a selection of agencies' documentation as to how industry assistance powers have been deployed since TOLA commenced. I am satisfied that the investigative steps they make possible can be characterised as less intrusive than telephone interception.[74]

4.70 Consequently, the INSLM said that there was significant benefit in aligning the definition in the *Telecommunications Act 1997* with the definition in the *Telecommunications (Interception and Access) Act 1979*:

> I see significant merit in aligning the definition of 'serious offence' under the Telecommunications Act and the TIA Act. To begin with, both the TIA Act and the Telecommunications Act concern the covert use of coercive powers in the investigation of certain types of offence. Because they have that fact in common, it is sensible that they use the same types of offence as the threshold for the exercise of powers. Further, risks arise from a proliferation of different standards for different powers, without any compelling reason for the distinction. Law enforcement officers are expected to exercise a range of different powers, in different jurisdictions, on application to different issuing authorities, who are tasked to apply different standards depending on the type of power involved. Adding another point of distinction between comparable powers – in terms of thresholds at which they become available for use – is liable to confuse and perhaps contribute to inadvertent excesses of power.[75]

4.71 The Department of Home Affairs said that amending this definition would increase the likelihood that law enforcement agencies would be unable to issue a technical assistance request:

---

72 Law Council of Australia, *Submission 24*, p. 23.

73 INSLM, TOLA Act Report, p. 236.

74 INSLM, TOLA Act Report, p. 237.

75 INSLM, TOLA Act Report, p. 237.

> The Monitor's recommendation would preserve the ability to obtain industry assistance in relation to the interception of telecommunications. However, it would exclude numerous offences which may form the basis of a warrant to obtain stored communications or install a surveillance device. Many technical assistance requests have been given to support the execution of surveillance device warrants. Surveillance devices warrants carry an offence threshold of three years' imprisonment which allows many offences outside of the section 5D threshold to form the basis of an application to use a surveillance device.
>
> Adopting this recommendation would increase the likelihood that law enforcement agencies will be unable to issue a technical assistance request. This recommendation would also limit the availability of industry assistance to overcome technological obstacles frustrating the use of stored communications and surveillance device warrants.[76]

# Committee comment

4.72 The Committee notes the concerns raised by industry bodies in relation to the impact of the introduction of TARs, TANs, and TCNs on Australia's ICT industry, and in particular, notes the survey results provided by the Communications Alliance outlining the perceived negative impact of the TOLA Act powers on industry.

4.73 Additionally, the Committee notes that because TANs and TCNs have not yet been used, it is difficult to quantify the economic impact of the legislation on Australia's ICT industry. The Committee considers that this issue warrants monitoring and recommends that the Department of Home Affairs conduct a periodic survey of industry bodies to ascertain any ongoing economic impacts.

4.74 In the interests of transparency wherever possible regarding the operation of the TOLA Act scheme, the Committee recommends that the result of such a periodic survey be made publicly available.

## Recommendation 1

**4.75 The Committee recommends that the Government implement a periodic survey, starting in three years from the presentation of this report, to ascertain ongoing economic impacts of the TOLA Act legislation on Australia's ICT industry and the results should be made publicly available.**

---

[76] Department of Home Affairs, *Supplementary Submission 16.2*, p. 7.

4.76 The Committees notes the evidence of the INSLM that the format of TARs varies between applications, and that a prescribed format for TARs would assist in ensuring that relevant information regarding the rights and obligations of designated communications providers are adequately articulated. The Committee also notes the benefit of providing consistent information for those who do not often receive TARs, as per the evidence of Internet Australia.

4.77 The Committee therefore recommends that the Department of Home Affairs work with industry, law enforcement and intelligence agencies to develop a prescribed set of requirements for TARs.

## Recommendation 2

**4.78 The Committee recommends the Government, in consultation with relevant stakeholders, develop a prescribed set of requirements for information that must be included in technical assistance requests.**

4.79 The Committee notes the recommendation of the INSLM that the proposed Investigatory Powers Commissioner should have a role in developing a prescribed form for TANs and TCNs, and the evidence from the Department of Home Affairs regarding the development of guidance material to facilitate consistency in industry assistance notices. The Committee expects that consideration of the development of a prescribed form for TANs and TCNs will form part of the Government's consideration of the recommended Investigatory Powers Commission and vesting of powers in the AAT outlined in Chapter 7.

4.80 In relation to definitional matters, the Committee notes the concerns from submitters regarding the potential for individuals to be served with a request or notice under the industry assistance framework. The Committee also acknowledges the evidence provided by the Department of Home Affairs that it is not the intention of the TOLA Act for a request or notice to be provided to an individual when it would more appropriately be directed to the body corporate.

4.81 The Committee considers, therefore, that it would be appropriate to amend this definition to provide assurance to Australian industry and ensure that definition operates as intended. The Committee recommends that the definition of designated communications providers be amended to clarify that it shall not be taken to be a natural person except in the case of a sole trader.

## Recommendation 3

**4.82 The Committee recommends that s317C of the *Telecommunications Act 1997* be amended to clarify that a designated communications provider does not include a natural person, where that natural person is an employee of a designated communications provider, but will only apply to natural persons insofar as required to include sole traders.**

4.83 The Committee notes that the definitions of 'systemic weakness' and 'systemic vulnerability' have unintentionally caused confusion from industry representatives. While the Committee notes the evidence of the Department of Home Affairs that the definition of 'systemic vulnerability' was initially introduced following consultation with industry, the Committee acknowledges the evidence of the INSLM that this definition has not continued following the introduction of the TOLA Act.

4.84 The Committee therefore recommends that the definition of systemic vulnerability be removed from the *Telecommunications Act 1997*.

## Recommendation 4

**4.85 The Committee recommends that Part 15 of the *Telecommunications Act 1997* be amended to remove references to 'systemic vulnerability'.**

4.86 The Committee notes the tangible benefits that arise from ensuring consistency and clarity in legislative definitions. In relation to 'prohibited effects' the Committee acknowledges the recommendation made by the INSLM and believes that this strikes a balance between the views of industry and the view of the Department of Home Affairs. The Committee therefore recommends that the *Telecommunications Act 1997* be amended to provide clarification on 'prohibited effects'.

## Recommendation 5

**4.87 The Committee recommends that s 317ZG of the *Telecommunications Act 1997* be amended to describe the 'prohibited effects' of a technical assistance request, a technical assistance notice or a technical capability notice.**

**Such an amendment could take the form of the words put forward by the Independent National Security Legislation Monitor in his recommendations 9 and 10, and the government may consider incorporation of additional definitions in s317B of the *Telecommunications Act 1997* arising from the proposed amendment.**

4.88 Additionally, the Committee notes the uncertainty raised by industry submitters in relation to 'whole class of technology' given the evidence by Atlassian that there is not a settled industry definition of the term.

4.89 While the Committee notes the concerns of the Department of Home Affairs that a definition could unintentionally restrict the operation of the powers, the Committee considers that a non-binding list of examples of what may constitute a 'whole class of technology' would provide more certainty to industry on their responsibilities in complying with industry assistance framework requests and notices. The Committee therefore recommends that non-exhaustive guidance documents that set out examples of what may constitute a 'whole class of technology' be developed, maintained and published by the Department of Home Affairs.

## Recommendation 6

**4.90 The Committee recommends that the Department of Home Affairs develop, maintain, and publish non-exhaustive guidance documents that set out non-binding examples of what may constitute a 'whole class of technology' for the purposes of defining a systemic weakness.**

4.91 In line with the Committee's recommendation 12 in its August 2021 *Advisory report on the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020,* the Committee considers that the definitions of 'serious offence' and 'relevant offence' should be made consistent across different Acts of Parliament, including the *Telecommunications (Interception and Access) Act 1979*, the *Telecommunications Act 1997* and the *Surveillance Devices Act 2004*.

4.92 The Committee notes it is probable the Government will address the issue of definitions of serious offences with the creation of the proposed Electronic

Surveillance Act. The Committee therefore recommends that the Government commission a review of Commonwealth legislation to provide consistency across different Acts of Parliament of the definitions of 'serious offence' and 'relevant offence' and that this body of work should inform the electronic surveillance bill being considered by the Department of Home Affairs and other departments.

## Recommendation 7

**4.93 The Committee recommends the Government commission a review of Commonwealth legislation to determine whether the concept of 'serious offence', 'relevant offence', and other similar concepts:**

- **should be made consistent across different Acts of Parliament; and**
- **whether the threshold for the concept of 'serious offence' in all Commonwealth legislation should be – at a minimum – an indictable offence punishable by a maximum penalty of seven years' imprisonment or more, with a limited number of exceptions.**

**This body of work should inform, or occur as part of, the eventual electronic surveillance bill being considered by the Department of Home Affairs and other departments.**

# 5. Schedules 2-4

5.1 This chapter provides an overview of the powers in Schedule 2-4, discusses matters raised by both the Inspector-General of Intelligence and Security (IGIS) and industry bodies in relation to the powers, and outlines the Independent National Security Legislation Monitor's (INSLM) findings in relation to these schedules.

## Overview of Schedule 2 to Schedule 4 powers

### Schedule 2

5.2 Schedule 2 of the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (TOLA Act) amends the *Surveillance Devices Act* 2004 to enable federal, and State and Territory law enforcement agencies to obtain computer access warrants when investigating a serious federal offence incurring a punishment of imprisonment of maximum period of 3 years or more.[1]

5.3 Prior to the introduction of the TOLA Act, the Australian Security Intelligence Organisation (ASIO) was required to apply for an interception warrant in addition to a computer access warrant.[2] However, the Department of Home Affairs said 'it is almost always necessary for law enforcement and ASIO to undertake limited interception for the purposes of

---

1 Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018, Explanatory Memorandum, p. 4.

2 Independent National Security Legislation Monitor (INSLM), *Trust but verify: A report concerning the* Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 *and related matters* (TOLA Act Report), p. 80.

executing a computer access warrant'.[3] Therefore, Schedule 2 of the TOLA Act also provided limited interception powers to permit the interception of communications passing over a telecommunication system to assist in the concealment of the fulfilment of the computer access warrant.[4]

5.4 The ability to intercept communications to carry out a computer access warrant is designed to facilitate law enforcement or ASIO entry to premises and, if required, remove a device in order to maintain operational integrity. The Department of Home Affairs said that the ability to remove a computer from premises is 'important in situations where an agency may have to use specialist equipment to access the computer but cannot for practical reasons bring that equipment onto the premises in a covert manner.'[5]

5.5 Schedule 2 introduces an assistance order regime, requiring a specified person to provide any information or assistance that is necessary to allow law enforcement officers to access, copy or convert data (into an intelligible form) that is the subject of a computer access warrant, or subject to an emergency authorisation.[6] Such applications must be made to and approved by an eligible judge or nominated Administrative Appeals Tribunal (AAT) member.[7]

5.6 In executing a computer access warrant the amendments to the *Australian Security Intelligence Organisation Act 1979* (ASIO Act) and the *Surveillance Devices Act 2004* allows law enforcement and intelligence agencies to use force against persons and things in the execution of computer access warrants. The Department of Home Affairs provided an example of how this power would be used in practice:

> … the use of force may be required due to the likely eventualities that officers face while executing a warrant. For example, it may be necessary to use force against a door or a cabinet lock to access a thing on the premises or to use force to install or remove a computer. In the case of force against a person, its use is constrained on the face of the legislation to circumstances where force is required to execute the computer access warrant. For instance, it may be

---

3 Department of Home Affairs, *Submission 16*, p.23

4 *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018*, Sch. 2.

5 Department of Home Affairs, *Submission 16*, p. 24.

6 See *Surveillance Devices Act 2004*, s. 64A.

7 Department of Home Affairs, *Supplementary Submission 16.1*, p. 5.

necessary to use reasonable force if a person is obstructing a doorway into the warrant premises and an officer needs to move past them.[8]

5.7 Schedule 2 of the TOLA Act also amended the *Mutual Assistance in Criminal Matters Act 1987* to allow applications for computer access warrants at the request of a foreign country.[9] During the 2018-19 reporting period, no such applications were made.[10]

5.8 A computer access warrant request made by ASIO can be authorised by the Attorney-General, and an eligible judge or nominated member of the AAT can issue a computer access warrant on behalf of law enforcement.[11] Between 1 July 2019 and 30 June 2020 the Australian Federal Police (AFP) obtained 16 computer access warrants, and during this period two applications for warrants were refused but later issued.[12] In the 2018-19 reporting period, the AFP and the Australian Criminal Intelligence Commission (ACIC) were granted a combined total of eight computer access warrants and in 2019-20 reporting period, the AFP and the ACIC were granted a combined total of 20 computer access warrants.[13]

## Schedule 3 and Schedule 4

5.9 The amendments contained in Schedules 3 and 4 of the TOLA Act cover search warrant provisions contained in the *Crimes Act 1914* and the *Customs Act 1901* for law enforcement and the Australian Border Force (ABF). The Department of Home Affairs said that the amendments contained in these Schedules were designed to modernise search warrants and assistance orders to account for advancements in technology.[14] The INSLM outlined the five main reforms in Schedule 3 as follows:

a. It introduces the concept of 'account-based data'.

---

8 Department of Home Affairs, *Submission 16*, p. 25.

9 INSLM, TOLA Act Report, p. 85.

10 Department of Home Affairs, *Surveillance Devices Annual Report 2018-19*, p. 20; Department of Home Affairs, *Surveillance Devices Annual Report 2019-20*, p. 21.

11 INSLM, TOLA Act Report, pp. 28-29.

12 Australian Federal Police (AFP), *Submission 33*, p. 4.

13 In 2018-19 the AFP were issued seven computer access warrants, and the ACIC were issued one. In 2019-20 the AFP were issued 16 computer access warrants, and the ACIC were issued four. See Department of Home Affairs, *Surveillance Devices Annual Report 2018-19*, p. 19 and *Surveillance Devices Annual Report 2019-20*, p. 20.

14 Department of Home Affairs, *Submission 16*, p. 25.

b. It expands the scope of actions police can take to access electronic data.

c. It permits remote access to data from a place other than warrant premises.

d. It increases the time during which an electronic device moved from warrant premises under s 3K [of the *Crimes Act 1914*] may be retained for processing or examination.

e. It amends both the circumstances in which an assistance order is available and the penalties for failing to comply with that order.

5.10 The definition of 'account-based data' is set out by s3CAA of the *Crimes Act 1914* to provide that if an electronic service has accounts for end users and either the person holds an account or is likely to be a user of an account with an electronic service, and that person can access the data provided by the service, it will be considered account-based data in relation to the person.

5.11 As part of the provisions covering account-based data, the powers allow a law enforcement officer to 'add, copy, delete or alter other data' on a computer or a device for the purpose of obtaining access to data.[15]

5.12 The Department of Home Affairs said that Schedule 3 also allows law enforcement officers to use other computers to give effect to the warrant:

> The law permits executing officers to give effect to the warrant by using other computers – including when remotely accessing data on the device. This measure is appropriately limited by the requirement for the executing officer to have regard for other methods to access relevant data if it is reasonable in the specific circumstance (paragraph 3F(2B)(c) in the Crimes Act and paragraph 199B(2)(c) in the Customs Act). This important safeguard ensures that the use of a third party's computer is not arbitrary, and will only occur if other methods of access cannot reasonably deliver the necessary and lawful outcomes for law enforcement and the ABF.[16]

5.13 The Department of Home Affairs said that the amendments under Schedule 4 of the TOLA Act replicated those provided by Schedule 3 in relation to the ABF powers to provide similar investigatory powers.[17]

5.14 Prior to the introduction of the TOLA Act, the ABF had the ability to seek a search warrant to search premises, but not to search computers or data

---

15 See *Crimes Act 1914*, s. 3F(2A) and s. 3F(2B).

16 Department of Home Affairs, *Submission 16*, p. 26.

17 Department of Home Affairs, *Submission 16*, p. 25.

storage devices.[18] The ABF also had the power to compel assistance with obtaining data through an assistance order.[19] However, the TOLA Act introduced new powers and enhanced existing powers as outlined by the INSLM:

a. It introduced a power for ABF officers to obtain a search warrant in respect of a person.

b. It expanded the ABF's powers in respect of electronic items and access to data in connection with the execution of a search warrant in respect of premises.

c. It increased the time during which a computer or data storage device moved from warrant premises by the ABF for examination or processing may be retained for that purpose.

d. It amended offence provisions and maximum penalties that apply where a person fails to comply with an assistance order.[20]

5.15 Like the law enforcement powers introduced by Schedule 3, the TOLA Act provides the ability for the ABF to 'add, copy, delete or alter other data'.[21] However, in contrast to the powers provided to law enforcement, ABF has not been granted powers in relation to account-based data.[22]

5.16 The most significant amendments to ABF powers are in relation to assistance orders, which have expanded to include 'data storage devices', expansion of liability for failure to comply with an assistance order, and significant increases to penalties for failure to comply with an assistance order.[23]

# Stakeholder views on Schedule 2 to 4 powers

## Industry and civil society concerns

5.17 In comparison with the number of concerns raised in relation to Schedule 1 – as discussed in Chapter 4 – the Committee received significantly fewer submissions from industry and civil society in relation to Schedules 2 to 4.

---

18 Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018, Revised Explanatory Memorandum, p. 23.

19 INSLM, TOLA Act Report, p 92.

20 INSLM, TOLA Act Report, p. 92.

21 See *Customs Act 1901*, s199(4A)(c).

22 INSLM, TOLA Act Report, p. 93. See para. 5.10 above for the definition of account-based data.

23 INSLM, TOLA Act Report, p. 94.

5.18 The Law Council of Australia (hereafter referred to as the 'Law Council') said that a number of concerns raised by them during the Committee's previous inquiries had been addressed.[24] However, the Law Council reiterated concerns regarding the emergency authorisation provisions which would allow for law enforcement to use interception powers without seeking appropriate authorisation:

> The [TOLA] Act introduced section 27A, the effect of which was the lowering of this threshold so that telecommunications interception may be permitted as part of a computer access warrant for a 'relevant' offence, defined in subsection 6(1) of the [*Surveillance Devices Act 2004*] as a Commonwealth offence, or a state offence with a federal aspect, that is punishable by imprisonment for a minimum of three years, or an offence otherwise prescribed in section 6(1) or by the regulation. This is a significant increase in the powers of law enforcement agencies, which does not appear to have been justified as a necessary and proportionate response.
>
> The Law Council is concerned that the amendment to subsection 32(4) of the [*Surveillance Devices Act 2004*] permits telecommunication interceptions under computer access warrants which have received emergency authorisation, meaning they have not been approved by an eligible Judge or a nominated AAT member, and these warrants can be issued for a much broader range of offences.[25]

5.19 The Law Council recommended that the *Australian Security Organisation Act 1979* (ASIO Act) and the *Surveillance Devices Act 2004* be amended to prohibit the use of force in executing computer access warrants.[26]

5.20 The Law Council raised additional concerns in relation to the authorisation powers granted under the ASIO Act and the *Surveillance Devices Act 2004* which allows the Attorney-General, Judge or nominated AAT member to authorise the temporary removal of computers or 'other things' for the purpose of entering specified premises or gaining entry or exiting specified premises.[27]

---

24 Law Council of Australia, *Submission 24*, pp. 46–52

25 Law Council of Australia, *Submission 24*, p. 48.

26 Law Council of Australia, *Submission 24*, p. 17. The International Civil Liberties and Technology Coalition also raised concerns about the use of force provisions in the context of expansion of national security powers (*Submission 19,* pp. 7–8).

27 See s25A of the *Australian Security Intelligence Organisation Act 1979* (ASIO Act) and s27E of the *Surveillance Devices Act 2004*.

5.21 The Law Council said the removal power is too broad as it allows the temporary removal of 'other things' with the potential to apply to any object on the premises in an arbitrary manner.[28] The Law Council recommended that a list of objects permitted to be removed be set out in legislation and that time limits should apply to the removal.[29]

5.22 In regard to concealment of access, the Law Council expressed concern that the absence of a time limit by which the concealment of access powers may be exercised:

> Concealment activities can be done 'at any time while the warrant is in force or within 28 days after it ceases to be in force'. However, if nothing has been done within the 28 day period to conceal the fact a computer has been accessed, they may be authorised 'at the earliest time after the 28-day period at which it is reasonably practicable' to conceal access to a computer under warrant.
>
> The Law Council expressed concerned that the absence of a time-limit by which concealment of access powers may be exercised may authorise privacy-intrusive activities in the absence of the reasonable grounds threshold which underpin the initial warrant…[30]

5.23 In addition, the Law Council suggested that wording relating to 'material' loss caused by concealment of access by ASIO and law enforcement in the ASIO Act and the *Surveillance Devices Act 2004* be revised:

> The requirement that the loss or damage be 'material' sets a higher bar than 'cause *any* loss or damage' – a bar which may be too high for a person to be able to access compensation for loss or damage.
>
> The Law Council recommends that these sections be amended to omit the requirement of 'material'.[31]

5.24 Finally, the Law Council noted that the *Surveillance Devices Act 2004* does not permit disclosures for the purposes of seeking legal advice in relation to computer access warrants, and recommends that the provisions be adjusted to allow for disclosure for the purpose of seeking legal advice.[32]

---

28 Law Council of Australia, *Submission 24*, p. 48.

29 Law Council of Australia, *Submission 24*, p. 49.

30 Law Council of Australia, *Submission 24*, p. 50.

31 Law Council of Australia, *Submission 24*, p. 51.

32 Law Council of Australia, *Submission 24*, p. 52.

5.25 Koji Payne said that computer access warrants – as provided by Schedule 2 – and other warrants amended by Schedule 3 and Schedule 4 of the TOLA Act should explicitly set out the kinds of actions that are permitted in adding, copying, deleting or otherwise altering data for the avoidance of doubt[33] and such provisions should apply to 'serious offences' not offences carrying a term of imprisonment of 3 years.[34]

5.26 In addition, the Media Entertainment and Arts Alliance (MEAA) raised concerns in a submission to the INSLM inquiry regarding the threshold for issue of warrants under Schedule 3, noting that the suspicion on 'reasonable grounds' may be inappropriate to authorise law enforcement to access communications data.[35]

## INSLM findings and recommendations

5.27 The INSLM was satisfied that the computer access warrant regime and associated powers contained in Schedule 2 were both necessary and proportionate.[36] The INSLM accepted the evidence of the Department of Home Affairs that some degree of interception is necessary at times for the purpose of executing a computer access warrant, as well as the assurances that agencies will not use these limited interception powers to circumvent the interception warrant process under the *Telecommunications (Interception and Access) Act 1979*.[37]

5.28 The INSLM considered evidence provided by the Department of Home Affairs, the Australian Human Rights Commission (AHRC) and the Law Council regarding the timeframe in computer access warrants authorising activities taken to conceal the execution of a warrant beyond the expiry date of the warrant. The INSLM noted that the ability to conceal activities taken under a covert computer access warrant was not subject to separate or additional authorisation and that such concealment activity could be undertaken at a location not included as part of the warrant application.[38]

---

33 Concerns regarding the power to 'add, copy, delete or alter data' were also raised by Riana Pfefferkorn (*Submission 4*, pp. 2–3) in the context of the potential impact on freedom of the press.

34 Koji Payne, *Submission 18*, p. 4.

35 INSLM, TOLA Act Report, p. 304.

36 INSLM, TOLA Act Report, p. 39.

37 INSLM, TOLA Act Report, p. 239.

38 INSLM, TOLA Act Report, p. 241.

5.29 Therefore, the INSLM recommended that an agency be required to seek external authorisation to exercise a concealment of access power where it is proposed to occur more than 28 days after the expiry of a warrant.[39]

5.30 Further, where it is necessary that a computer or device is removed from the premises, the INSLM considered the evidence of the Law Council and determined that it is not satisfactory to return a computer or device within 'a reasonable period' and recommended that the relevant provisions be amended to require a computer or device to be returned where it is no longer prejudicial to security or otherwise as soon as reasonably practicable.[40]

5.31 In relation to Schedule 3 and Schedule 4, the INSLM was generally satisfied that the powers conferred were both necessary and proportionate.[41]

5.32 The INSLM discussed the definition of suspicion on 'reasonable grounds' raised by the MEAA and determined that the matter had been settled by case law, citing the decision in *George v Rockett*,[42] where in order to meet the threshold there must be facts present which would cause suspicion in the mind of a reasonable person.[43] The INSLM did not make any recommendation to alter or amend this threshold.

5.33 A number of recommendations were made regarding assistance orders. While the INSLM considered that, given an assistance order may be sought at the same time as a computer access warrant, the seniority of issuing officer for an assistance order was appropriate,[44] the INSLM said that the *Crimes Act 1914* and the *Customs Act 1901* should be amended to specifically state that an assistance order does not authorise the detention of a person where the agency in question does not have any lawful basis to detain an individual.[45]

5.34 The INSLM welcomed the introduction of a monetary penalty for failure to comply with an assistance order as an alternative to imprisonment.[46] At the

---

39 INSLM, TOLA Act Report, p. 39

40 INSLM, TOLA Act Report, p. 243.

41 INSLM, TOLA Act Report, p. 39.

42 [1900] HCA 26; (1900) 170 CLR 104

43 INSLM, TOLA Act Report, p. 305.

44 INSLM, TOLA Act Report, p. 244

45 INSLM, TOLA Act Report, p. 249

46 INSLM, TOLA Act Report, p. 40.

same time, the INSLM suggested additional reporting requirements in relation to assistance orders that will be discussed further in Chapter 7.

## Government agency views

5.35 The Department of Home Affairs said that computer access warrants provided by Schedule 2 are an important covert investigatory tool:

> Computer access warrants are an important covert investigatory tool which allows law enforcement and ASIO officers to search electronic devices and content on those devices. The Assistance and Access Act introduced provisions in the SD Act and ASIO Act to ensure these warrants continue to be operationally effective while respecting the need to appropriately limit access to intrusive powers.[47]

5.36 As indicated above, the AFP and the ACIC have used the computer access warrant powers to assist in a number of investigations since the introduction of the TOLA Act. The AFP indicated that these powers have provided access to evidential material not previously available:

> The AFP notes that they continue [to] explore less intrusive options for current active investigations before application for a computer access warrant which is provided in Schedule 2 of the Assistance and Access Act. Computer access warrants are necessary and the ability to escalate to this level of access is critical to operational effectiveness. The AFP takes the application of such intrusive powers very seriously and with due consideration. These warrants have been used in a very measured and considered way and have provided access to evidence that had not previously been available.[48]

5.37 In considering the recommendations made by the INSLM in relation to the TOLA Act, the Department of Home Affairs supported the INSLM's finding that incidental interception for the purpose of executing a computer access warrant was appropriate.[49]

5.38 The Department of Home Affairs noted there are operational challenges in retrieving devices and concealing access without alerting the subject of an investigation:

---

47 Department of Home Affairs, *Submission 16*, p. 23.

48 Department of Home Affairs, *Submission 16*, p. 9. The ACIC also indicated use of powers under Schedule 2 (p. 10), but due to the classified nature of the investigations was not able to comment further in public fora.

49 Department of Home Affairs, *Supplementary Submission 16.2*, p. 10.

> Officers cannot always reliably predict whether, or when, they will be able to safely enter a premises to retrieve devices or conceal access without compromising a covert operation. For example, a person may unexpectedly relocate their computer or device before it can be removed by law enforcement for concealment purposes. This may ultimately undermine an ongoing investigation. The ability for law enforcement and ASIO to intercept communications pursuant to the purposes discussed above will allow officers to better predict when it is safe and appropriate to enter a premises.[50]

5.39 Noting the risks associated with alerting subjects of an investigation of the execution of a covert warrant, the Department of Home Affairs indicated that it would need to consult with operational agencies regarding the potential impact of the INSLM's recommendation to impose a requirement for external approval where concealment activities are not carried out within 28 days of the expiry of a computer access warrant.[51]

5.40 Superintendent Robert Nelson of the AFP said that there would be operational difficulties with seeking external authorisation prior to undertaking concealment activities:

> It relates to having to go back and obtain a new authorisation. That has an overhead in terms of that. Sometimes the circumstances in which we may effect the removal of a surveillance device are timed more by the suspect. When those opportunities arise we do need to utilise them as quickly and as efficiently as we can. In theory, there could be some delays whilst we obtain that authorisation.[52]

However, Superintendent Nelson considered that external authorisation to extend the ability to undertake concealment activities for an additional window of time, rather than a specific incident, may not adversely impact investigation outcomes.[53]

5.41 The INSLM's recommendation to amend the ASIO Act to require the return of items temporarily removed under a computer access warrant would impose a positive obligation to return items that did not accord with the

---

50 Department of Home Affairs, *Submission 16*, p. 24.

51 Department of Home Affairs, *Supplementary Submission 16.2*, p. 10.

52 Superintendent Robert Nelson, Digital Surveillance Collection, AFP, *Committee Hansard*, Canberra, 7 August 2020, p. 21

53 Superintendent Robert Nelson, Digital Surveillance Collection, AFP, *Committee Hansard*, Canberra, 7 August 2020, p. 21.

requirements of other warrants said the Department of Home Affairs in response to the recommendation.[54]

5.42 Additionally, in relation to the use of force powers in the ASIO Act and the *Surveillance Devices Act 2004*, the Department of Home Affairs said that if law enforcement and intelligence agencies did not have access to these provisions they would be open to civil and criminal prosecution for proportionate actions taken in executing otherwise lawful actions:

> The absence of a power to use reasonable and necessary force could potentially lead to civil action or criminal charges should a law enforcement officer do acts or things against a person proportionate to what is contemplated by warrant. Reasonableness and necessity requires the use of force to be proportionate in all circumstances.[55]

5.43 The Department of Home Affairs indicated that the enhancements enacted by Schedule 3 have been used very regularly by the AFP:

> The Australian Federal Police has used the enhanced search warrant provisions amended by Schedule 3 of the Assistance and Access Act **very regularly across a variety of investigations**. The new search warrant framework has enabled more accurate targeting of suspects and improved identification, access and collection of otherwise secure and encrypted communications.[56]

5.44 The AFP provided an example of the use of the assistance order regime provided by updated s 3LA of the *Crimes Act 1914* to compel assistance with an investigation involving importation of drugs via cryptocurrency through the dark web.[57] The Department of Home Affairs said that there are protections in place under the *Crimes Act 1914* where those subject to an assistance order are not able to assist.[58]

5.45 In addition, the Department of Home Affairs indicated that the amendments to *Crimes Act 1914* enabled the search warrants executed in June 2019 in relation to secrecy offences. The Department noted that the actions permitted by the amendments to the TOLA Act did not allow for a search warrant to destroy or modify the contents of documents:

---

54 Department of Home Affairs, *Supplementary Submission 16.2*, p. 10

55 Department of Home Affairs, *Submission 16*, p. 25.

56 Department of Home Affairs, *Supplementary Submission 16.1*, p. 6.

57 AFP, *Submission 33*, p. 6.

58 Department of Home Affairs, *Submission 16*, p. 41.

Schedule 3 of the Assistance and Access Act expanded the types of actions that may be authorised by a search warrant to include:

- using electronic equipment to access 'relevant data' that is held in a computer or data storage device found in the course of a search, in order to determine whether the data is evidential material of a kind specified in the warrant; and
- using electronic equipment to access relevant 'account-based data' in relation to a person (living or deceased) who is (or was) an owner, lessee or user of a computer found in the course of a search.

This amendment does not authorise officers executing a search warrant to destroy or modify the contents of documents on electronic devices. The power to 'add, copy, delete or alter other data' is used solely to obtain access to data held on a computer system.[59]

5.46 The Department of Home Affairs did not outline a position in relation to the recommendations made by the INSLM pertaining to Schedules 3 and 4.

5.47 However, the Department of Home Affairs confirmed that the assistance orders power under the *Crimes Act 1914* and *Customs Act 1901* do not authorise the detention of an individual where the agency in question does not otherwise have a lawful basis to do so.[60] The AFP confirmed this position.[61]

# Committee comment

5.48 The Committee notes the evidence it has received from the Department of Home Affairs and the AFP regarding the benefits to investigatory processes arising from the implementation of computer access warrants in Schedule 2 and the enhanced assistance order powers under Schedules 3 and 4.

5.49 The Committee accepts the evidence received by the Department of Home Affairs and the conclusion reached by the INSLM regarding the utility and practicality of limited telecommunications interception for the purpose of executing a computer access warrant under Schedule 2 without seeking an additional interception warrant to do so.

---

59 Department of Home Affairs, *Submission 16*, p. 10.

60 Department of Home Affairs, *Supplementary Submission 16.2*, pp. 10–11.

61 Department of Home Affairs, *Supplementary Submission 16.2*, p. 11.

5.50 In addition, the Committee notes the statutory construction of the provision relating to interception which requires the powers to be used only for the purposes of fulfilling activities as specified by the computer access warrant. Noting that such warrants are subject to external consideration by the judiciary or the AAT in the case of law enforcement applications, or the Attorney-General in the case of ASIO applications, the Committee is satisfied with the provisions as currently stated.

5.51 The Committee notes the concerns raised by submitters in relation to the use of force provisions, however, the Committee also notes that a computer access warrant also authorises the physical activity of entering premises and seizing items and is not willing to make a recommendation to restrict use of force powers that would open Australia's law enforcement and intelligence agencies to civil and criminal prosecution for unavoidable but unforeseen incidents that may arise in the course of executing a lawfully obtained warrant.

5.52 The Committee appreciates the careful consideration given by the INSLM in relation to concealment of activities undertaken in the course of executing a computer access warrant. In addition, the Committee notes the evidence provided regarding the potential operational impacts of implementing a requirement to seek external authorisation when undertaking concealment activities.

5.53 The Committee is therefore minded to make a slightly different recommendation that attempts to balance the privacy concerns of submitters and the operational requirements of Australia's law enforcement and intelligence agencies.

5.54 The Committee recommends that authorisation from the Attorney-General or issuing authority be sought for a window of time not exceeding six months from the expiry of the 28 day window provided for by the ASIO Act and the *Surveillance Devices Act 2004*. Further, the Committee recommends that law enforcement and ASIO be authorised to apply for a further period not exceeding six months should concealment activities be unable to be carried out in the initial window of time.

## Recommendation 8

**5.55 The Committee recommends that the relevant provisions of the *Australian Security Intelligence Organisation Act 1979* and the *Surveillance Devices Act 2004* be amended to require the Australian Security Intelligence Organisation and law enforcement agencies to seek external authorisation from the Attorney-General or issuing authority to carry out concealment activities in relation to the execution of computer access warrants following the initial 28 day window provided in the respective acts.**

**The Committee recommends that such an application should allow the Australian Security Intelligence Organisation or law enforcement agencies to carry out concealment activities within a window of time not exceeding six months from the expiry of the initial 28 day window, with the option to seek additional external authorisation for a further six months if required.**

5.56 In relation to Schedule 3 and Schedule 4, the Committee notes that enhancements to the search warrants provisions and assistance orders have provided the AFP with access to evidential material not previously available. In light of such evidence, the Committee considers that the provisions are operating as intended.

5.57 However, the Committee notes the ability to 'add, copy, delete or alter other data' has prompted several submitters to raise concerns regarding the scope of the powers. The Committee has considered these concerns carefully, and has considered the INSLM's views on the evidence received on the matter.

5.58 In the example of the operation of the enhanced Schedule 3 powers provided by the AFP – notwithstanding the execution of these warrants resulted in the Committee's recently concluded inquiry into the impact of law enforcement and intelligence powers on the freedom of the press – the Committee is persuaded that the increasing use of technology in the commission of crime has required law enforcement and intelligence agencies to be provided with the tools to ensure that, where necessary, evidence of access to data and information may be rightfully concealed.

5.59 In the course of its inquiry into the amendments made by the TOLA Act, the Committee has not uncovered any evidence that the ability to 'add, copy, delete or alter other data' would allow law enforcement or ASIO to carry out any of the potential destructive activities raised by submitters in relation to this issue. However, the Committee will continue to monitor this issue.

5.60 The Committee notes the clarifying statement provided by the Department of Home Affairs in its supplementary submission regarding submitter concerns that the assistance orders power in the *Crimes Act 1914* and the *Customs Act 1901*, and supports the conclusion that these powers alone do not authorise the detention of a person.

5.61 However, the Committee considers there is an opportunity to clarify certain aspects of the legislation to align with the accepted intent. Therefore the Committee recommends that the Government make clear that no mandatory assistance order, including those defined in relevant sections of the *Crimes Act* and the *Customs Act 1901,* can be executed in a manner that amounts to the detention of a person where that agency does not otherwise have a lawful basis to detain the person.

## Recommendation 9

**5.62 The Committee recommends that the Government make clear that no mandatory assistance order, including those defined in section 3LA of the *Crimes Act 1914* and section 201A of the *Customs Act 1901*, can be executed in a manner that amounts to the detention of a person where that agency does not otherwise have any lawful basis to detain the person.**

5.63 The Committee discusses the INSLM's recommendations regarding additional reporting and monitoring requirements further in Chapter 7.

# 6. Schedule 5: Operation of ASIO Powers

6.1 This chapter discusses the powers provided to the Australian Security Intelligence Organisation (ASIO) by Schedule 5 of the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (TOLA Act) in relation to voluntary and compulsory assistance requests and the Director-General of Security's statutory powers to confer immunity from civil liability for actions undertaken at the request of ASIO.

## Overview of Schedule 5 powers

6.2 Prior to the introduction of the powers under Schedule 5 of the TOLA Act, ASIO did not have the power to compel assistance from a person in relation to accessing a computer, in contrast to the existing powers given to the Australian Federal Police (AFP) and Australian Border Force (ABF) to compel assistance in appropriate circumstances.[1]

6.3 Powers akin to those provided to the AFP and the ABF were provided by a new s34AAA to the *Australian Security Intelligence Organisation Act 1979* (ASIO Act) provided by amendments in the TOLA Act to allow for a voluntary and compulsory assistance framework.[2]

---

1 Independent National Security Legislation Monitor (INSLM), *Trust but verify: A report concerning the* Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 *and related matters* (TOLA Act Report), p. 95.

2 Department of Home Affairs, *Submission 16*, p. 26. In January 2021 s34AAA, in relation to compulsory assistance orders, became s34AAD following the Assent of the *Australian Security Intelligence Organisation Amendment Act 2020*. The Committee refers to s34AAD in this chapter's Committee comment and recommendations.

6.4 At the request of the Director-General of Security, the Attorney-General may issue a compulsory assistance order compelling a person to assist in accessing data held on a computer or storage device.[3] The INSLM said that compulsory assistance orders must have a tangible connection to an existing warrant:

> The computer or data storage device the subject of an order must have a prescribed connection to a warrant. For instance, the computer or storage device must be the subject of a warrant, or on warrant premises, or be removed or seized under warrant, or found in the course of a search of a person authorised by warrant. The effect of this is that s 34AAA is only available in respect of a computer or device that is already lawfully available to ASIO.[4]

6.5 Additional requirements apply when the computer or device is not on the premises to which the underlying authorising warrants relates, as outlined by the Department of Home Affairs:

> Subsection 34AAA(3) provides additional conditions or safeguards which requires the compulsory assistance order to have regard for the fact that the premises in which the relevant computer or data storage device is located is not the premises that is specified in the warrant in force.
>
> In such circumstances, the order must: specify the period within which the person must provide the information or assistance; and specify the place at which the person must provide the information or assistance; and specify the conditions (if any) determined by the Attorney-General as the conditions to which the requirement on the person to provide the information or assistance is subject.[5]

6.6 Mr Mike Burgess, Director-General, ASIO said that compulsory assistance orders would be used to require an individual to share information to gain access to a device and associated material:

> … it's the issue where they've got a device that they have a password or PIN code to and we would require them to share that with us so we could get access to the device and the material on the device.[6]

---

3 INSLM, TOLA Act Report, p. 30.

4 INSLM, TOLA Act Report, p. 97.

5 Department of Home Affairs, *Submission 16*, p. 27.

6 Mr Mike Burgess, Director-General, ASIO, *Committee Hansard,* Canberra, 7 August 2020, p. 31.

6.7 Prior to issuing the order, the INSLM indicated that there are a number of matters that must be satisfied:

> The Attorney-General may make an order under s 34AAA where satisfied of various things, including the purpose and importance of obtaining the data; that the person the subject of the order has a sufficient connection with the computer or device (or, if not, that he or she is suspected of 'being involved in activities that are prejudicial to security'); and that the person has the knowledge to comply with the order.[7]

6.8 Penalties apply to a failure to comply with a compulsory assistance order when a person is capable of doing so – at the time of this inquiry the penalty included five years' imprisonment or a monetary penalty of 300 units.[8]

6.9 Under the voluntary assistance framework, the Director-General may request a person or body to engage in conduct to assist ASIO in the performance of its functions, where such conduct doesn't involve the commission of an offence against Australian law or result in significant loss or damage to property.[9] The voluntary assistance framework also provides for circumstances where an individual may provide information, including producing a document or making one or more copies of a document, without a specific request from the Director-General of Security.[10]

6.10 Though the Attorney-General was empowered to confer on a person protection from civil or criminal liability where the person engaged in 'special intelligence conduct' by the ASIO Act, there was not a more general immunity power available to ASIO until the introduction of the TOLA Act.[11]

6.11 For both voluntary assistance requests and unsolicited disclosure of information, undertaking actions in compliance with the requirements of the section confers immunity from civil liability.[12] The INSLM noted that the conferral of this immunity is not absolute:

> The immunity that s 21A confers on a person is not absolute. It only applies to conduct which the person engages in 'in accordance with the request' of the Director-General. Further, no protection against liability applies to conduct

---

7 INSLM, TOLA Act Report, p. 97.

8 *Australian Security Intelligence Organisation 1979* (ASIO Act), s. 34AAA(4).

9 *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018*, sch. 5, s. 2.

10 INSLM, TOLA Act Report, p. 30.

11 INSLM, TOLA Act Report, p. 95.

12 See the ASIO Act, s. 21A(1) and s. 21A(5).

that involves an offence against Commonwealth, State or Territory law. Also, it does not apply to conduct that results in significant loss of or damage to property.[13]

6.12 The INSLM further noted the civil liability immunity for unsolicited disclosure of information applied to a more narrow set of provisions than those available in a request made by the Director-General of Security under s 21A of the ASIO Act.[14]

# Remaining issues with Schedule 5 powers

## Industry and civil society concerns

6.13 A number of concerns with the provisions in Schedule 5 were raised by the International Civil Liberties and Technology Coalition, and the Law Council of Australia (hereafter referred to as the Law Council).

6.14 The Law Council remained concerned that the Director-General of Security has the power to make a voluntary assistance request without statutory restriction, and that such a request confers immunity from civil liability – a power historically reserved for the Attorney-General of Australia.[15]

6.15 The International Civil Liberties and Technology Coalition raised concerns about the broad drafting of provisions related to the voluntary assistance framework, which has been interpreted as providing ASIO with the ability to circumvent the technical assistance request (TAR) process in Schedule 1.[16] This position was also supported by the Law Council.[17]

6.16 While a number of the Law Council's recommendations were addressed in part by amendments to the Telecommunications and Other Legislation

---

13 INSLM, TOLA Act Report, p. 96.

14 INSLM, TOLA Act Report, p. 96.

15 Law Council of Australia, *Submission 24*, p. 18.

16 International Civil Liberties and Technology Coalition, *Submission 19*, p. 7.

17 The Law Council suggested that clarification should be provided regarding the relationship between voluntary assistance requests and technical assistance requests (TARs), noting that the construction of the provisions could allow the Director-General of Security to circumvent the more onerous TAR process in favour of the process in s. 21A of the ASIO Act. See Law Council of Australia, *Submission 24*, pp. 18-19.

Amendment (Assistance and Access) Bill 2018,[18] the Law Council indicated there were several ongoing concerns with the provisions of Schedule 5.

6.17 The Law Council suggested that the civil immunity provisions associated with the voluntary assistance requests should not cover 'conduct that causes economic loss or physical or mental harm or injury which might otherwise constitute negligence'.[19]

6.18 When the INSLM's report was available, the Law Council made a number of additional recommendations in a supplementary submission to the inquiry to suggest clarification on aspects of the voluntary assistance powers under s21A of the ASIO Act:

> Subsection 21A(1) request-based immunities should be:
>
> - subject to a maximum period of effect;
> - subject to an express statutory issuing criterion directed to assessing the reasonableness and proportionality of the request for voluntary assistance, including the impact of the civil immunity on third parties whose rights to legal remedies will be extinguished;
> - incapable of immunising the repeated provision of the same act of assistance (that is, a 'standing request' that continues indefinitely or for a prolonged period). Rather, a fresh s 21A request must be made for each act of assistance;
> - subject to express statutory provisions governing variation and revocation; and
> - subject to statutory notification requirements to the Attorney-General and IGIS, if ASIO becomes aware that the person providing voluntary assistance exceeds the limitations of the civil immunity. There should be a corresponding statutory obligation on ASIO to make all reasonable efforts to monitor the conduct of the person upon whom ASIO has conferred immunity under s 21A(1).[20]

6.19 The International Civil Liberties and Technology Coalition said that the provision appeared to authorise 'deprivation of liberty and/or inhumane treatment'.[21] Similarly the Law Council stated that statute should clarify the

---

18 See discussion in Law Council of Australia, *Submission 24*, pp. 53–54.

19 Law Council of Australia, *Submission 24*, p. 19.

20 Law Council of Australia, *Supplementary Submission 24.1*, p. 30.

21 International Civil Liberties and Technology Coalition, *Submission 19*, pp. 7–8.

interaction of the compulsory assistance orders with ASIO's questioning warrant powers:

> Further, there should be statutory clarification of the interaction of compulsory assistance orders under s 34AAA with ASIO's questioning warrants. (That is, where a person who is attending for questioning under an ASIO questioning warrant is issued with a s 34AAA assistance notice during their attendance.)
>
> For example, questions will arise about whether:
>
> - compulsory questioning under the questioning warrant may or must be paused for the purpose of executing the assistance order;
> - the time a person spends complying with the assistance order should be offset against the maximum questioning period under the questioning warrant, in recognition that the person is under coercion; and
> - the legal power of IGIS officials (who are in attendance to supervise compulsory questioning under the questioning warrant) attending the execution of the assistance order at the place of questioning.[22]

Further, the Law Council suggested that consideration of such interactions should form part of the Attorney-General's decision-making process.[23]

6.20 The Law Council also made a number of suggestions regarding improved oversight of ASIO's activities in this regard, which is discussed further in Chapter 7.

## INSLM review and findings

6.21 The INSLM made a number of findings in relation to the voluntary assistance requests and compulsory assistance orders powers provided by Schedule 5 of the TOLA Act.

6.22 In relation to the Director-General of Security's voluntary assistance request powers, the INSLM concluded that amendments should be made to limit the breadth of s21A(1) and clarify its scope.[24] In the view of the INSLM, to

---

22 Law Council of Australia, *Supplementary Submission 24.1*, p. 31.

23 Law Council of Australia, *Supplementary Submission 24.1*, p. 31.

24 INSLM, TOLA Act Report, p. 40

request a person to engage in 'conduct'[25] is a term that is undefined and may operate too broadly,[26] and further, is not necessary:

> Section 21A(1) is both unnecessary and disproportionate. Given ASIO's other powers to obtain information and assistance, I consider it is only necessary for ASIO to have power under s 21A(1) to request what equally could be volunteered under s 21A(5).[27]

6.23 The INSLM noted that the insertion of s16A into the ASIO Act would allow the Director-General of Security to delegate powers to senior position-holders to authorise the making of voluntary assistance requests.[28] The INSLM echoed the observation of the Law Council that allowing the Director-General of Security to confer immunity from civil liability was a significant step, and as a consequence, the INSLM recommended that the powers under s21A should be approved by the Director-General of Security of a Deputy Director-General only.[29]

6.24 The INSLM noted that the legislation is not clear on the interaction between the voluntary assistance requests and TARs, noting that significantly more safeguards exist under the TAR process outlined in Schedule 1:

> The power to issue a TAR under Part 15 of the Telecommunications Act, as introduced by Schedule 1 of TOLA, includes a number of important safeguards. So do other powers under the ASIO Act. It is necessary to make clear that s 21A does not empower the Director-General to circumvent those protections by making the request under s 21A instead.[30]

The INSLM recommended that s21A(1) of the ASIO Act should be amended to make clear that the provisions as described do not allow the Director-General of Security to bypass the requirement to seek a TAR.[31]

6.25 Additionally, the INSLM considered the adequacy of the civil liability provisions for voluntary assistance requests and unsolicited disclosure of information. While the provisions exempt unlawful conduct from conferral

---

25 Section 21A(1) provides for the Director-General of Security to request 'a person or body to engage in conduct'

26 INSLM, TOLA Act Report, p. 251.

27 INSLM, TOLA Act Report, p. 251.

28 INSLM, TOLA Act Report, p. 253.

29 INSLM, TOLA Act Report, p. 253.

30 INSLM, TOLA Act Report, p. 254.

31 INSLM, TOLA Act Report, p. 255.

of civil immunity, the INSLM noted that conduct resulting in significant personal injury could result in the conferral of immunity, leaving the injured individual unable to seek compensation:

> My chief concern is that a person who suffers injury as a result of conduct that ASIO requests not be deprived of the right to pursue compensation for interference to his or her quality of life or ability to earn a living. Only injury of some significance will sound in compensation in any case. On that basis, I consider it appropriate to limit the exclusion to conduct that causes death or serious personal injury to a person.[32]

The INSLM recommended amendments to s21A(1)(e) and s21A(5)(e) to add that the conduct must not result in 'death of or serious personal injury to any person'.[33]

6.26 In relation to compulsory assistance orders, the INSLM received submissions recommending clarification of detention powers under s34AAA. During the course of the inquiry, the INSLM was satisfied that ASIO's power would not be used as a power of detention:

> I assess that there is no real risk that ASIO's power will be construed or exercised as a power of detention, so I consider there is no need to introduce the safeguards that ordinarily apply to detention to which both the Australian Human Rights Commission and IGIS submissions refer.[34]

However, the INSLM recommended expressly stating that the powers under s34AAA do not authorise the detention of a person where ASIO does not otherwise have a lawful basis to do so.[35]

## Government agency views

6.27 In relation to the INSLM's recommendation to limit the Director-General's power to confer civil liability to the types of conduct contained in the unsolicited disclosure of information provision,[36] the Department of Home Affairs said that effective controls on the types of conduct which could have

---

32 INSLM, TOLA Act Report, p. 253.

33 INSLM, TOLA Act Report, p. 253.

34 INSLM, TOLA Act Report, p. 257.

35 INSLM, TOLA Act Report, p. 257.

36 Section 21A(5) confers immunity from civil liability for providing information or documents to ASIO where the person reasonably believes the conduct will assist ASIO in the performance of its functions, subject to limitations.

immunity from civil liability are already contained in the section, and amendments would provide a disincentive for cooperation:

> The types of conduct where the conferral of civil immunity is available are effectively limited by the restrictions in paragraphs 21A(1)(d) and 21A(1)(e) to only conduct which does not amount to the commission of an offence against a law of the Commonwealth, a State or Territory, or which does not result in significant loss of, or serious damage to, property.
>
> Implementing this recommendation could remove a potential incentive for external sources to cooperate with ASIO by closing an avenue to provide them with a limited civil immunity where their actions may otherwise give rise to an action against them.[37]

6.28 Mr Mike Burgess, Director-General, ASIO indicated that implementing the INSLM's recommendation to confine immunity powers to the same conduct as listed under s 21A(5) would cause operational difficulties for ASIO:

> It was recommendation 19, which is that the scope of 21A(1) be limited to the scope of 21A(5). We think narrowing of those powers needs further consideration. We can use the current provisions under section 21A to provide legal protections to an entity that will provide voluntary assistance to us to physically access a facility. That is a circumstance where narrowing it would cause a problem for us, and therefore I don't agree with what the INSLM was thinking about. I'm sure he was thinking about information and access, but this is slightly different and we'd use it in a different way.
>
> …
>
> We believe it would stop us from doing things like asking someone for voluntary assistance to get physical access to a facility to set up an observation post, for example.[38]

6.29 In addition, the Department of Home Affairs indicated that the INSLM's recommendation to restrict the ability of the Director-General of Security to delegate voluntary assistance request powers may affect ASIO's operational responsiveness in an emergency situation[39] and further, that the ability to confer immunity through voluntary assistance as written is proportionate and appropriate:

---

37 Department of Home Affairs, *Supplementary Submission 16.2*, p. 11.

38 Mr Mike Burgess, Director-General, ASIO, *Committee Hansard,* Canberra, 7 August 2020, p. 30.

39 Department of Home Affairs, *Supplementary Submission 16.2,* pp 11–12.

> The Director-General is responsible for issuing requests for assistance under section 21A of the ASIO Act. The Director-General represents the highest-level of authority in ASIO and is well equipped to consider the grounds of an order and considerations of reasonableness and necessity. Given the authority of the Director-General, the community can be satisfied that any request issued is proportionate and relevant for ASIO's functions which includes maintaining national security.[40]

6.30 In addition, the Department of Home Affairs said that the Director-General of Security's ability to issue an evidentiary certificate under subsection 21A(8) provides the factual basis of the request and details how the conduct was likely to assist ASIO in its operations, giving further confidence on the use of the power.[41]

6.31 The Inspector-General of Intelligence and Security (IGIS) raised a concern that there is no requirement set out in statute for the Director-General of Security to consider the reasonableness and proportionality of conduct undertaken in relation to conduct associated with carrying out a voluntary assistance request.[42] The IGIS noted this omission is in contrast to the proportionality requirements in the statutory authorisation criteria applying to the Attorney-General for ASIO's special intelligence operations, which also confers immunity from civil liability on participants.[43]

6.32 Mr Mike Burgess, Director-General, ASIO said that he agreed with the proposal in principle to require consideration of the reasonableness and proportionality, but would have to consider the drafting of any amendment and potential operational impacts.[44]

6.33 The IGIS said that the powers under s 21A(1) was 'not subject to equivalent statutory decision-making criteria, statutory limitations, or a statutory requirement to keep written records of reasons.[45]

6.34 In relation to the IGIS' comments on keeping written records of reasons when issuing voluntary assistance requests, Mr Mike Burgess, Director-

---

40 Department of Home Affairs, *Submission 16*, p. 38.

41 Department of Home Affairs, *Submission 16*, p. 38.

42 Inspector-General of Intelligence and Security (IGIS), *Submission 28*, p. 7.

43 IGIS, *Submission 28*, p. 7.

44 Mr Mike Burgess, Director-General, ASIO, *Committee Hansard,* Canberra, 7 August 2020, pp. 28–29.

45 IGIS, *Submission 28*, p. 7.

General, ASIO indicated his agreement with an amendment to require retaining written reasons and said that this practice already formed part of internal processes.[46]

6.35 The IGIS also indicated that consideration may be given to implementing a maximum period of effect for voluntary assistance requests, and statutory requirements to govern how requests may be varied or revoked.[47]

6.36 In relation to submitter's concerns and the recommendation made by the INSLM to clarify that the voluntary assistance provisions are not designed to replace the TAR process in Schedule 1, the Department of Home Affairs said that an amendment to clarify the intent of the provisions may prevent ASIO from using the powers in legitimate circumstances:

> This would have the effect of preventing subsection 21A(1) being used to seek assistance when the assistance would be sought from an entity which is also a designated communications provider and where the assistance is of the same kind, class or nature as those listed acts or things set out in subsection 317E(1) of the Telecommunications Act.
>
> Adopting this recommendation may frustrate ASIO's ability to issue similar assistance requests to multiple different entities simultaneously where some entities are designated communications providers and may be given a technical assistance request or notice, while others are not. This would confer different legal protections and place entities within different legal frameworks when they provide ASIO with the same type of assistance simultaneously.[48]

6.37 Ms Heather Cook, Deputy Director-General, ASIO said that steps to clarify the use of voluntary assistance requests and TARs would not cause a particular problem for ASIO:

> The IGIS has indicated that there is significant overlap. There is some overlap. I'm not sure if we would describe it as significant, so that indicates that there are different reasons why we would use 21A as opposed to, for instance, a technical assistance request. But, in terms of aligning those requirements, there's not a particular problem with that. But there are different reasons why we would be using them.[49]

---

46 Mr Mike Burgess, Director-General, ASIO, *Committee Hansard,* Canberra, 7 August 2020, p. 29.

47 IGIS, *Submission 28*, 7.

48 Department of Home Affairs, *Supplementary Submission 16.2*, p. 12.

49 Ms Heather Cook, Deputy Director-General, Intelligence Service Delivery, ASIO, *Committee Hansard*, Canberra, 7 August 2020, p. 28.

6.38 Mr Mike Burgess, Director-General, ASIO, in responding to general industry concerns that the powers under s34AAA of the ASIO Act could be used to compel industry assistance without using the more onerous provisions of Schedule 1, stated that clarification of the operation of s34AAA to exclude industry personnel unless they were the target of an investigation would not interfere with the intended operation of the provisions.[50]

6.39 In relation to compulsory assistance powers under 34AAA, the IGIS echoed the concerns of other submitters that the construction of statute could confer a power of detention.[51] The Department of Home Affairs indicated that was not the intention of the powers.[52] Mr Mike Burgess, Director-General, ASIO said that amending the section to provide clarification would not be an issue for ASIO.[53]

6.40 The IGIS noted, additionally, that there is no requirement to serve an order on the person who is subject to the order, meaning a person could technically be in breach of an order they are unaware exists.[54] Mr Mike Burgess, Director-General, ASIO said that amending the provision to state that a compulsory assistance order was not enlivened until served on the particular person would not cause operational issues for ASIO.[55]

6.41 Similarly, the IGIS noted there is currently no requirement to inform a person subject to the order the place at which they must attend, the period of timing they must render assistance, the information or assistance they are obligated to provide nor any other conditions the Attorney-General has imposed on the order.[56]

6.42 Mr Mike Burgess, Director-General, ASIO said that ASIO would be open to considering amendments in this regard, noting that ASIO may not always have all information available at the time an order was made:

> I think the [Inspector-General] nailed it, though, when she said we may not know at the time. But, of course, when we are in that process of wanting to

---

50 Mr Mike Burgess, Director-General, ASIO, *Committee Hansard,* Canberra, 7 August 2020, p. 31.

51 IGIS, *Submission 28*, p. 9.

52 Department of Home Affairs, *Supplementary Submission 16.2*, p. 12.

53 Mr Mike Burgess, Director-General, ASIO, *Committee Hansard,* Canberra, 7 August 2020, p. 30

54 IGIS, *Submission 28*, p. 8.

55 Mr Mike Burgess, Director-General, ASIO, *Committee Hansard,* Canberra, 7 August 2020, p. 29.

56 IGIS, *Submission 28*, pp. 8-9.

execute on it, we may know further, so I'm open to consideration on this one. I can't think of anything that's materially problematic for us.[57]

# Committee comment

6.43 The Committee notes the evidence received from civil society and government agencies regarding the operation of Schedule 5 of the TOLA Act, and opportunities to clarify the intent of certain provisions to ensure the appropriate balance is achieved ensure appropriate flexibility to address operational requirements, and the removal of ambiguity in the operation of the Schedule.

6.44 In relation to the concerns raised by the Law Council and the INSLM regarding the potential delegation of voluntary assistance requests and unsolicited provision of information to a range of ASIO officers, the Committee agrees that providing the power to confer immunity from civil liability to the Director-General of Security is a significant step.

6.45 While the Committee acknowledges that requiring senior ASIO officers to approve voluntary assistance requests as per the recommendation by the INSLM may result in some delay, the Committee is not convinced that requiring the Director-General or a Deputy Director-General to authorise such requests would result in an unacceptable delay to ASIO's operations. The Committee therefore recommends that the relevant provisions of the ASIO Act be amended to require the Director-General or Deputy-Directors-General within ASIO to authorise powers under s21A.

## Recommendation 10

**6.46 The Committee recommends that s21A of the *Australian Security Intelligence Organisation Act 1979* be amended to limit authorisation of activities under voluntary assistance provisions to the Director-General of Security and Deputy Directors-General of the Australian Security Intelligence Organisation.**

6.47 In addition, the Committee notes the concerns raised by the Law Council and the INSLM regarding the scope of conferral of immunity from civil liability which could preclude individuals from seeking a remedy as a result of serious personal injury or serious damage to property.

---

57 Mr Mike Burgess, Director-General, ASIO, *Committee Hansard,* Canberra, 7 August 2020, p. 29.

6.48 Though the Department of Home Affairs suggests that the current construction of the provisions excluding unlawful conduct from eligibility for conferral of civil immunity provides sufficient legal coverage in the event of loss, the Committee is persuaded by the arguments put forward by the INSLM, noting that conduct that falls short of illegality can still result in serious personal injury or serious damage to property. Therefore, the Committee recommends that that the scope of immunity from civil liability in s21A of the ASIO Act be confined to 'conduct that does not result in serious personal injury or death to any person or significant loss of, or serious damage to, property'.

## Recommendation 11

**6.49 The Committee recommends that s 21A(1)(e) and s 21A(5)(e) of the *Australian Security Intelligence Organisation Act 1979* be amended to confine the scope of the immunity from civil liability offered under the Act to 'conduct that does not result in serious personal injury or death to any person or significant loss of, or serious damage to, property'.**

6.50 The Committee notes that a number of concerns raised by submitters related to the broad construction of s21A. The Committee notes the evidence of the Department of Home Affairs and ASIO that the power would be used in a broad range of circumstances and considers that a certain degree of flexibility is required. The Committee has considered the INSLM's recommendation to limit the scope of assistance that can be requested to that contained in s21A(5) for voluntary assistance requests, but, noting the evidence received from the Director-General of Security regarding the range of matters for which ASIO could request assistance, the Committee is not minded to recommend such a change at this point.

6.51 The Committee expects that ASIO will have robust internal guidance surrounding the matters for which ASIO can request voluntary assistance.

6.52 However, noting the conferral of immunity from civil liability arising from s21A, the Committee recommends that requiring the Director-General of Security to have consideration of the reasonableness and proportionality of a voluntary assistance request would bring this section closer to other powers for which civil liability immunity applies.

## Recommendation 12

**6.53 The Committee recommends that s21A of the *Australian Security Intelligence Organisation Act 1979* be amended to require the Director-General of Security to be satisfied of the reasonableness and proportionality of the conduct of a voluntary assistance request prior to issuance.**

6.54 In addition, the Committee notes the IGIS' suggestion that ASIO be required to keep written reasons underlying a voluntary assistance request, and the evidence provided by the Director-General of Security that this is a practice already undertaken by ASIO. To ensure the alignment of statutory requirements with existing practice, the Committee recommends that s21A of the ASIO be amended to require the retention of reasons underpinning a voluntary assistance request.

## Recommendation 13

**6.55 The Committee recommends that s21A of the *Australian Security Intelligence Organisation Act 1979* be amended to require the Australian Security Intelligence Organisation to retain written reasons underpinning a voluntary assistance request.**

6.56 The Committees notes the concerns raised by submitters in relation to the potential power to circumvent TAR powers in issuing a voluntary assistance request or compulsory assistance order. The Committee appreciates the evidence from the Department of Home Affairs and ASIO to advise that is not the intent of the powers in Schedule 5, however, the Committee considers there is value in amending s21A and s34AAD to ensure the sections operate as intended.

## Recommendation 14

**6.57 The Committee recommends that s21A and s34AAD of the *Australian Security Intelligence Organisation Act 1979* be amended to state that nothing in either section authorises the Director-General of Security to make a request of a person that is properly the subject of a technical assistance request as set out by s317G of the *Telecommunications Act 1997*.**

6.58 In relation to the concerns raised by submitters that the construction of s34AAD powers under the ASIO Act may provide a detention power, the Committee notes the evidence received by the Department of Home Affairs

and ASIO to clarify detention is not the intent of the provision. The Committee also notes the INSLM's finding regarding the intent of the power, and supports the INSLM's conclusion on this matter.

6.59 The Committee recently concluded its inquiry into the Australian Security Intelligence Organisation Amendment Bill 2020 which proposed replacing the detention framework provided by Division 3 of the ASIO Act with a more limited apprehension framework designed to ensure attendance at questioning. The Committee's references to 'detention' in this report reflect the common meaning of the term rather than the provisions proposed for repeal and replacement by the ASIO Amendment Bill 2020.

6.60 The Committee notes that there may be legitimate scenarios where a person attending questioning as part of the revisions to the ASIO Act may also be subject to an assistance order under s34AAD of the ASIO Act. However, to align with the stated intent put forward by the Department of Home Affairs, the Committee recommends that the Government make clear that the compulsory assistance order power in the ASIO Act does not authorise the detention of a person to whom the order applies where the ASIO does not otherwise have any lawful basis to detail the person.

## Recommendation 15

**6.61 The Committee recommends that the Government make clear, for the avoidance of doubt, that the compulsory assistance order power in s34AAD of the *Australian Security Intelligence Organisation Act 1979* does not authorise the detention of person to whom the order applies where the Australian Security Intelligence Organisation does not otherwise have any lawful basis to detain the person.**

6.62 The Committee notes the IGIS' evidence that, as written, the compulsory assistance orders do not require that they be served on an individual to take effect, nor that there is any requirement to inform the subject of a compulsory assistance order of a number of conditions imposed by the order. Given the penalty related to non-compliance with a compulsory assistance order, the Committee considers that the s34AAD should be amended to provide for additional conditions attached to the making of such orders.

6.63 The Committee, therefore, recommends that s34AAD be amended to state that the requirement to comply with a compulsory assistance order is only enlivened once the specified individual has been provided with a written

notice that outlines what they must do to ensure compliance with the order and the consequences of failing to comply.

## Recommendation 16

**6.64 The Committee recommends that s34AAD of the *Australian Security Intelligence Organisation Act 1979* be amended to state that the requirement to comply with a compulsory assistance order is only enlivened once the specified individual has been provided with a written notice that outlines what they must do to ensure compliance with the order. This notice should also clarify the consequences of failing to comply.**

6.65 In addition, the Committee also recommends that a further amendment be made to s34AAD to require ASIO to advise the conditions that apply to a compulsory assistance order to the individual that is subject to the order at the time written notice is provided, or at the time the conditions are known. Such an amendment will ensure that the individual subject to a compulsory assistance order will not inadvertently breach the order.

## Recommendation 17

**6.66 The Committee recommends that s34AAD of the *Australian Security Intelligence Organisation Act 1979* be amended to require the Australian Security Intelligence Organisation to advise the individual subject to a compulsory assistance order the conditions associated with that order at the time the written notice is provided or at such time as the conditions are known.**

6.67 The Committee notes the additional recommendations made by the INSLM and the IGIS in relation to oversight and record-keeping, and will address the recommendations in Chapter 7.

# 7. Reporting and Oversight

7.1 This chapter discusses the role of oversight organisations, oversight by the judiciary, as well as the reporting and transparency requirements set out in the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (TOLA Act) and considers recommendations regarding improvements to these arrangements.

## Schedule 1: Industry assistance framework

7.2 As discussed in Chapter 4, Schedule 1 of the TOLA Act introduced an industry assistance framework, comprising technical assistance requests (TARs), technical assistance notices (TANs) and technical capability notices (TCNs). These powers are provided to both law enforcement and intelligence agencies, and are subject to various oversight responsibilities.

### Overview of authorisation and oversight of TARs, TANs and TCNs

#### *Technical assistance requests*

7.3 TARs are voluntary assistance agreements made between heads of the Australian Security Intelligence Organisation (ASIO), the Australian Secret Intelligence Service (ASIS), the Australian Signals Directorate (ASD), Australian Federal Police (AFP), Australian Criminal Intelligence Commission (ACIC), or the Police Force of a State or the Northern Territory (defined as 'interception agencies') with designated communications providers (DCPs).

7.4 As TARs are voluntary assistance agreements made in consultation between one of the above agencies and a DCP, they are not subject to an external authorisation process.

7.5 The head of the Australian Security and Intelligence Agency (ASIO), Australian Secret Intelligence Service (ASIS) and the Australian Signals Directorate (ASD) must inform the Inspector-General of Intelligence and Security (IGIS) within seven day of issuance.[1]

7.6 For other interception agencies such as Federal, State and Territory police, the Commonwealth Ombudsman must be informed seven days after issuance. State and Territory police may also disclose details of a TAR to a State or Territory inspecting body, where the disclosure to the inspecting body is in connection with the performance of its functions.

7.7 In addition, the TOLA Act requires the Home Affairs Minister to prepare an annual report to detail the number of TARs given by interception agencies during the applicable year financial year, which is made available to the public under the *Telecommunications (Interception and Access) Act 1979* annual reporting mechanism.[2]

7.8 ASIO, ASIS and ASD are not required to report publicly on the use of TARs. However, ASIO Act requires ASIO to report on the number of TARs issued in a given financial year in its classified annual report.[3]

### *Technical assistance notices and technical capability notices*

7.9 The Director-General of Security or the chief officer of an interception agency may issue a TAN to a designated communications provider.[4] In the case of a TAN from a State or Territory police force, the AFP Commissioner must provide approval for the head of the State or Territory police force to issue the TAN.[5]

---

1 *Telecommunications and Other Legislation Amendments (Assistance and Access) Act 2018* ('TOLA Act'), s. 317HAB

2 TOLA Act, s. 317Zs. See also Department of Home Affairs, *Telecommunications (Interception and Access) Act 1979* Annual Report 2018-2019.

3 *Australian Security Intelligence Organisation Act 1979* (ASIO Act), s. 94 (2BA).

4 TOLA Act, s. 317L

5 TOLA Act, s. 317LA

7.10 Once a TAN has been issued, the Director-General of ASIO or the chief officer of an interception agency must advise their relevant oversight body within seven days.[6]

7.11 ASD and ASIS are unable to issue TANs or TCNs.

7.12 TCNs are issued by the Attorney-General pursuant to a request from the Director-General Security or the chief officer of an interception agency. The Attorney-General must not give a TCN to a designated communications provider, unless the Attorney-General has given the Minister of Communications written notice of the proposal, and the Minister for Communications has approved the notice.[7] The Department of Home Affairs has described the process as, effectively, a 'triple-lock' mechanism.[8]

7.13 Like TARs above, the number of TANs and TCNs issued must be outlined in the Minister for Home Affairs' annual report each financial year.[9] Additionally, the ASIO Act requires ASIO to report on the number of TANs and TCNs issued in a given financial year in its annual report.[10]

7.14 Neither TANs nor TCNs are subject to judicial authorisation or AAT authorisation prior to issuing.

## Adequacy of authorisation process

7.15 A number of submitters to this inquiry, and the Committee's previous inquiries,[11] raised concerns about the level of authorisation required for the issuance of a TAR, TAN or TCN.[12]

7.16 The Office of the Australian Information Commissioner recommended that the TOLA Act be amended to require independent judicial oversight of the issue of a TAN or TCN:

---

6 TOLA Act, s. 317MAB

7 TOLA Act, s. 317TAAA

8 Department of Home Affairs, *Submission 16*, p. 37.

9 TOLA Act, s. 317ZS

10 ASIO Act, s. 94 (2BA)

11 See Parliamentary Joint Committee on Intelligence and Security, *Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018*, April 2019, p. 55.

12 See Australian Information Industry Association, *Submission 7*, p. 7; Australian Civil Society Coalition, *Submission 13*, p. ; Amazon, *Submission 17*, p. 2; International Civil Liberties and Technology Coalition, *Submission 19*, p. 5; Law Council of Australia, *Submission 24*, p. 14; Internet Australia, *Submission 27*, p. 13; Atlassian, *Submission 31*, p. 3.

> The OAIC notes that many stakeholders have continued to express concern that judicial authorisation is not required before issuing a TAR, TAN or TCN, as set out at Appendix A of the PJCIS report.
>
> Law enforcement initiatives that impact on privacy require a commensurate increase in oversight, accountability and transparency, to strike an appropriate balance between any privacy intrusions and law enforcement and national security objectives. In order to build trust and confidence in the framework, and as previously submitted, we recommend that the Act be amended to introduce independent judicial oversight before a TAN or TCN is issued or varied. An application to a judge to issue or vary a TAN or TCN should be accompanied by a mandatory technical assessment.[13]

7.17 Some submitters noted the requirement for assessors to consider TCNs, and Kaspersky suggested that the assessment requirement is limited in its utility:

> Assessors, in the new subsection 317WA (7), must only 'consider' whether TCNs are reasonable and proportionate as well as whether compliance with the TCN is practicable and technically feasible, but assessors do not have the right either to approve or disapprove TCNs. This questions the real role of assessors and their opinions' value in the consultation process. The TOLA provides ambiguous wording as to whether the assessment carried out under the consultation notice is binding or not – 'if a copy of the assessment report has been given to the Attorney General, the Attorney General must have report considering whether to proceed in giving the notice' (new subsection 317WA (11)).[14]

7.18 In addition, Amazon expressed concern that once a notice is issued, it cannot be reviewed on its merits.[15]

7.19 While the Independent National Security Legislation Monitor (INSLM) did not consider it necessary to amend the authorisation process associated with TARs,[16] the INSLM considered at length the concerns of submitters in relation to TANs and TCNs:

> Almost every non-Government submitter had strong concerns regarding, and objections to, the following aspects of TANs and TCNs:

---

13 Office of the Australian Information Commissioner, *Submission 26*, p. 5.

14 Kaspersky, *Submission 2*, p. 3.

15 Amazon, *Submission 17*, p. 3.

16 Independent National Security Legislation Monitor (INSLM), *Trust but verify: A report concerning the* Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 *and related matters* ('TOLA Act Report'), p. 203.

- the absence of independent authorisation for notices
- the absence of independent technical assessment of proposed notices in relation to such matters as whether they met the statutory definitions of being 'reasonable and proportionate' or 'technically feasible', or would result in a 'systemic weakness or systemic vulnerability'
- whether those definitions, as well as the definition of 'Designated Communications Providers' (DCPs), should be amended.[17]

7.20 The INSLM considered it inappropriate in Australia's federal system that the AFP has a role in the approval of state and territory police issuing industry assistance notices. The INSLM recommended that these powers of the AFP be revoked.[18] The Department of Home Affairs, the AFP and NSW Police supported the INSLM's recommendation.[19] The Law Council of Australia supported the implementation of the INSLM's recommendation, contingent on the implementation of all of the INSLM's recommendations relating to the industry assistance framework, and other matters identified by the Law Council.[20]

7.21 While the definitional matters discussed by the INSLM are covered in Chapter 4, the INSLM's finding on independent authorisation follows.

### *A proposed model for independent authorisation*

7.22 The INSLM consulted with the Investigatory Powers Commissioner's Office (IPCO) in the United Kingdom (UK) in considering the powers under the TOLA Act.[21] A brief history of the introduction of the *Investigatory Powers Act 2016* (UK) and the IPCO is contained in Chapter 3.

7.23 The INSLM recommended that TANs and TCNs should be issued independently of government with those authorising bodies having access to technical advice. Specifically, the INSLM recommended the establishment of an Investigatory Powers Division (IPD) within the Administrative

---

17 INSLM, TOLA Act Report, p. 188.

18 INSLM, TOLA Act Report, p. 206.

19 Department of Home Affairs, *Supplementary Submission 16.2*, pp. 9–10; AFP and NSW Police, *Committee Hansard*, Canberra, 7 August 2021, p. 17.

20 Law Council of Australia, *Supplementary Submission 24.1*, p. 2.

21 INSLM, TOLA Act Report, p. 55.

Appeals Tribunal (AAT) who would be empowered to hear applications for TANs and TCNs, based on the existing security division.[22]

7.24 In addition, the INSLM recommended the establishment of a new statutory office, the Australian Investigatory Powers Commissioner (IPC), who could be appointed as a Deputy President within the AAT, and be assisted by technical advisers.[23]

7.25 The rationale for appending the function onto the existing AAT mechanism recognises that, although it is likely that TANs and TCNs will be issued in the future, the INSLM does not consider it reasonable to establish an entirely new body solely for the purpose of overseeing the TOLA Act.[24] In addition, in making the recommendation, the INSLM notes that it is necessary for DCPs to protect their intellectual property, and for agencies to keep operational objectives secret.[25]

7.26 The INSLM considered whether it was appropriate for decisions to be made *persona designata,* and concluded that decisions should be contestable, and decision-makers should be given the time to build up knowledge and expertise in technology related applications, and therefore decisions should not be made under the *persona designata* function:

> … a key part of the success of the UK IPCO is that the IPC and the judicial commissioners become very familiar with the work and the technology used by the agencies seeking the issue of intrusive warrants and bring that knowledge to bear in considering subsequent applications, ensuring both insight and efficiency. The operation of the *persona designata* function can mean that the eligible judge or tribunal member never exercises the same function twice and cannot build up experience and knowledge.[26]

7.27 The INSLM noted that a number of submissions into the review were concerned with the absence of a requirement to seek an independent technical assessment of TANs to determine if they were reasonable, proportionate and technically feasible or if they would result in a systemic weakness or vulnerability. The INSLM recommended that the legislation be

---

22 INSLM, TOLA Act Report, p. 215.

23 INSLM, TOLA Act Report, p. 215.

24 INSLM, TOLA Act Report, p. 216.

25 INSLM, TOLA Act Report, p. 217.

26 INSLM, TOLA Act Report, p. 219.

amended to require that independent technical advice should be available for both TANs and TCNs.[27]

7.28 In addition, the INSLM suggested that the members of the proposed IPD be assisted by a technical advisory panel drawn from Government, industry and academia covering a range of scientific and technical disciplines[28] and that industry should be consulted in their appointment.[29] The INSLM considered that this would strengthen the existing 'assessor' requirement for TCNs.[30]

7.29 While the INSLM noted that the Attorney-General considers applications for the exercise of ASIO powers, applications made by ASIO could still be approved by the Attorney-General prior to being heard by the proposed IPD within the AAT – a process currently proposed by the Telecommunications Legislation Amendment (International Production Orders) Bill 2020 ('IPO Bill') under consideration by the Committee.[31]

7.30 The Law Council of Australia (hereafter referred to as the 'Law Council') supported a process that would allow applications for TANs and TCNs to be authorised independently of the requesting agency, but noted that authorisation by a court was still preferable to an AAT model, given that a judicial officer exercising a power *persona designata* was constitutionally bound to act in a just and fair manner with judicial detachment.[32]

7.31 Notwithstanding the proposal for a nominated member of the AAT to issue international production orders to ASIO via a double-lock mechanism in the IPO Bill,[33] the Department of Home Affairs said that the AAT may not be the appropriate body to undertake the function:

> As a primary decision-making exercise, the approval of technical assistance notices and technical capability notices would be a significant departure from the merits review function performed by the AAT. A similar function is not conferred on AAT members in their official capacity by any other piece of

---

27 INSLM, TOLA Act Report, p. 212.

28 INSLM, TOLA Act Report, p. 222.

29 INSLM, TOLA Act Report, p. 220.

30 INSLM, TOLA Act Report, p. 222.

31 INSLM, TOLA Act Report, p. 224.

32 Law Council of Australia, *Supplementary Submission 24.1*, p. 8.

33 Telecommunications Legislation Amendment (International Production Orders) Bill 2020, proposed Sch. 1, s. 83.

> legislation. Therefore, the proposed Investigatory Powers Division would operate differently to any other AAT division and may require significant legislative amendments to the *Australian Administrative Appeals Tribunal Act 1975*, including modifying the basic objectives of the AAT and creating an entirely new function for the AAT.[34]

## Adequacy of oversight and reporting mechanisms

7.32 The Commonwealth Ombudsman has oversight of the use of TARs, TANs and TCNs by interception agencies – including state and territory police forces. Interception agencies have an active obligation to provide notification on the issuing, varying, revoking or extending the notice to the Commonwealth Ombudsman. In addition, the Commonwealth Ombudsman may inspect the records of interception agencies to determine the extent of compliance with TOLA Act requirements and provide a report to the Minister for Home Affairs.[35]

7.33 The INSLM's report noted that a number of stakeholders raised concerns with the ability of the Minister for Home Affairs to delete information in a report where it could reasonably be expected to prejudice an investigation or compromise operation activities.[36] The INSLM also noted that the Commonwealth Ombudsman explicitly recommended that section be repealed, and concluded that this should occur.[37]

7.34 Additionally, the Commonwealth Ombudsman may disclose information about a TAN or TCN with a State or Territory integrity body in the performance of its functions.[38] The Law Council suggested that this power be expanded to allow for the Commonwealth Ombudsman to communicate more freely with integrity bodies for the purpose of facilitating a national approach to oversight of the powers:

> Further, the permitted disclosure provisions applying to the Commonwealth Ombudsman only appear to allow the disclosure of information about a TAR or a TAN to the State or Territory oversight body that has responsibility for oversight of the particular State or Territory law enforcement agency that issued the TAR or TAN. This does not provide a clear basis for the

---

34 Department of Home Affairs, *Supplementary Submission 16.2*, p. 6.

35 INSLM, TOLA Act Report, p. 282.

36 *Telecommunications Act 1997*, s. 317ZRB.

37 INSLM, TOLA Act Report, pp. 238–239.

38 TOLA Act, s. 317ZF (5A) – (5C).

> Commonwealth Ombudsman to undertake broader information-sharing with its State and Territory counterparts, about TARs and TANs issued by other State or Territory law enforcement bodies, for the purpose of facilitating national consistency in the approach to the oversight of TARs or TANs that are directed to the same or similar subject-matter.[39]

7.35 Further the INSLM noted the evidence of the Law Enforcement Conduct Commission (LECC) which said that while there were legislative avenues for the LECC to cooperate with the NSW Ombudsman, there was not a provision to allow for broader cooperation in the *Telecommunications Act 1997*. The INSLM considered there was an opportunity to amend s317ZRB of the *Telecommunications Act 1997* to allow for the Commonwealth Ombudsman to undertake joint investigations with a State Ombudsman or Independent Commission Against Corruption oversight bodies like Inspectors-General.

7.36 The Inspector-General of Security (IGIS) has broad oversight of the use of Schedule 1 powers by ASIO, ASIS, and ASD and said that many concerns regarding Schedule 1 powers were addressed by amendments made in December 2018.[40]

7.37 The 2017 Independent Intelligence Review recommended that the ACIC, along with the intelligence functions of the AFP and the ABF – noting that the ABF forms part of the Department of Home Affairs – be subject to oversight by the IGIS and the PJCIS.[41] The Richardson Review recommended that the IGIS have oversight of the ACIC, as well as AUSTRAC, and a Bill to give effect to this recommendation was introduced to on 9 December 2020.[42] The Richardson Review did not consider that the IGIS should have oversight of the intelligence functions of the Department of Home Affairs or the AFP.[43] The reason for this conclusion largely rested on the perceived adequacy of existing oversight functions:

> The IGIS does not have oversight of any department of state. Also, the intelligence function in Home Affairs is not encapsulated in a semi-autonomous agency such as DIO. Rather, it is simply another division in a

---

39 Law Council of Australia, *Supplementary Submission 24.1*, p. 13.

40 Inspector-General of Intelligence and Security (IGIS), *Submission 28*, p. 3.

41 Commonwealth of Australia, *2017 Independent Intelligence Review*, June 2017, p. 116.

42 Intelligence Oversight and Other Legislation Amendment (Integrity Measures) Bill 2020

43 Attorney-General's Department, *Report of the Comprehensive Review of the Legal Framework of the National Intelligence Community*, p. 262.

> wider department. Home Affairs has existing and effective oversight mechanisms for a department of state. We question the value of adding more oversight.
>
> The AFP is a law enforcement agency, not an intelligence agency. To the extent that the AFP engages in intelligence collection activities, it does so in support of its policing functions. Its intelligence function is integrated across the organisation rather than being a stand-alone unit. Extending the IGIS' oversight to the AFP's 'intelligence functions' would be challenging, to say the least, given the dispersed nature of that function across the organisation.[44]

7.38 The Richardson Review also noted that the IGIS and the Commonwealth Ombudsman have tools available to de-conflict, and that they have expressed their commitment to coordination. Further, the Richardson Review notes that the Commonwealth Ombudsman expressed that 'some overlap of oversight bodies responsibilities can be useful to ensure that no gaps arise in coverage.'[45]

7.39 In making the recommendation regarding the establishment of the IPD within the AAT, the INSLM also recommended that the Deputy President of the AAT that heads the IPD should also be a statutory office holder in the role of an IPC, as mentioned above.[46] The INSLM considered that the IPC would be responsible for activities such as:

- monitoring the operation of Schedule 1 of the TOLA Act, including sharing information with relevant oversight bodies;
- participating in the appointment of technical and legal decision-makers who can assist in the IPC's monitoring role;
- developing a prescribed form for TARs, TANs and TCNs and issuing guidelines;
- in consultation with the AAT president, issuing practice notes for the IPD;[47] and
- receive reports from agencies on:
- the number of industry assistance orders taken each year;[48] and

---

44 Attorney-General's Department, *Report of the Comprehensive Review of the Legal Framework of the National Intelligence Community*, p. 262.

45 Attorney-General's Department, *Report of the Comprehensive Review of the Legal Framework of the National Intelligence Community*, p. 261.

46 INSLM, TOLA Act Report, p. 220.

47 INSLM, TOLA Act Report, pp. 220–221.

48 INSLM, TOLA Act Report, p. 245.

- the number of requests made of carriers of carriage service providers under the *Telecommunications Act 1997*.[49]

7.40 As mentioned above, agencies accessing TARs, TANs and TCNs are subject to a variety of oversight and reporting mechanisms. For interception agencies, annual reporting requirements are set out in the *Telecommunications Act 1997*.[50] Additionally, ASIO's annual reporting requirements are set out in the ASIO Act.[51]

7.41 However, several submitters to the inquiry suggested increasing reporting requirements.[52] Internet Australia noted that the written report required to be published each year was not required to include details on the matters TARs, TANs or TCNs were produced for, and were only required to include numbers sought.[53]

7.42 Access Now said that more extensive statistics should be published each year on the use of TARs, TANs and TCNs:

> All uses of TARs, TANs, and TCNs should be tracked and outcomes should be regularly reported. Statistics regarding the judicial approval, denial, or request for modification of TARs, TANs, and TCNs should be published at least semi-annually, along with identification of authorities seeking to invoke the authorities and the specific objectives being pursued that constitute legitimate government aims.[54]

7.43 Internet Australia noted that while DCPs were granted the ability to produce transparency reports, it is a voluntary requirement, and thus cannot be used to 'build a picture of the extent of the use of the powers'.[55]

7.44 In addition, Internet Australia submitted to the INSLM's review that transparency reports were not permitted to include the types of matters that

---

49 INSLM, TOLA Act Report, p. 234.

50 *Telecommunications Act 1997*, s. 317ZS.

51 ASIO Act, s. 94.

52 Mr Peter Jardine, *Submission* 10, p. 6; Australian Civil Society Coalition, *Submission 13*, p. [5]; Koji Payne, *Submission 18*, p. 3; Access Now, *Submission 21*, pp. 4–5; Internet Australia, *Submission 27*, p. [13].

53 Internet Australia, *Submission 27*, p. [13].

54 Access Now, *Submission 21*, pp. 4–5.

55 Internet Australia, *Submission 27*, p. [13].

requests or notices were submitted for, but rather, were only able to include basic statistics.[56]

7.45 The TOLA Act provides discretionary powers to the Attorney-General, the Director-General of Security and the chief officers of interception agencies to grant requests by DCPs to authorise disclosures.[57] The Law Council recommended that this provision be amended to require that a request for disclosure must be authorised unless there are reasons the disclosure should not occur:

> … the Law Council supports the proposed amendment that section 317ZF be amended so that a request for disclosure must be authorised unless it would prejudice an investigation, a prosecution or national security, or unless there are operational reasons for the disclosure not being made.[58]

7.46 Noting the prohibitions on disclosure for activities undertaken under Schedule 1 of the TOLA Act, the Law Council recommended that disclosure of TAR, TAN or TCN information to the Office of the Australian Information Commissioner (OAIC) and the Australian Commission for Law Enforcement Integrity (ACLEI) should form part of the authorised disclosure provisions.[59] Further, the Law Council recommended that a defence to the unauthorised disclosure of information provisions should be included when made in accordance with the *Public Interest Disclosure Act 2013* and the *Freedom of Information Act 1982*:

> It is important the legislation provides explicit confirmation that it is lawful and appropriate for public officials to make disclosures in accordance with the PID Act and FOI Act; and for DCPs and DCPs and public officials to make disclosures to the OAIC and ACLEI; and for the OAIC and ACLEI to make subsequent disclosures for the purpose of performing their functions.
>
> The absence of explicit provisions to this effect may create legal uncertainty or complexity. Irrespective of the ultimate, technical legal construction of how the different sets of provisions interact, the mere existence of uncertainty due to the absence of a clear pathway for disclosure on the face of the Telecommunications Act, could create a disincentive to people coming

---

56 INSLM, TOLA Act Report, p. 283.

57 Law Council of Australia, *Submission 24*, p. 26

58 Law Council of Australia, *Submission 24*, p. 26.

59 Law Council of Australia, *Supplementary Submission 24.1*, p. 16

forward to OAIC or ACLEI, or making public interest disclosures under the PID Act (as applicable).[60]

## Schedule 2: Computer access warrants

7.47 As discussed in Chapter 5, Schedule 2 of the TOLA Act provided ASIO and law enforcement agencies with the ability to apply for computer access warrants. For ASIO, a computer access warrant is issued by the Attorney-General[61] and for law enforcement agencies the warrant is authorised by an eligible judge or a member of the AAT.[62]

7.48 In addition, a computer access warrant allows for activities to be undertaken to conceal the execution of a warrant and to intercept data for the purpose of facilitating the execution of a computer access warrant without seeking additional authorisation. Committee deliberation on the appropriateness of this ability is contained in Chapter 5.

7.49 Where law enforcement agencies are granted a computer access warrant the chief officer of the relevant law enforcement agency must report to the Minister as soon as possible following the cessation of the warrant to state whether the warrant or authorisation was executed, and if so, give details regarding the execution of the warrant.[63] Law enforcement agencies must include details regarding the number of arrests and prosecutions resulting from the use of computer access warrants, and the number of time in which the safe recovery of a child was assisted by information obtained by a computer access warrant.[64]

7.50 The Commonwealth Ombudsman has the ability to inspect records relating to computer access warrants,[65] and cooperate with state inspection bodies in relation to their own investigations.[66] Law enforcement agencies must report to the Commonwealth Ombudsman on activities taken in respect of concealment of access under a computer access warrant.[67] The

---

60 Law Council of Australia, *Supplementary Submission 24.1*, p. 16.

61 ASIO Act, s. 25A

62 *Surveillance Devices Act 2004*, Part 2, Division 4.

63 See *Surveillance Devices Act 2004*, s. 49 (2B)

64 *Surveillance Devices Act 2004*, s. 50.

65 *Surveillance Devices Act 2004*, s. 55.

66 *Surveillance Devices Act 2004*, s. 58.

67 *Surveillance Devices Act 2004*, s. 49B.

Commonwealth Ombudsman said that it has been in discussions with the Department of Home Affairs and the Attorney-General's Department about funding for oversight of powers exercised under the TOLA Act:

> These funding discussions have been premised on my Office monitoring use of the industry assistance powers by the AFP, the Australian Criminal Intelligence Commission, the Australian Commission for Law Enforcement Integrity and each of the state and territory police forces. If the Government were to implement the INSLM's recommendation to extend the industry assistance powers to state and territory anti-corruption bodies (recommendation 1), my Office may need to seek appropriate funding to ensure it has capacity to also monitor those agencies.[68]

7.51 The IGIS retains oversight of ASIO's functions including the processes in place for seeking computer access warrants. The IGIS does not have oversight of the decision-making process of the Attorney-General, however.

7.52 For computer access warrants sought by ASIO, a report must be provided to the Attorney-General on the usefulness of the warrant in assisting ASIO to carry out its functions and details of anything done to:

- conceal access
- intercept communications or
- remove a device

with details of anything that materially interfered with, interrupted or obstructed the lawful use of technology by other persons.[69]

7.53 The IGIS said that including a reporting requirement for all instances of temporary removals of computers and other things would assist in oversight requirements:

> IGIS continues to support the inclusion of a reporting requirement for all instances of temporary removals of computers or other things from warrant premises under computer access warrants. The absence of such a requirement will make oversight complex and inefficient:
>
> - It will be very difficult to determine whether a temporary removal caused material interference with the lawful use of a computer. Arguably, given the centrality of computers in lawful, routine personal and business activities, any temporary deprivation may be likely to cause a material interference with lawful use.

---

68 Office of the Commonwealth Ombudsman, *Supplementary Submission 15.1*, p. 2.

69 ASIO Act, s. 34

- The absence of a specific reporting requirement for all removals may also mean that suitably detailed records may not be made (or may not be made consistently) of the reasons for, and duration of, each removal.[70]

7.54 In addition, any activities undertaken by ASIO to conceal access to a computer post-cessation of the warrant must be reported to the Attorney-General, including what was done, and the usefulness of the actions to the operations of ASIO.[71]

7.55 While ASIO is not required to publish information publicly about its use of the computer access warrant mechanism in Schedule 2, law enforcement agencies are required to report annually on the use of the warrant regime.[72] Neither law enforcement, nor ASIO are required to report on the use of assistance orders provided for by Schedule 2.[73]

## Schedule 3 and Schedule 4: Crimes Act warrants and assistance orders

7.56 As mentioned in Chapter 5, Schedule 3 and Schedule 4 of the TOLA Act amends search warrant provisions under the *Crimes Act 1914* and the *Customs Act 1901*, and introduces assistance orders to the *Customs Act 1901*.

7.57 The AFP or the Australian Border Force (ABF) applies to a magistrate or a 'justice of the peace or other person employed in a court of a State or Territory who is authorised to issue search warrants'.[74] For assistance orders sought under the *Crimes Act 1914* and the *Customs Act 1901* an application may be made to a magistrate. In relation to these powers, the INSLM concluded that there was no requirement to alter how these warrants are issued.[75]

7.58 Statistical reporting on the use of the specific powers granted by Schedule 3 and Schedule 4 is not required as the amendments form part of already

---

70 IGIS, *Submission 28*, p. 11. The Law Council suggested a similar approach, which would require law enforcement agencies to notify the Commonwealth Ombudsman when temporarily removing a device from a premises (*Supplementary Submission 24.1,* p. 24).

71 ASIO Act, s. 34A

72 *Surveillance Devices Act 2004*, s. 50.

73 Department of Home Affairs, *Supplementary Submission 16.1*, p. 5.

74 *Customs Act 1901*, s. 183UA. See also *Crimes Act 1914*, s. 3C which adds 'or warrants for arrest, as the case may be'.

75 INSLM, TOLA Act Report, p. 244.

existing powers. Additionally, the legislation does not require the AFP or the ABF to retain records of the number of assistance orders issued in a given timeframe.[76]

7.59 The INSLM suggested that the AFP and the ABF should keep a record of the number of assistance orders that are executed, but that there is no need for any record or report on the number of assistance orders obtained but not executed.[77] The INSLM also suggested that should the IPC recommendation be implemented, that these reports should be made to the IPC.[78]

7.60 The Law Council largely supported this position, but added that agencies should be required to maintain records to ensure that oversight bodies – like the Commonwealth Ombudsman – could conduct oversight activities as required. The Law Council considered this could include 'oversight of agencies' decision-making about whether to seek an assistance order and the terms of that order, and whether to execute it'.[79]

7.61 Though penalties for failure to comply with an assistance order were increased by the TOLA Act, the INSLM noted there was little statistical evidence to allow for consideration of the appropriateness of the penalty and was ultimately unable to reach a conclusion of the reasonableness and proportionality of the provisions:

> I requested information on the number of criminal prosecutions, and ultimately convictions, for these offences and the sentences imposed in respect of those convictions; and also to seek agencies' views as to what effect (if any) the increase in the penalty for failing to comply with an assistance order has had on those metrics.
>
> The information I received was inconclusive. The absolute number of prosecutions and convictions for breach of these offences is low. For instance, the CDPP response notes 63 charges in respect of the AFP's assistance order provision in the 17-year pre-TOLA period, 37 of which were discontinued, and ultimately 23 convictions. The CDPP reports that 9 of those convicted were sentenced to imprisonment, 4 were sentenced to a recognisance release order, 9 were given a fine and 1 was a juvenile.

---

76 INSLM, TOLA Act Report, p. 245.

77 INSLM, TOLA Act Report, pp. 245–246.

78 INSLM, TOLA Act Report, p. 245.

79 Law Council of Australia, *Supplementary Submission 24.1*, p. 22.

> During that same 17-year pre-TOLA period, in respect of the ABF's assistance order provision, the CDPP report notes there were 8 charges for failure to comply with an ABF assistance order, 6 of which were discontinued, 2 of which proceeded to conviction, and both of which resulted in a fine.[80]

7.62 Further, the INSLM recommended that stakeholders should continue to monitor prosecutions and convictions to permit trends to be established as time passes.[81] The Law Council said that this responsibility should be undertaken by the Commonwealth Director of Public Prosecutions.[82]

## Schedule 5: ASIO voluntary and compulsory assistance powers

7.63 As mentioned in Chapter 6, Schedule 5 introduces voluntary and compulsory assistance provisions into the ASIO Act. The voluntary assistance requests are issued by the Director-General of Security or a senior-position-holder to whom the Director-General has delegated authority to make decisions. A senior position-holder is defined as:

> … an ASIO employee, or an ASIO affiliate, who holds, or is acting in, a position in the Organisation that is:
>
> a. equivalent to or higher than a position occupied by an SES employee; or
>
> b. known as Coordinator.[83]

7.64 Compulsory assistance orders are issued by the Attorney-General after a request from the Director-General of Security.[84] Where a compulsory assistance order is issued, the Director-General of Security is required to report to the Attorney-General on the extent to which both the action taken under the warrant, and compliance with the order, has assisted ASIO in carrying out its functions.[85]

7.65 Additional administratively binding requirements are contained in the *Minister's Guidelines in relation to the performance by Australian Security*

---

80 INSLM, TOLA Act Report, p. 247.

81 INSLM, TOLA Act Report, p. 248

82 Law Council of Australia, *Supplementary Submission 24.1*, p. 21.

83 ASIO Act, s. 16A

84 ASIO Act, s. 34AAA(1)

85 ASIO Act, s. 34 (1) and s. 34 (1A).

*Intelligence Organisation of its functions and exercise of powers.*[86] The Law Council considers that the administrative nature of the guidelines is not sufficient to ensure compliance by ASIO, and recommended that the requirements be contained wholly in primary legislation:

> The ASIO Guidelines do not place a legal limitation on the power of ASIO to confer civil immunities, or the power of the Attorney-General to issue compulsory assistance orders. As such, mere administrative requirements in the ASIO Guidelines, which are vulnerable to unilateral repeal or amendment by the Minister for Home Affairs, are not legal safeguards that limit the availability of these extraordinary powers to confer immunities or compel assistance.
>
> Further, the Law Council is concerned that the prolonged inaction in making critical amendments to the ASIO Guidelines (despite multiple recommendations of the Committee for at least the past six years) means that the public and the Parliament do not have a reasonable basis on which to be assured that the Guidelines would be updated in a timely way. In particular, the Law Council notes that the TOLA measures have been operational since December 2018, yet no amendments to the Guidelines have been made to address matters arising from the TOLA Act.[87]

7.66 The Hon. Margaret Stone, Inspector-General of Intelligence and Security said that although aspects of the ASIO Guidelines were valuable, there were still areas for improvement:

> Can I say that we are very pleased finally to have new guidelines, but, while they are valuable in many ways, we still have issues, for instance in relation to proportionality, which we think could be more clearly spelt out. There is the provision that there will be a review of these guidelines within 18 months—it will commence within 18 months—and regularly every three years after that. That should enable us to both address outstanding concerns and ensure that we don't have such a long period of outdated guidelines, as we had last time. So we're grateful for what we got out of that and, as usual, we're looking for more.[88]

7.67 In addition, amendments to the ASIO Act made by Schedule 5 of the TOLA Act require ASIO's annual report to include a statement of the total number

---

86 The guidelines were updated in August 2020 and can be accessed at https://www.asio.gov.au/ministers-guidelines.html

87 Law Council of Australia, *Supplementary Submission 24.1*, p. 30.

88 The Hon. Margaret Stone AO, Inspector-General of Intelligence and Security, *Committee Hansard*, Canberra, 7 August 2020, p. 10.

of voluntary assistance requests as well as the total number of compulsory assistance orders made during the period.[89]

7.68 The INSLM noted that the requirement to report on compulsory assistance orders was confined to the number of orders, and did not include a requirement to report on the assistance or things implemented as part of the compulsory assistance order. The INSLM therefore recommended that the annual reporting requirement be amended to – similar to the recommendation in Schedule 3 and Schedule 4 powers – provide additional broad information.[90] In addition, the INSLM recommended that the report on the use of these powers should be provided to oversight agencies, and the PJCIS, but may not necessarily be appropriately recorded in a public annual report.[91]

7.69 The Law Council supported additional reporting requirements, but did not agree with the INSLM's suggestion that such reporting may not be made publicly available. The Law Council said the Committee or the INSLM undertake a review on the ongoing appropriateness of the classification of warrant reporting under telecommunications legislation.[92]

7.70 The IGIS has oversight responsibility of the exercise of ASIO's powers, and where ASIO has issued a voluntary assistance order, the IGIS must be informed within seven days.[93] The IGIS did not make any further suggestions related to their ability to oversight voluntary assistance requests made by ASIO.

7.71 The Law Council said it supported the need for the IGIS to be adequately resourced to carry out its oversight functions, and said that it was important to ensure the IGIS could undertake oversight of the propriety of ASIO's decision-making process in conferring immunity under the voluntary assistance provisions:

> A hypothetical example of the type of decision-making that would require close scrutiny for propriety issues could be any decision-making by ASIO to focus its efforts on recruiting (as human sources) people who live, work or socialise with the targets of investigations, in order to use the immunity power in s 21A(1) to task them with obtaining information or documents possessed

89 ASIO Act, s. 94 (2BC).

90 INSLM, TOLA Act Report, p. 232.

91 INSLM, TOLA Act Report, p. 232.

92 Law Council of Australia, *Submission 24.1*, p. 29.

93 ASIO Act, s. 21A (3A).

> by the target, which are located in a shared place of work or residence, to which the human source (but not ASIO) has lawful access. In this type of scenario, propriety concerns could arise if the threshold for ASIO obtaining a warrant (such as a computer access, surveillance or search warrant) to directly collect the relevant material could not be met. This may indicate that the immunity is being used to circumvent those thresholds.[94]

7.72 The IGIS said that five additional staff would be required to 'conduct appropriately thorough and rigorous oversight of the new powers'.[95] The Hon. Margaret Stone AO, Inspector-General of Intelligence and Security, said that if the IGIS' jurisdiction was extended to cover the National Intelligence Community additional funding would be required:

> If our jurisdiction was extended to those four agencies then I think we would need this extra assistance in addition to what we have for those four agencies. We're able to manage at the moment, because there has been no final decision on that jurisdiction… I think one needs to remember that the additional legislation, of which we're all aware, not only expands the scope of what we do, but, in order to oversee activities carried out under that legislation, requires additional depth of investigation. And it will also depend on usage by the agencies. So there are some unknowns and some knowns, but with the increasing technical requirements for oversight we will, for instance, need more technically competent or expert staff. We've got technically competent staff, but we will need more expertise than we presently have.[96]

7.73 As discussed in Chapter 6, the provisions relating to the requirements that can be contained in a compulsory assistance order are not specified. The IGIS suggested that the requirements be set out in the legislation to facilitate a standard of compliance, and establish a benchmark for the IGIS to assess ASIO's compliance.[97]

7.74 In relation to the ability for ASIO to make an oral request to the Attorney-General for a compulsory assistance order,[98] the IGIS suggested that when ASIO makes a subsequent written request, a copy of the oral request should

---

94 Law Council of Australia, *Supplementary Submission 24.1*, p. 28.

95 IGIS, *Submission 28*, p. 4.

96 The Hon. Margaret Stone AO, Inspector-General of Intelligence and Security, *Committee Hansard*, Canberra, 7 August 2020, p. 4.

97 IGIS, *Submission 28*, p. 8.

98 ASIO Act, s. 34AAA (3A)

be provided to the Attorney-General to ensure the written request accords with the initial verbal approval.[99]

7.75 In addition, the IGIS noted that the reporting requirements for compulsory assistance orders are incongruent with the reporting requirements for warrants issued under the *Telecommunications (Interception and Access) Act 1979*[100] which provides a timeframe for report to the Attorney-General. The IGIS suggested that the ASIO Act could be amended to require ASIO to report to the Attorney-General within three months.[101] Additionally, the IGIS noted that the requirement to report does not require the provision of information on how the orders have been executed. The IGIS suggested that such information could include:

- what 'information' and/or 'assistance' was required under the order;
- whether the order has been satisfied;
- when the order was served on the person; and
- whether the information or assistance satisfied the reason for which the order was issued (i.e. whether the assistance provided ASIO the access it required).[102]

# Ongoing oversight and the role of the INSLM

7.76 As discussed in Chapter 2, the TOLA Act came into existence against a backdrop of credible terrorist threats. Though the powers have been in existence for several years, a number of the provisions in Schedule 1 – such as TANs and TCNs – have not yet been used.

7.77 Section 29 of the *Intelligence Services Act 2001* was amended at the time the TOLA Act was introduced to provide for the Committee to undertake a review of the operation of amendments made by the act.

7.78 In addition, s 6 of the *Independent National Security Legislation Monitor Act 2010* was amended to provide for the INSLM to conduct a review on the operation, effectiveness and implications of the amendments made by the Act.

---

99 IGIS, *Submission 28*, p. 8.

100 Section 17.

101 IGIS, *Submission 28*, p. 10.

102 IGIS, *Submission 28*, p. 10.

7.79 Neither amendment requires an additional review or oversight role for the Committee or the INSLM, except as provided as part of the general oversight provisions contained in the relevant acts.

7.80 The INSLM recommended that the enabling legislation be amended to allow for an INSLM to review the act of their own motion as necessary.[103]

# Committee comment

7.81 The Committee considers the appropriate oversight and accountability mechanisms for the powers in the TOLA Act are critical in ensuring the public's ongoing confidence in the use of the powers. Appropriate oversight and reporting mechanisms also provides industry and government agencies with assurance on their use of the powers.

7.82 Part of ensuring adequate oversight means providing certainty in the ability of the IGIS and the Commonwealth Ombudsman to oversee the use of powers. The Committee notes the conclusion reached by the Richardson Review that the oversight responsibilities of the IGIS should not be amended in line with the recommendations of the 2017 Independent Intelligence Review. The Committee is considering IGIS oversight responsibilities further in its current review of the Intelligence Oversight and Other Legislation Amendment (Integrity Measures) Bill 2020.

7.83 The Committee is not persuaded by the conclusion of the Richardson Review that the IGIS should not have oversight of the intelligence functions of the AFP. Given the considerable expertise of the IGIS in overseeing intrusive and covert intelligence functions, and the increasing number of intelligence powers granted to the AFP, the Committee considers that the Government should give further consideration to the implementation of this recommendation.

7.84 As demonstrated by the distinction between AUSTRAC intelligence-related, and non-intelligence-related, functions set out in the Intelligence Oversight and Other Legislation Amendment (Integrity Measures) Bill 2020, the Committee suggests that it would be possible to provide the IGIS with the ability to oversee the intelligence functions of the AFP while still ensuring that the Commonwealth Ombudsman retains the necessary oversight of law enforcement powers. The Committee recommends that the Government amend the *Inspector-General of Intelligence and Security Act 1986* to provide the

103 INSLM, TOLA Act Report, p. 187.

IGIS with oversight responsibilities for the intelligence functions of the Australian Federal Police.

## Recommendation 18

**7.85 The Committee recommends that the Government amend the *Inspector-General of Intelligence and Security Act 1986* to expand the jurisdiction of the IGIS to oversee the intelligence functions of the Australian Federal Police.**

7.86 The Committee notes that the Intelligence Oversight and Other Legislation Amendment (Integrity Measures) Bill 2020 provides the Committee with the ability to oversee the intelligence functions of AUSTRAC. In line with the discussion above, the Committee notes the increasing number of intelligence powers it has had a role in granting to bodies like the ACIC, the Department of Home Affairs and the AFP. The Committee is considering its role in oversight of these agencies in its current review of the Intelligence Oversight and Other Legislation Amendment (Integrity Measures) Bill 2020.

7.87 The Committee considers that the significant and intrusive nature of these powers requires robust oversight with appropriate security considerations provided by the *Intelligence Services Act 2001*. While the Committee holds the oversight of the Parliamentary Joint Committee on Law Enforcement in significant regard, given that the intelligence powers of the ACIC mirror the powers granted to ASIO in many respects, the Committee considers that it should have a role in overseeing the intelligence functions of the ACIC.

## Recommendation 19

**7.88 The Committee recommends that the Government amend the *Intelligence Services Act 2001* to provide the Parliamentary Joint Committee on Intelligence and Security with the ability oversee to the intelligence functions of the Australian Criminal Intelligence Commission.**

7.89 The Committee notes the consideration undertaken by the INSLM in relation to the implementation of a more robust authorisation process for powers exercised under the TOLA Act provisions.

7.90 The Committee considers that there would be benefits to a 'double-lock' model, given the success of the Investigatory Powers Commissioner's Office model in the United Kingdom, and also notes that a similar process has been recommended for the international production orders process which has been considered by the Committee.

7.91 However, the Committee considers that appropriate weight should be given to the evidence of the Department of Home Affairs that the proposal would be a departure from the usual processes of the AAT and that the AAT may not be the appropriate forum to vest a new authorisation process.

7.92 The Committee therefore recommends that the Government consider the INSLM's recommendation, and respond with an appropriate model by no later than September 2022.

## Recommendation 20

**7.93 The Committee recommends the Government give further consideration to the proposal from the INSLM for an Investigatory Powers Division within the Administrative Appeals Tribunal and provide a response on the proposed model or any recommended alternatives by September 2022.**

7.94 The Committee notes that the INSLM also recommended the establishment of a statutory office holder – the Investigatory Powers Commissioner – who would be responsible for the proposed IPD, oversee the use of powers in the TOLA Act, and undertake a number of important additional functions including development of standard form for TARs, TANs and TCNs and take reporting from those using the TOLA Act provisions.

7.95 The Committee acknowledges the reasoning of the INSLM that there would be a benefit in consolidating processes related to the oversight of the use of the regime, especially noting industry concerns outlined in Chapter 4. The Committee agrees, and therefore recommends that the Government give consideration to the appropriate form of an IPC when considering the proposal for an IPD.

## Recommendation 21

**7.96 The Committee recommends the Government consider the proposal for an Investigatory Powers Commissioner, as recommended by the INSLM, and provide a response on the proposed model or any recommended alternative models by September 2022.**

7.97 The Committee notes the conclusion reached by the INSLM that section 317ZRB (7) of the *Telecommunications Act 1997*, which provides the power for the Minister for Home Affairs to delete sections of an annual report where there is the potential to prejudice an investigation or compromise operation activities, be repealed. The Committee recommends that the Government expressly clarify that the Commonwealth Ombudsman must consult with

relevant agencies to identify operationally sensitive material that should be removed or amended before publication of a report. Section 317ZRB(7) of the *Telecommunications Act 1997* should then subsequently be repealed.

## Recommendation 22

**7.98 The Committee recommends that the Government expressly clarify that the Commonwealth Ombudsman must consult with relevant agencies to identify operationally sensitive material that should be removed or amended before publication of a report. Section 317ZRB(7) of the *Telecommunications Act 1997* should then subsequently be repealed.**

7.99 In relation to authorisations, the Committee notes the INSLM's recommendation that the AFP no longer have a role in the consideration of industry assistance notices requested by or issued on behalf of State and Territory police, and the Department of Home Affairs' support for this recommendation. The Committee notes the potential impact on the independence of state and territory police investigations of requiring the AFP to approve TANs. The Committee therefore recommends the *Telecommunications Act 1997* be amended to remove the requirement for State and Territory police to seek the approval of the AFP for TANs.

## Recommendation 23

**7.100 The Committee recommends that s317LA of the *Telecommunications Act 1997* be repealed so that State and Territory police are not required to seek the approval of the Australian Federal Police for a technical assistance notice.**

7.101 In relation to disclosure of information relating to powers exercised under Schedule 1, the Committee notes the concerns raised by industry and civil society and the Law Council's recommendation to amend the provision requiring authorisation for release unless it would prejudice an investigation. Given that the Committee has not yet received evidence on the operation of these procedures, the Committee is not willing to make a recommendation on this issue at this time.

7.102 The Committee notes the concerns of Internet Australia in relation to transparency reports provided by DCPs, but considers that the following recommendations to improve transparency in reporting may provide some assurance regarding these concerns. The Committee supports the continued provision of transparency reports by DCPs on a voluntary basis.

7.103 In relation to the computer access warrant provisions in Schedule 2, the Committee supports the view of the IGIS that the ongoing advancement and societal dependence on technology creates difficulty in determining the threshold of material interference, interruption or obstruction in reporting. The Committee therefore recommends the ASIO Act be amended to require ASIO to report to the Attorney-General on when a device is removed from a premises and the duration of removal when exercising a computer access warrant.

## Recommendation 24

**7.104 The Committee recommends that s 34 of the *Australian Security Intelligence Organisation Act 1979* be amended to require the Australian Security Intelligence Organisation to report to the Attorney-General when a device is removed from premises in the execution of a computer access warrant and the duration of the removal.**

7.105 The Committee notes that unlike law enforcement, ASIO is not required to report in a public forum on its use of powers. The Committee notes the views of the Law Council that the ongoing classified nature of aspects of ASIO's annual report affects the transparency of the use of the regime, however, the Committee considers the classification of some aspects of the ASIO annual report to be proportionate to operational risks.

7.106 The Committee is satisfied with the level of transparency and detail provided in ASIO's annual report and is not recommending any amendment to considerations of national security classification in annual reporting requirements at this time.

7.107 However, the Committee notes that it is provided annually with a copy of ASIO's annual report appendix in relation to telecommunications data access authorisations, which includes national security classified material that may not be included in the publicly available report. The Committee would welcome being provided with a copy of ASIO's annual report appendix in relation to TOLA authorisations also, consistent with current practice for telecommunications data access authorisations. This would assist the PJCIS in its oversight of the functions and powers of ASIO, such as during its annual review of ASIO's Administration and Expenditure. The Committee further recommends that the *Intelligence Services Act 2001* be amended, as required, to provide that the PJCIS may review matters in relation to TOLA authorisations of ASIO.

## Recommendation 25

**7.108 The Committee recommends that:**

- **the Australian Security Intelligence Organisation provide annually to the Parliamentary Joint Committee on Intelligence and Security (PJCIS) a copy of its annual report appendix in relation to Telecommunications and Other Legislation Amendment (TOLA) authorisations, consistent with current practice for telecommunications data access authorisations; and**

- **the *Intelligence Services Act 2001* be amended, as required, to provide that the PJCIS may review matters in relation to TOLA authorisations of the Australian Security Intelligence Organisation.**

7.109 The Committee concurs with the views of the INSLM that reporting of additional details on compulsory assistance orders would provide additional context on the appropriateness of the use of ASIO's powers. The Committee recommends that ASIO brief the PJCIS on the acts or things implemented as part of the compulsory assistance orders regime to facilitate and assist the ongoing oversight of the legislation.

## Recommendation 26

**7.110 The Committee recommends that the Australian Security Intelligence Organisation brief the Parliamentary Joint Committee on Intelligence and Security on the acts or things implemented as part of a compulsory assistance order to facilitate and assist the ongoing review and oversight of the legislation.**

7.111 Similarly, the Committee concurs with the conclusion of the INSLM that agencies empowered to seek an assistance order under Schedule 3 and Schedule 4 should be required to retain records and report to the relevant inspection agency on their use of these necessarily intrusive powers. Further, the Committee agrees with the INSLM that requiring the AFP to report on assistance orders sought and not executed would not provide an appropriate view of the use of the powers.

7.112 Therefore, the Committee recommends that the assistance order provisions in in the *Crimes Act 1914* and the *Customs Act 1901* be amended to require agencies to report to inspection bodies and in their annual reports on the use of these powers.

## Recommendation 27

**7.113 The Committee recommends that s 3LA of the *Crimes Act 1914* and s 201A of the *Customs Act 1901* be amended to require agencies to report to inspection bodies on the execution of assistance orders and publish those figures in their respective annual reports.**

7.114 The Committee notes the concerns raised regarding ASIO's guidelines, and the significant time between the most recent iteration and the version prior. The Committee agrees that it is appropriate for the guidelines to be updated within 18 months in the first instance, and every three years thereafter unless ASIO is granted significant new powers.

7.115 The Committee expects that the next iteration of the ASIO guidelines will address the concerns raised by the IGIS in relation to proportionality, and any other matters identified.

7.116 The Committee notes the Law Council's concerns in relation to the ASIO guidelines, but is not persuaded that amendments in this respect are required at this point. The Committee notes the evidence from the IGIS regarding the enforceability of the conditions of the guidelines and considers that this evidence provides assurances that the IGIS is appropriately considering ASIO's use of powers under the relevant guidelines.

7.117 Noting that some of the most contentious powers granted by the TOLA Act have not yet been used, the Committee agrees with the INSLM's recommendation that it may be appropriate for the INSLM to review the provisions of the TOLA Act at a future time, and therefore recommends that the relevant provisions of the act be updated accordingly so as not to preclude the INSLM from inquiring into the legislation.

## Recommendation 28

**7.118 The Committee recommends the definition in s 4 of the *Independent National Security Legislation Monitor Act 2010* be amended to allow the Independent National Security Legislation Monitor to review the amendments made by the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* of its own motion.**

7.119 The Committee also considers that it would be valuable for the Committee to undertake a review of the TOLA Act in three years when there may be more data available to review the impact and implications of the powers in

the act, but notes that this would only be a particularly relevant exercise once TANs and TCNs have been used.

7.120 The Committee notes that stakeholders have contributed to the Committee's initial consideration of the TOLA Bill and two statutory reviews since the TOLA Act was introduced. The Committee is, therefore, reluctant to impose a continuing administrative burden should TAN and TCN powers not be used in the next three years. Therefore, the Committee recommends that a statutory review only commence once the use of powers have been notified in existing annual reporting obligations.

## Recommendation 29

**7.121 The Committee recommends s 29 of the *Intelligence Services Act 2001* be amended to require the Parliamentary Joint Committee on Intelligence and Security to commence a review within three years once the Committee becomes aware through existing annual reporting requirements that the technical assistance notices or technical capability notices provided by Schedule 1 of the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* have been used.**

**Senator James Paterson**
**Chair**

**15 December 2021**

# A. List of Submissions

**1** Mr David Gates

**2** Kaspersky

**3** *Name Withheld*

**4** Riana Pfefferkorn

**5** Dr Isaac Kfir, Australian Strategic Policy Institute (private capacity)

**6** The Software Alliance

**7** Australian Information Industry Association

**8** Startup Aus

**9** Ms Mary Greene

**10** Mr Peter Jardine

**11** Vault

**12** Electronic Frontiers Australia

**13** Australian Civil Society Coalition

**14** Synod of Victoria and Tasmania Uniting Church in Australia

**15** Commonwealth Ombudsman

- 15.1 Supplementary to submission 15

**16** Department of Home Affairs

- 16.1 Supplementary to submission 16
- 16.2 Supplementary to submission 16
- 16.3 Supplementary to submission 16
- 16.4 Supplementary to submission 16

**17** Amazon

**18** Koji Payne

**19** International Civil Liberties and Technology Coalition

**20** Office of the Victorian Information Commissioner

**21** Access Now

**22** Telstra

**23** Communications Alliance, Ai Group, AIIA, AMTA, DIGI, ITPA

- 23.1 Supplementary to submission 23
- 23.2 Supplementary to submission 23

**24** Law Council of Australia

- 24.1 Supplementary to submission 24

**25** Department of Communications and the Arts

**26** Office of the Australian Information Commissioner

**27** Internet Australia

- 27.1 Supplementary to submission 27

**28** Office of the Inspector-General of Intelligence and Security

**29** Australian Security Intelligence Organisation

- 29.1 Supplementary to submission 29

**30** US Department of Justice

**31** ATLASSIAN

- 31.1 Supplementary to submission 31

**32** Australian Information Industry Association (AIIA) and BSA│The Software Alliance

**33** Australian Federal Police

- 33.1 Supplementary to submission 33
- 33.2 Supplementary to submission 33

**34** NSW Police

**35** Senetas Corporation Limited

# B. Witnesses appearing at public hearings

## Monday, 27 July 2020

Committee Room 2R1, Canberra

*ATLASSIAN*

- Mr Patrick Zhang, Head of IP, Policy and Government Affairs
- Mr Julian Lincoln, Partner, Herbert Smith Freehills
- Ms Anna Jaffe, Senior Associate, Herbert Smith Freehills

*Australian Civil Society Coalition*

- Mr Angus Murray, Chair of Electronic Frontiers Australia's Policy Committee and Vice President of the Queensland Council for Civil Liberties
- Ms Elizabeth O'Shea, Chair

*BSA - The Software Alliance*

- Mr Brian Fletcher, Director Policy - APAC

*Communications Alliance, Ai Group, AIIA, AMTA, DIGI, ITPA*

- Mr John Stanton, CEO, Communications Alliance
- Ms Christiane Gillespie-Jones, Director Program Management, Communications Alliance

*Law Council of Australia*

- Ms Pauline Wright, President
- Dr Natasha Molt, Director of Policy, Policy Division

- Professor Peter Leonard, Member, Media Committee, Business Law Section (Via Teleconference)
- Ms Olga Ganopolsky, Chair, Privacy Law Committee, Business Law Section (Via Teleconference)

## Friday, 7 August 2020

Committee Room 2R1, Canberra

*Office of the Inspector-General of Intelligence and Security*

- The Hon Margaret Stone, Inspector-General of Intelligence and Security
- Mr Jake Blight, Deputy Inspector-General of Intelligence and Security

*Australian Federal Police*

- Commissioner Reece Kershaw
- Deputy Commissioner Investigations Ian McCartney
- Commander Christopher Goldsmid, Cybercrime Operations
- Ms Susan Williamson-DeVries, Manager Government and Executive Advice
- Superintendent Robert Nelson, Digital Surveillance

*NSW Police Force*

- Assistant Commissioner Michael Fitzgerald APM, Commander, Forensic Evidence & Technical Services Command (Via Teleconference)

*Australian Security Intelligence Organisation*

- Mr Mike Burgess, Director-General
- Ms Heather Cook, Deputy Director-General, Intelligence Service Delivery

*Department of Home Affairs*

- Mr Anthony Coles, First Assistant Secretary, Law Enforcement Policy Division
- Mr Andrew Warnes, Assistant Secretary, National Security Policy Branch
- Ms Cath Patterson, Deputy Secretary, Strategy and Law Enforcement

# Additional Comment by Labor Members

Subject to the comments below, Labor members support the Committee's report and recommendations.

First, Labor members believe – as we have long believed – that there must be a robust and independent authorisation process for the powers contained in the Assistance and Access Act. For example, we think that technical assistance notices and technical capability notices should be issued, or at least approved under a UK-style "double-lock" mechanism, by a current or former senior judicial officer.

At paragraph 7.90, Liberal members of the Committee have come close to agreeing with us, writing that "there would be benefits to a 'double-lock' model, given the success of the Investigatory Powers Commissioner's Office model in the United Kingdom, and also notes that a similar process has been recommended for the international production orders process which has been considered by the Committee".

However, Liberal members of the Committee go on to say that "appropriate weight should be given to the evidence of the Department of Home Affairs that the proposal would be a departure from the usual processes of the AAT".

With respect, we do not know what "evidence" Liberal members are referring to. The Department of Home Affairs has offered the Committee no compelling rationale – let alone evidence – for declining to adopt, at the very least, the Independent National Security Legislation Monitor's proposal for a new Investigatory Powers Division within the Administrative Appeals

Tribunal which would be tasked with authorising the use of the powers introduced by the Assistance and Access Act.

Second, Labor members strongly disagree with the rejection by Liberal members of the Independent Monitor's recommendation to extend the industry assistance powers to state and territory anti-corruption bodies. As the Monitor wrote in his report on the Assistance and Access Act:

> The rationale for the extension of these powers to such agencies is clear. They are already empowered under other legislative schemes to exercise various investigative powers, including, for instance, the power to make requests under s 313 of the Telecommunications Act and the power to obtain warrants to lawfully intercept communications under the Telecommunications (Interception and Access) Act 1979 (Cth) (TIA Act). Indeed, the real question appears to be: why should integrity agencies be excluded from the exercise of these powers? There has been no real opposition to them being included.

Labor members note that the original version of the Assistance and Access Bill extended the industry assistance powers to state and territory anti-corruption commissions. And in early 2019, a few months after the passage of the Assistance and Access Bill, the current Government introduced Telecommunications and Other Legislation Amendment (Miscellaneous Amendments) Bill 2019 – the primary purpose of which was to extend the industry assistance powers to state and territory anti-corruption commissions.

In other words, the position of Liberal members is at odds with the position taken by the Morrison Government in late 2018 and early 2019 – but which the Morrison Government appears to have now walked away from.

So, what has changed?

More than 1,000 days after promising to establish a federal anti-corruption commission, the Prime Minister has not even introduced a bill into the Parliament. Instead, the Prime Minister has launched an extraordinary series of improper attacks on the NSW Independent Commission Against Corruption – and on anti-corruption bodies more generally.

Against that background, the fact that the Government has walked away from its position that anti-corruption bodies should have access to the industry assistance powers appears to be politically motivated (noting that it could undermine the Prime Minister's misplaced, misleading and hysterical criticisms of the NSW ICAC if he followed through on his now-forgotten commitment to hand new powers to that very body).

As the Independent Monitor noted in his report, "integrity commissions identified concrete disadvantage that flows from their exclusion from the power to issue industry assistance notices". Liberal members have offered no explanation for their refusal to address that "concrete disadvantage".

**Senator Jenny McAllister**
**Deputy Chair**

**Hon Mark Dreyfus QC MP**

**Mr Peter Khalil MP**

**Senator the Hon Kristina Keneally**

**Dr Anne Aly MP**