



**Australian Government**  
**Department of Home Affairs**

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

Parliamentary Joint Committee on Intelligence and  
Security

**Main Submission**

## Contents

Contents	2
Introduction	4
Context – Overview of Australia’s electronic surveillance framework	4
Overview of the Assistance and Access Act	5
Reviews of the Assistance and Access legislation	6
PJCIS review of the Assistance and Access Bill (December 2018)	6
PJCIS further interim recommendations (February 2019)	6
First PJCIS review of the Assistance and Access Act (April 2019)	7
Implementation of the Act	7
The Australian Federal Police	8
The Australian Criminal Intelligence Commission	9
Use of the powers	9
The Australian Federal Police	9
The Australian Security Intelligence Organisation	10
The Australian Criminal Intelligence Commission	10
PJCIS term of reference 1: threshold, scope and proportionality of powers provided for in the Assistance and Access Act	11
Industry assistance – Schedule 1	11
Scope of ‘designated communications provider’ definition	11
Things that may be requested	13
Exhaustiveness / Non-exhaustiveness of things that may be requested	14
Prohibition on systemic weaknesses and vulnerabilities	15
Prohibition on side-stepping warrants and authorisations (section 317ZH)	20
Prohibitions on metadata, browsing history and interception capability	22
Relevant objectives / purposes	22
Computer access warrants – Schedule 2	23
Telecommunications interception and entering premises	24
Use of force and computer access warrants	25
Search warrants issued under the <i>Crimes Act 1914</i> and the <i>Customs Act 1901</i> – Schedules 3 and 4	25
Alternative methods of access and minimising the impact on the human rights of third parties	25
ASIO device access and immunities – Schedule 5	26
Proportionality of compulsory assistance under section 34AAA	26
PJCIS term of reference 2: Authorisation processes and decision-making criteria	29
Industry assistance – Schedule 1	29
TCN approval process	29
Coordination of TANs by AFP Commissioner	30
Decision-making criteria	32
Consultation and compensation	33

Statutory time limits	35
Centralised and efficient administration	36
Other proposals	36
ASIO device access and immunities – Schedule 5	38
Director-General of ASIO and voluntary assistance under section 21A	38
PJCIS term of reference 3: Enforcement provisions and immunities	39
Industry assistance – Schedule 1	39
Compliance measures	39
Unauthorised disclosure of information rules and offences	40
Civil immunity	40
Search warrants issued under the Crimes Act 1914 and the Customs Act 1901 – Schedules 3 and 4	41
Non-compliance with an assistance order	41
ASIO device access and immunities – Schedule 5	42
Civil liabilities and impact to third parties	42
PJCIS term of reference 4: Interaction with foreign laws	43
Global approaches to the ‘going dark’ problem	43
<b><i>The Statement of Principles on Access to Evidence and Encryption</i></b>	43
Interaction between the CLOUD Act and the Assistance and Access Act	44
PJCIS term of reference 5: Interaction with intelligence agencies’ other powers	45
Voluntary assistance under section 21A	45
Interaction with ASIO warrants and authorisations	45
Compulsory assistance orders under section 34AAA	45
Assistance orders under sections 21A and 34AAA, and Schedule 1 powers	46
PJCIS term of reference 6: Impact on industry and competitiveness	48
Obligations	48
Financial compensation for assistance	48
Cost assessment	49
Arbitration	50
Decision-making criteria and consultation requirements	50
Australian products and services are secure	50
Requests for assistance are served on the corporate entity	51
Communications material	51
PJCIS term of reference 7: Reporting obligations and oversight measures	53
Commonwealth Ombudsman	53
Inspector-General of Intelligence and Security	53
Conclusion	54

## Introduction

1. The Home Affairs Portfolio welcomes the opportunity to make a submission to the Parliamentary Joint Committee on Intelligence and Security's (PJCIS) latest review of the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (the Assistance and Access Act). This submission is made on behalf of the Department of Home Affairs (the Department), and includes material from the Australian Federal Police (AFP), the Australian Security Intelligence Organisation (ASIO), and the Australian Criminal Intelligence Commission (ACIC) (together, the Home Affairs Portfolio). Agencies may make additional individual submissions to the PJCIS separately.
2. This submission seeks to address each of the PJCIS's terms of reference, with a particular focus on the matters for further consideration set out in Appendix A to the PJCIS's review of the Assistance and Access Act released on 2 April 2019 (Act Review Report). This submission also seeks to update the PJCIS on efforts to implement and operationalise the Assistance and Access Act, and discusses how key measures have been used by Australian law enforcement, national security and intelligence agencies (within the limits of the disclosure of information provisions).
3. The Assistance and Access Act has provided subsidiary powers to law enforcement, national security and intelligence agencies to facilitate their lawful investigations into issues such as terrorism, transnational, serious and organised crimes, and other threats to national security. The Assistance and Access Act was passed following a review by the PJCIS, and a three-stage consultation process which provided an opportunity for oversight bodies, the media, industry, academics, advocacy groups and the public to comment on the measures.
4. Since the commencement of the Assistance and Access Act on 9 December 2018, the Home Affairs Portfolio has been working with the communications industry, and with government colleagues from across the Commonwealth and in the jurisdictions, to implement and operationalise the legislation. The Department and the AFP have delivered training to operational agencies, and are leading on the development of administrative guidance material to ensure the powers in the Assistance and Access Act are used consistently. This guidance and training is informing agencies' use of the powers for the investigation of matters related to transnational, serious and organised crime, cybercrime and serious crimes against the person, and national security matters.
5. The Department is also continuing to develop shorter, sharper communications material such as factsheets and answers to frequently asked questions. This material is made available on the Department's website as and when it is developed. This material is designed to provide succinct and accurate information on the legislation for industry, investors and the broader community.

## Context – Overview of Australia's electronic surveillance framework

6. Technology is a part of nearly every aspect of our daily lives, bringing significant benefits to individuals, business and the community more broadly – in Australia and around the world. While modern technology has clear benefits for the Australian community and economy, the use of this technology is a key tool in the arsenal of serious criminals and those that intend to harm Australia's national security. The availability of powers for law enforcement, national security and intelligence agencies to lawfully gain access to communications and devices is critical to the investigation of serious crimes and threats.
7. Efforts to equip agencies with these powers began with the *Telecommunications (Interception and Access) Act 1979* (TIA Act). The TIA Act is the primary legislation governing law enforcement,

national security and intelligence agencies' investigatory powers to intercept communications, and to access communications held by a carrier or carriage service provider (including associated telecommunications data relevant to those communications). The TIA Act has dual objectives:

- to protect the privacy of communications; and
  - to enable interception and access to communications in order to investigate serious crime and threats to national security.
8. The *Surveillance Devices Act 2004* (SD Act) governs the use of surveillance devices by agencies, including state and territory law enforcement agencies when they are using surveillance devices under Commonwealth laws. The SD Act provides for:
    - data surveillance devices—devices or programs used on computers
    - listening devices—devices used to listen to or record conversations
    - optical surveillance devices—devices used to record visuals or observe activities; and
    - tracking devices—devices used to locate or track a person or object.
  9. The SD Act limits the use of information obtained through surveillance devices. Agencies may use this information only for the investigation and prosecution of crimes, national security issues and providing mutual legal assistance to other countries.
  10. The *Telecommunications Act 1997* (Telecommunications Act) contributes to the protection of communications by preventing carriers and carriage service providers from disclosing communications unless specifically provided for under law.
  11. 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.
  12. The Assistance and Access Act is the latest reform in the history of telecommunications law.

## Overview of the Assistance and Access Act

13. 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. Agencies can continue to discharge their lawful investigatory functions with fewer technological impediments, without undermining the cybersecurity of devices and networks or the privacy of Australians.
14. Specifically, the Assistance and Access Act:
  - **established a modern, technologically neutral industry assistance framework (Schedule 1)**. The framework established a structure through which Australian agencies and the modern communications industry can work together to address technological obstacles to investigations into serious crimes and national security threats; and
  - **enhanced investigatory and procedural powers (Schedules 2-5)** to improve agencies' ability to search for, and collect, data. Today, most information is held in digital format and

the Assistance and Access Act modernises the search warrant framework to account for this new reality.

15. The Assistance and Access Act is supported by strong safeguards and oversight measures that protect business interests and the privacy of Australians, maintains the security of the digital ecosystem and ensure the powers are exercised responsibly.

## Reviews of the Assistance and Access legislation

16. The legislation has been scrutinised by the PJCIS through two previous reviews which allowed government agencies, industry, advocacy groups and the public to provide evidence and submissions.

### PJCIS review of the Assistance and Access Bill (December 2018)

17. On 5 December 2018 the PJCIS tabled its report on the then Assistance and Access Bill (Advisory Report) which included seventeen recommendations. Subsequently, the Government moved amendments in the Senate on 6 December 2018 to give effect to these recommendations. The legislation was referred to the PJCIS for further review.

### PJCIS further interim recommendations (February 2019)

18. On 12 February 2019 the Chair of the PJCIS outlined to Parliament two interim recommendations from the PJCIS's second review of the legislation. In response, the Government introduced the Telecommunications and Other Legislation Amendment (Miscellaneous Amendments) Bill 2019 into the Senate on 13 February 2019.
19. The purpose of the Bill was to:
  - allow Commonwealth and State anti-corruption bodies and investigative commissions to have access to the industry assistance framework, and
  - expedite the timeframes for a statutory Independent National Security Legislation Monitor (INSLM) review.
20. The Bill has now lapsed.
21. An expansion to allow Commonwealth and State anti-corruption bodies and investigative commissions to have access to the industry assistance framework is consistent with the Government's original intent in the exposure draft of the Assistance and Access Act. Such an approach balances the legislation by ensuring that Commonwealth, State and Territory law enforcement agencies' use of the new powers can be scrutinised for misconduct and corruption and that the powers themselves are not misused. The industry assistance framework would also assist these bodies to identify and investigate serious misconduct and corruption across the public sector, and maintain confidence in the conduct of public frameworks and officers.
22. To facilitate the use of the industry assistance framework by these anti-corruption bodies and investigative commissions, and consistent with the issuing of a technical assistance notice (TAN) by State and Territory law enforcement agencies, it is important that a central coordinator is established for maintaining consistency, avoiding duplication and enabling the exchange of information across jurisdictions. This central coordinator must be independent and impartial, and should not be within the investigatory remit of these bodies.

23. Non-Government amendments to the Bill were tabled during debate in the Senate. The Department's analysis of these amendments, and other significant proposals, is included below.
24. On 27 March 2019, the PJCIS referred the Assistance and Access Act to the INSLM for review and report. The INSLM will consider the operation, effectiveness and impact of the powers in the Assistance and Access Act, and report to the PJCIS by 1 March 2020.

## First PJCIS review of the Assistance and Access Act (April 2019)

25. On 3 February 2019 the PJCIS released its Review of the Assistance and Access Act which made three recommendations:
  1. *That a legislative amendment be passed to defer the deadline for the PJCIS's current review and report on the Act to June 2020 (from April 2020, to allow the PJCIS to take into account the findings of the INSLM review discussed in the next recommendation).*

The Government is considering the question of a legislative amendment to this effect.
  2. *That sufficient resources be made available to the INSLM to enable the review of the Act, as referred by the PJCIS, and report by 1 March 2020.*

The Department of Home Affairs has temporarily seconded an officer to the INSLM to assist.
  3. *That the Government continue to ensure that the Inspector-General of Intelligence and Security and the Commonwealth Ombudsman have sufficient resources to properly execute their additional responsibilities under the Assistance and Access Act.*

Any requests for additional resourcing for the Inspector-General of Intelligence and Security (IGIS) and the Commonwealth Ombudsman will be considered by the Government through standard process.

## Implementation of the Act

26. The implementation and operationalisation of the Assistance and Access Act has been led by the Department in consultation with Portfolio and other Commonwealth agencies, and the communications and technology industry. A key part of the ongoing implementation efforts has been the development of interim and formal administrative guidance material.
27. On 21 December 2018, the Department distributed interim guidelines to law enforcement, national security and intelligence agencies to support their use of the powers over the critical Christmas and New Year period. This was a short-term solution while more formalised administrative guidance could be developed.
28. The Department has led the development of the *Industry assistance under Part 15 of the Telecommunications Act 1997 (Cth)* (administrative guidance), which outlines procedures and best practice standards under the Assistance and Access Act. The guidance is designed for use by agencies and designated communications providers (providers) from whom agencies seek assistance.
29. The administrative guidance outlines when it is appropriate to use the industry assistance framework, and the rights and obligations for agencies and providers under the Assistance and Access Act. The administrative guidance also outlines how agencies are expected to consult with providers when they wish to seek assistance, and the need to provide procedural fairness and avoid placing providers in a diminished bargaining position. Information is also included on issues such as determining if a decision meets the decision-making criteria and how to conduct a cost assessment of assistance provided.

30. The administrative guidance reflects the Department's ongoing engagement with a consultation group of industry organisations and peak bodies. To inform the development of guidance, in February 2019 this group was asked to respond to an issues paper that identified key areas of contention for the Assistance and Access Act's operation. In March and April 2019, a draft version of the guidance was circulated to agencies and the industry consultation group for scrutiny and comment. The Department updated the draft administrative guidance in light of feedback received. The guidance material is now available on the Department's website:  
<https://www.homeaffairs.gov.au>.
31. The Department has also been working with Commonwealth agencies to develop a communications materials. The purpose of the communications material is to ensure that there is accurate and accessible information to industry and the public and build understanding of the industry assistance framework.
32. The Department has also provided training material to law enforcement agencies for using the industry assistance framework and the other key powers in the legislation. The Department has conducted face-to-face training with the AFP and with jurisdictions that have accepted the Department's invitation for training which includes New South Wales, Victoria and Queensland. The Department has also been assisting law enforcement agencies by offering advice on ad-hoc queries regarding the operation of the Assistance and Access Act.
33. The Department is also working to progress a number of other projects to operationalise the Assistance and Access Act. The Department is currently drafting a standard contract for use by agencies wishing to enter into commercial terms (under section 317K for a voluntary request) with a provider to fulfil more complex types of technical assistance such as developing new capabilities. Work is also continuing to find suitable judicial and technical assessors to review technical capability notices (TCN) upon the request of providers, and to create dispute resolution procedures to govern proceedings in the event of disputes between providers and agencies.
34. Operational agencies have also taken separate action to implement and operationalise the measures in the Assistance and Access Act to be consistent with how the powers will be used for their lawful purposes:

## **The Australian Federal Police**

35. Implementation of the Assistance and Access Act has been a priority for the AFP, with initial implementation focused on providing AFP appointees with both a targeted and general overview of the legislation and key points of contact for further information/advice on use of powers.
36. The AFP has also developed a range of training, procedures, and provided legal support, to ensure delegated officers are well aware of the need for lawful and proportionate application of the provisions.
37. The AFP has set up a hotline and email address to enable state and territory agencies to seek guidance and assistance in application of the powers, as well as to centrally coordinate the processing of Commissioner approval of any TANs. This was promoted during the training sessions provided by Home Affairs to State and Territory agencies. The AFP has similarly collaborated with interception agencies in relation to TARs that provide a benefit across agencies, including in relation to cost sharing models.
38. The AFP would be happy to provide further information on implementation of the Assistance and Access Act should the PJCIS require it.



## The Australian Criminal Intelligence Commission

39. The ACIC is committed to ensuring that powers are used in a measured and considered way. As such, since implementation of the Assistance and Access Act, the ACIC has been dedicated to ensuring as a first priority that appropriate internal legal advice, governance, accountability and training processes are in effect for the new regime.
40. As part of this process, assisted by guidance material provided by Department, the ACIC has developed appropriate templates and processes, training programs and internal procedures to ensure all relevant officers are aware of the scope of lawful use of the legislation, as appropriate opportunities arise.
41. Much of this internal guidance material is classified. The ACIC would welcome the opportunity to expand privately to the PJCIS on the implementation steps taken by the agency if appropriate.

## Use of the powers


42. In late 2018 and early 2019, agencies have used the industry assistance and computer access based powers in the Act to support their lawful investigations and operations into serious crimes and national security matters.
43. Agencies are currently working with providers under the industry assistance framework to seek assistance for the investigation of transnational, serious and organised crime, cybercrime and serious crimes against the person. Agencies are also working with providers on national security matters.
44. Agencies are taking a collaborative approach with industry in utilisation of the industry assistance powers, beginning with technical assistance requests (TAR) to engender support and cooperation.

## The Australian Federal Police

45. The AFP has used the industry assistance framework in support of their lawful activities. To date all requests for assistance have been provided voluntarily pursuant to TARs. The AFP has found its engagement with industry to be positive and cooperative. Cooperation with the PJCIS is critical, and this information is provided to meet the PJCIS's oversight role. However, further information on the use of framework is limited by the authorised disclosure provisions in section 317ZF.
46. The AFP notes that they continue have 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.

## Amendments to search warrants under section 3F

47. In June 2019, the Australian Federal Police executed two search warrants in relation to secrecy offences in Part 6 (Offences by and against public officers) and Part 7 (Official secrets and unlawful soundings) of the Crimes Act.
48. In executing these search warrants, the AFP used section 3F of the Crimes Act, which was amended by Schedule 3 of the Assistance and Access Act.

- 
49. 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.
  50. 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.
  51. These changes to the Crimes Act have allowed pre-existing overt powers to be exercised remotely. This accords with forensic best practice by allowing law enforcement agencies to execute warrants and authorisations without having to be on the target premises or in the presence of the target individual. This means that specialty equipment located offsite can be used in the course of the investigating a premises or person.
  52. The use of the measures provided by Schedule 3 is discussed further in the AFP's submission to the PJCIS.

### ***The Australian Security Intelligence Organisation***

53. ASIO has made use of the powers granted by the Assistance and Access Act and intends to make a classified submission detailing this to the PJCIS.

### ***The Australian Criminal Intelligence Commission***

54. The ACIC is continuing to consider appropriate operational scenarios in which to utilise the Assistance and Access Act. To date the ACIC has utilised Schedule 2 of the Act. The ACIC could provide further advice to the PJCIS in classified hearings as appropriate.

## PJCIS term of reference 1: threshold, scope and proportionality of powers provided for in the Assistance and Access Act

55. The operation of the Assistance and Access Act to date indicates that overall, the current key settings have objectively delivered an appropriate balance between the operational needs of agencies, the protection of civil liberties and the interests of providers.
56. The Department and the broader Portfolio will continue to monitor this closely, including through engagement with the INSLM and PJCIS reviews and ongoing direct engagement with the communications industry.
57. The Department will also continue to work with oversight bodies and relevant on solutions to outstanding issues raised by oversight bodies in previous engagement with the earlier reviews by the PJCIS.

### Industry assistance – Schedule 1

#### Scope of ‘designated communications provider’ definition

58. The use of industry assistance powers contained in Schedule 1 relies upon seeking assistance from a technology provider within a defined category that reflects an aspect of the modern communications environment. These categories are also informed by the growing presence of non--traditional communications providers globally. The Department’s first submission to the PJCIS’s Bill Review<sup>1</sup> provides a detailed justification for the scope of these categories. The following discussion reflects the advice circulated to industry and agencies in relation to the scope of communications providers captured under Schedule 1.
59. The definition of ‘designated communications provider’ sets out 15 categories of entities that may be asked to assist Australian authorities. This reflects the globalised, multi-layered communications industry and the types of entities that could meaningfully assist law enforcement, national security and intelligence agencies. It is crafted in technologically neutral language to allow for new types of entities and technologies to fall within its scope as the communications industry evolves. This ensures that the industry assistance measures will continue to be relevant for law enforcement and national security purposes irrespective of any changes to technology and digital communications.
60. The definition also accounts for the range of providers who are in a position to assist with access to content that may be unintelligible, without undermining the security of a service or device. Further limitations to the scope of providers would undermine the effectiveness of the industry assistance framework. It is critical to the success of the framework that assistance is available from providers across the full communications supply chain. This is particularly the case in circumstances where the Australian Parliament and the Australian Government have decided to prohibit agencies from requiring industry to build capabilities to decrypt communications.
61. In the past, carriers and carriage service providers dominated the communications market and provided comprehensive material in response to lawful requests for communications content and data. The proliferation of digital platforms and online messaging applications (‘over-the-top communications’) in addition to the rise in encryption mean that these carriers can no longer provide reliable access to intelligible content. While requiring encrypted online messaging applications to

---

<sup>1</sup> *Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018*, Submission 18 page 12.

host an 'exceptional access' solution (i.e. provide for ready law enforcement and intelligence agency access to encrypted content) would go some way to resolving this problem by allowing agencies to approach these entities for content, the Department was repeatedly advised of the information security risks inherent in this approach. Accordingly, given the strong support of the Australian Government for cyber security, not solutions were put forward that would undermine encryption. Instead, the Department examined the spread of entities in the communications supply chain who could provide discrete and valuable assistance without falling short of the strict cyber-security protections in the legislation. This reflects the scope of providers within Part 15.

62. It is not uncommon for several entities to be involved in providing an electronic service to a customer. For instance, the transmission of a single communication to an end-user may involve:
- an offshore electronic service provider, like Facebook
  - a Content Delivery Network to facilitate the supply of the communication in the given geographic location
  - the NBN as the dominant fixed line network in Australia
  - an Australian telecommunications carrier, like Telstra
  - a fixed line telecommunications retailer such as TPG contractor of a carrier that maintains a relevant part of the carrier's network
  - a company that develops software that facilitates the transmission of electronic services in the network, or
  - a data centre operator that becomes the physical location of information relevant to the electronic service.
63. Every type of provider listed in items 1–15 of section 317C may be, and often is, an integral part of the communications supply chain and multiple providers can be involved in the transmission of a single electronic service. While an investigation may not require assistance from every single type of provider, depending on the scenario, one or more may be in a position to play a critical role in facilitating lawful access to a communication. In every instance, voluntary or compulsory assistance from a provider is subject to thresholds of reasonableness, proportionality, practicality and technical feasibility.
64. Restricting the definition of 'designated communications provider' to, for example, more traditional or large scale telecommunications companies would ignore the reality of nefarious and security-vitiating activity. The current definition reflects the relatively low barriers to entry into the communications market and accounts for the ability of those seeking to evade authorities to abuse the services of smaller providers.
65. However, it is important to emphasise that individual employees who receive a notice can and should discuss that notice with their employer for the purposes of actioning it. While the notice may be handed or sent to an individual employee (for example an individual nominated by an organisation to receive these notices), it is the corporate entity (not the individual) who is being served with the request or notice.<sup>2</sup> The Act does not have the intention, or effect, of requesting or compelling individual employees within a company to act without the knowledge or sanction of their employers. This has been made explicitly clear in all administrative material and guidance distributed to the independent oversight bodies who receive direct notice of any requests for assistance and scrutinise administrative and legal compliance with regime. Sections 317HAA, 317MAA and 317TAA require that authorities support smaller providers who may be subject to a request or notice to ensure that they understand their obligations.


---

<sup>2</sup> This is further discussed below in relation to the unauthorised disclosure of information provisions.

66. Assistance, and immunities connected to assistance, must be related to the eligible activities of a provider. A provider cannot be asked to assist with things that are not tied to its communications functions. For example, a computer parts manufacturer that provides full disk encryption could not be required to provide access to the contents of a device as it is not relevant to their communications functions. Importantly, each eligible activity must have a nexus to Australia which ensures there is some connection with activities within Australia.
67. Previous industry obligation frameworks have focused on traditional communications providers, such as domestic carriers and carriage service providers. This approach fails to acknowledge the increasing role played by over-the-top providers in providing communication services to Australians through internet-connected devices. This leaves the majority of assistance obligations with companies playing a decreasing part in the communications marketplace. The Assistance and Access Act has levelled the playing field considerably between traditional and more modern communications providers – domestic and international.
68. Criticism of the scope of the ‘designated communications provider’ definition does not properly consider that reducing the definition’s scope would allow illicit activities to be pursued using the products of companies no longer covered by the Act. Reforming the definition to exclude smaller businesses, offshore businesses and hardware manufacturers would drive uptake in these companies’ products by users looking to exploit loopholes in the law. For this reason, while the Assistance and Access Act does not impose standing obligations on any of the providers contained within the definition, it is imperative that the definition retain its current scope so it is possible to seek assistance when necessary.
69. The inclusion of hardware manufacturers provides a clear example of how the definition has been drafted to cover the field where it is unclear at which point in the supply chain industry assistance will be necessary. In certain situations, seeking assistance from a component manufacturer may provide the only pathway for lawful access that avoids jeopardising the integrity of a device’s other security features. An isolated hardware fix on a particular device could provide the assistance required while avoiding the generation of systemic weaknesses, as it would be physically limited to the targeted components in the targeted device. Were hardware manufacturers excluded, illicit activities could be concealed behind hardware-based verification methods without any scope for agencies to compel assistance from certain providers, or offer civil and criminal protections to providers giving assistance voluntarily.

### Things that may be requested

70. Once a provider is chosen, the assistance that may be sought is limited by reference to the listed acts or things set out in section 317E of the Assistance and Access Act. Paragraphs 317E(1)(a)–(j) were developed in close consultation with agencies. To a large extent these paragraphs reflect the nature of assistance traditionally received from domestic carriers and carriage service providers under the pre-existing assistance requirements in section 313 of the Telecommunications Act. That section lacks the specificity of Part 15, simply noting that carriers and carriage services providers must give such help as ‘reasonably necessary’ without stipulating what this help encompasses. As elsewhere, listing the things that may be requested provides a more robust framework industry assistance.
71. The items are broadly cast in order to be responsive to operational needs and to reflect the rapidly changing capabilities of the communications industry. Regulation in such a dynamic and future-orientated industry quickly becomes overly burdensome, obsolete and ineffective if prescriptive requirements are established in the legislation. Instead, the Assistance and Access Act adopts global safeguards that can be appropriately applied to given circumstances to ensure things required of providers are reasonable and proportionate and that the integrity of personal information and security of systems is protected.

- 
72. The Home Affairs Portfolio's submission to the PJCIS Bill Review<sup>3</sup> details the reasons behind the design of this setting.
  73. In response to feedback from industry, subsection 317E(2) was included in the legislation to ensure that if a provider is asked to conceal legitimate surveillance activities of an agency, the provider cannot be asked to make active false or misleading statements or engage in dishonest conduct.
  74. One of the things listed in paragraph 317E(1)(a) is the removal of electronic protection. However, an agency **cannot** seek this kind of assistance under a TCN. Subparagraph 317T(4)(c)(i) provides that an agency cannot seek assistance under a TCN which involves removing a form of electronic protection. This means that the only compulsory power within the legislation which can require the construction of new capabilities **cannot** require a provider build a capability which will allow it to remove encryption (i.e. a decryption capability). This accords with the Assistance and Access Act's general prohibition on the creation or implementation of systemic weaknesses (whether under a TAR, a TAN or a TCN), set out in section 317ZG.
  75. Also of note is paragraph 317E(1)(da) – an explicit pathway for the execution of warrants and authorisations. The Department's first submission to the PJCIS's Act Review<sup>4</sup> sets out the rationale for this amendment. Additional information is set out below.
  76. In response to recommendation 10 of the Advisory Report, the Government amended section 317E to ensure the listed acts or things is exhaustive for compulsory industry assistance measures. To balance this amendment against the legislative intention of keeping the powers current with new technological developments, it was necessary to add a new item to the list of acts or things. Paragraph 317E(1)(da) allows the industry assistance powers to be used in facilitation of an activity conducted under a warrant or authorisation under a law of the Commonwealth, a State or a Territory or the effective receipt of information in connection with a warrant or authorisation.
  77. The introduction of paragraph 317E(1)(da) ensures that interception agencies are able to use the industry assistance measures for one of their chief purposes: to give effect to a warrant or authorisation. This is an appropriate addition as it only authorises activities that are immediately incidental to doing a thing that has been approved pursuant to an underlying authority subject to existing safeguards and thresholds, such as judicial and/or Ministerial approval of warrants. Paragraph 317E(1)(da) also ensures that industry assistance measures can continue to support law enforcement and security agencies to give effect to warrants and authorisations in the context of rapidly evolving technologies.
  78. It is essential to keep legislation fit-for-purpose as an industry evolves; particularly when seeking assistance from an innovative and fluid sector such as the communications industry. Without technology-neutral legislation, it would be necessary to consider wholesale legislative reform again in the near future – causing regulatory uncertainty and inefficiency.
  79. Additionally, this approach finds precedent in subsection 313(7) of the Telecommunications Act which specifies that "giving help" in the context of domestic industry assistance includes giving effect to warrants and authorisations under the TIA Act.

### **Exhaustiveness / Non-exhaustiveness of things that may be requested**

80. The Assistance and Access Act as introduced, applied the listed acts or things to the industry assistance powers at different levels of exhaustiveness. In response to recommendation 10 of the Advisory Report, the legislation was amended to make the listed acts of things exhaustive for all industry assistance powers that impose mandatory requirements on providers.

---

<sup>3</sup> *Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018*, Submission 18 page 14.

<sup>4</sup> *Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018*, Submission 16 page 7.

81. The acts or things that may be sought under a TAR remain non-exhaustive and may include both listed acts or things and things of the same kind, class or nature as those in the listed acts or things. The ability to request broader assistance under a TAR reflects the voluntary nature of TARs. The voluntary nature of a TAR means it is up to the provider to determine whether or not to provide the assistance requested. By law, providers must be notified that compliance with a TAR is voluntary. Providers' discretion to refuse to comply with a TAR places a significant limitation on this power that is not present for the other powers.
82. The utility of TARs would be significantly reduced if the assistance that may be requested was limited to the listed acts or things. This would defeat the policy intention behind TARs and may lead to a greater number of compulsory powers such as TANs being issued. Assistance under TARs is also to be governed by contractual agreements with commercial terms that could be preferable to providers.
83. Non-exhaustiveness of the listed acts or things does not equate to an unlimited ability to request assistance under a TAR. Allowing TARs to remain non-exhaustive merely confers greater flexibility for the phrasing of TARs than the more rigid requirements of TANs and TCNs. TARs must still refer to the list of acts or things when requesting assistance. These activities must still be connected to the eligible activities of providers and are still covered by the limitations that apply to all listed acts or things in subsection 317E(1). TARs cannot be used to request the construction of a decryption capability as this activity is ruled out by the global prohibition in section 317ZG.
84. Similarly, the ability for the Home Affairs Minister to designate additional activities through legislative instruments issued under subsection 317T(5) provides an avenue to keep the Assistance and Access Act current by responding to emerging and unforeseen technological trends. As with the introduction of the warrants pathway in paragraph 317E(1)(da), retaining this provision is necessary to avoid the policy intention of the legislation being frustrated by technological advancement. Failing to enact policies that consider future technologies is a common issue in this area of lawmaking and is a key reason the Assistance and Access Act is needed. Any new activity introduced under a legislative instrument will also be subject to the same limitations as the existing list of acts or things and scrutiny by the Parliament as a disallowable instrument.

## **Prohibition on systemic weaknesses and vulnerabilities**

### **The global protection (section 317ZG)**

85. The Portfolio's first submission to the PJCIS Bill Review<sup>5</sup> sets out a detailed justification for the design of the general prohibition against building or implementing systemic weaknesses or vulnerabilities. The following comments build upon this.
86. A critical protection in the Assistance and Access Act is the prohibition against building or implementing a systemic weakness or systemic vulnerability into a form of electronic protection – expressed in section 317ZG. As subsection 317ZG(3) makes clear, this prohibition captures any effort that would make methods of encryption or authentication less effective. It also prohibits the construction of a decryption capability. Electronic protection is an expansive concept and is defined in section 317B to include encryption or forms of authentication. The Explanatory Memorandum elaborates that it also includes password rate limits on a device.
87. Paragraph 317ZG(1)(b) explicitly prevents an industry assistance power being used to prevent a provider from fixing a systemic weakness or vulnerability they have identified in a form of electronic protection. This means that decision-makers cannot request that providers refrain from taking steps

---

<sup>5</sup> *Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018*, Submission 18 page 19.

to strengthen the security of their systems (for example, by patching a service to fix a flaw) – even if those steps frustrate lawful access to communications.

88. If compliance with an industry assistance power will create a systemic weakness or systemic vulnerability, then the notice or request has no effect to the extent (if any) to which it has that effect. In other words, the provider will not be required to meet those obligations in the request or notice which, if satisfied, will create a systemic weakness or systemic vulnerability in a device or network. However, the provider would still be required to meet any other requirements in the request or notice which do not fall foul of the test in section 317ZG.
89. As discussed in the administrative guidance, the preliminary and mandatory consultation periods provide an opportunity for the provider to formally raise any issues for the decision-maker's consideration, including whether the provider legitimately believes that the obligations in a request or notice will introduce a systemic weakness or vulnerability. Accordingly, and practically speaking, upon the recommendation of the provider the agency may alter the obligations in the request or notice to ensure they do not fundamentally undermine a form of electronic protection, or the overall security of a device or network.
90. In the case of a TCN, during the consultation period, there is a mechanism under section 317WA for an independent panel to conduct an assessment of whether a proposed notice would contravene section 317ZG. If a provider is of the view that a notice or request given to them contravenes section 317ZG (even following an independent assessment through section 317WA), they may decide to not comply with the notice. In this circumstance, the government may seek to enforce compliance with the notice, or accept the decision of the provider to not comply. The provider may also seek a declaration through the court that the notice has been issued in contravention of section 317ZG to confirm that they do not need to comply with it.
91. A provider that believes on an evidential basis that an industry assistance power would contravene section 317ZG has grounds for not complying with the requirements of a notice and could seek judicial review for the administrative decision. The presence of any systemic weakness or vulnerability could then be assessed by a court with the aid of expert testimony or, in the case of a TCN, the independent panel appointed to conduct an assessment.

### [What amounts to a systemic weakness?](#)

92. The sophistication of some forms of electronic protection such as encryption and the breadth of the prohibition, means that there will be instances where industry is not able to assist agencies as the only realistic means of doing so would make the communications of non-target persons vulnerable. To make this clear subsections 317ZG(4A), (4B) and (4C) were introduced following the PJCIS's Advisory Report.
93. Subsections 317ZG(4A) and (4B) reinforce that if a weakness is selectively introduced to a particular device or service, the activity **must not** jeopardise information security of any other person. Subsection 317ZG(4C) clarifies that an activity jeopardises the security of information if it will, or would be likely to, create a material risk that otherwise secure information (i.e. encrypted information) could be accessed by an unauthorised third party, like a cyber-criminal. In effect, the clarification ensures that even an inadvertent impact on broader cyber security that might arise from an agency's targeted activities is also prohibited by the Assistance and Access Act.
94. Criticism of the prohibition has focused on the alleged ability of this provision to permit the creation of exceptional access systems. However, such systems are expressly prohibited by section 317ZG. Persistent capabilities deployed onto networked devices to create new access points for law enforcement are prohibited regardless of any safety assurances provided. This is because the creation of additional access points reduces the security of users' data generally and places the data of users other than the targeted user in jeopardy.



### Application of protection to all listed acts or things

95. The Assistance and Access Act prohibits systemic weaknesses or vulnerabilities being built or implemented under industry assistance through a general prohibition. This applies to all types of assistance that may be sought from the listed acts or things provided by subsection 317E(1). The prohibition against systemic weaknesses applies to all types of assistance that may be sought from the listed acts or things provided by section 317E. However, as the prohibition is framed in terms of not weakening “electronic protection” it may appear that it only applies to the paragraphs within section 317E that relate to the concept of electronic protection – only paragraph 317E(1)(a).
96. However, in order for the protection of section 317ZG to apply, it is not necessary for each listed act or thing to contain a reference to electronic protection. If, in the course of performing activities consistent with a paragraph such as paragraph 317E(1)(c) – installing, maintaining, testing or using software or equipment – a provider was requested or required to build or implement a systemic weakness into a form of electronic protection, the section 317ZG protection would be triggered, invalidating the legal effect of the notice. This is true of every listed act or thing found in subsection 317E(1), regardless of conceptual difficulty determining how the listed act or thing could interact with electronic protection.

### Definitions of systemic weakness and vulnerability

97. Definitions of ‘systemic weakness’ and ‘systemic vulnerability’, introduced in response to recommendation 9 of the Advisory Report, were drafted to create greater certainty regarding the prohibition while preserving the framework’s utility. As discussed in the Department’s first submission to the PJCIS’s Act Review<sup>6</sup>, ‘systemic weakness (or vulnerability)’ now means “a ‘weakness (or vulnerability)’ 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 purpose. For this purpose, it is immaterial whether the person can be identified.”
98. The key part of the definition is the prohibition against any requirements which affect a whole class of technology. 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.
99. 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.
100. This targeted nature is expressed in the second element of the definition which carves out the permissible use of the powers for the sake of clarity. The selective introduction of a vulnerability or weakness – a so-called ‘reserve capability’ – as it relates to a target technology connected with a particular person is allowable.

---

<sup>6</sup> *Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018*, Submission 16 page 10.

101. 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, 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.
102. 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 – as discussed below in relation to the prohibition against side-stepping warrants or authorisations.

### Previously proposed amendments to the definitions and prohibition

103. Amendments moved but not passed in February 2019 included a revised approach to prohibiting systemic weaknesses. The amendment would have repealed the definitions of ‘electronic protection’, ‘systemic weakness’, ‘systemic vulnerability’ and ‘target technology’. While not the original design from the exposure draft of the Assistance and Access Act, these definitions were introduced in response to calls from industry and recommendation 9 of the Advisory Report to clarify the meaning of ‘systemic weakness’.
104. Removing these definitions would have the effect of removing the clarification that a ‘systemic weakness’ is something that affects a ‘whole class of technology’ rather than an isolated ‘target technology’. These clarifications provide the best expression of what is meant by ‘systemic weakness’ and set the threshold of what is required to enliven the prohibition of section 317ZG. A conceptual regime to explain this distinction should be proposed to replace the current definitions if these are repealed.
105. The amendment also proposed to rewrite the prohibition of section 317ZG in the following terms (emphasis added):

**317ZG Designated communications provider must not be requested or required to implement or build a systemic weakness or systemic vulnerability etc.**

(1) A technical assistance request, technical assistance notice or technical capability notice must not have the effect of:

- (a) requesting or requiring a designated communications provider to implement or build a systemic weakness, or a systemic vulnerability; or
- (b) preventing a designated communications provider from rectifying a systemic weakness, or a systemic vulnerability.

(2) The reference in paragraph (1)(a) to implement or build a systemic weakness, or a systemic vulnerability, includes a reference to implement or build a new decryption capability.

(3) The reference in paragraph (1)(a) to implement or build a systemic weakness, or a systemic vulnerability, includes a reference to one or more actions that would render systemic methods of authentication or encryption less effective.

(4) The reference in paragraph (1)(a) to implement or build a systemic weakness, or a systemic vulnerability, includes a reference to any act or thing that would or may create a material risk that otherwise secure information would or may in the future be collected, accessed, used, manipulated, disclosed or otherwise compromised by an unauthorised third party.



(5) The reference in subsection (4) to otherwise secure information includes a reference to the information of, about or relating to any person who is not the subject, or is not communicating directly with the subject, of an investigation to which the relevant technical assistance request, technical assistance notice or technical capability notice relates.

(6) The reference in subsection (4) to an unauthorised third party includes a reference to any person other than:

(a) the person who is the subject of, or who is a person communicating directly with the subject of, an investigation to which the relevant technical assistance request, technical assistance notice or technical capability notice relates; or

(b) the person that issued, or asked the Attorney-General to issue, the relevant technical assistance request, technical assistance notice or technical capability notice.

(7) Subsections (2), (3) and (4) are enacted for the avoidance of doubt.

(8) A technical assistance request, technical assistance notice or technical capability notice has no effect to the extent (if any) to which it would have an effect covered by paragraph (1)(a) or (b).

106. This proposal removes references to 'electronic protection' in current paragraphs 317ZG(1)(a) and 317ZG(1)(b) and subsection 317ZG(2) while retaining the language of 'implementing or building a systemic weakness'. Without reference to 'electronic protection', which includes passwords, encryption methodology and other security layers, it is unclear what the provision is intended to prevent. Prohibiting the creation of systemic weaknesses in the abstract will not have the intended effect of protecting security. Reference to 'electronic protection' or another phrase that refers to the security features of a product or service is required to make clear what the prohibition in section 317ZG is intended to prevent.
107. The proposal would also change the current standard of probability from 'will, or is likely to, jeopardise' to 'would, or may create a material risk that otherwise secure information would or may in the future' for enlivenment of the prohibition. Lowering the standard of likeliness would severely, if not completely, limit the operation of the legislation. Use of the term 'may' potentially prohibits a range of assistance of extremely limited risk because of theoretical concerns. Additionally, 'may in the future' creates an impossible expectation on decision-makers to foresee all possibilities, no matter how hard to anticipate. Indeed, this standard may be higher than what can be expected of providers themselves, who have suffered data breaches as an unforeseen result of coding errors.
108. In addition, the proposal would limit the current concept of 'otherwise secure information' from existing subsection 317ZG(4C) by reference to the information of anyone who is not 'communicating directly with the subject, of an investigation'. This element creates an unnecessarily narrow and conceptually difficult test for what constitutes 'otherwise secure information'. This would exclude the protection's application to users of popular methods of communication – for example, private internet forum users, users of the encrypted messaging application Telegram, and online broadcast platforms such as Twitch – which facilitate communication by indirect (or less direct) methods.
109. Finally, it is unclear how proposed paragraph 317ZG(6)(b) could accommodate sharing developed capabilities between partner agencies for purposes of efficiency. For example, where an agency that did not issue the TAR or TCN utilises capability enabled by that assistance, via an appropriate legal instrument, that agency would be an unauthorised third party, as they had not issued the request or notice used to create the capability. This would occur after the assistance had been provided but, in many cases, would be contemplated at the time that the assistance was sought.

## Prohibition on side-stepping warrants and authorisations (section 317ZH)

110. Industry assistance powers are not vehicles for evidence or intelligence collection in their own right and safeguards in the Assistance and Access Act prevent them from being used in substitution of an established warrant or authorisation. This feature provides independent oversight of the use of industry assistance powers by tying the use of these powers to independent approval to collect underlying personal information. Section 317ZH was broadened to meet recommendation 17 of the Advisory Report and now extends its application to TARs in addition to TANs and TCNs. However, as discussed below, this has led to new legal ambiguity.
111. The Portfolio's first submission to the PJCIS Bill Review sets out in detail the justification for the design of this prohibition which remains largely accurate. The following comments build on this.
112. Section 317ZH states that industry assistance powers have no effect to the extent they ask a provider to do an act or thing which would require a warrant or authorisation under the TIA Act, the SD Act, the *Crimes Act 1914*, the *Australian Security Intelligence Organisation Act 1979* (ASIO Act), or any law of the Commonwealth, a State or Territory.
113. The effect of this section is that industry assistance cannot ask a provider to intercept communications without an interception warrant under the TIA Act being in force. Similarly, an industry assistance power has no effect to the extent it asks a provider to use a surveillance device or access data held in a computer where a State or Territory law requires a warrant or authorisation for that use or access and this additional authority is not present.
114. The limitation reinforces a key purpose of the industry assistance powers. Industry assistance is intended to complement the execution of warrants or authorisations and will be issued to support an underlying instrument that provides the authority to access communications, devices or data. This is why the avoidance of doubt subsections 317ZH(4)–(5) state that the limitation does not prevent an industry assistance power from requiring a provider to assist in, or facilitate, giving effect to a warrant or authorisation under a law of the Commonwealth, a State or Territory. Accordingly, the use of a TAN without an associated warrant will be limited to types of assistance that do not directly facilitate access to communications, such as the provision of technical information.
115. Subsections 317ZH(4)–(5) are **not** exceptions to the prohibition created by subsection 317ZH(1). These avoidance of doubt provisions clarify that the prohibition is **not** intended to prevent warrants or authorisations being used together with industry assistance powers. Rather, section 317ZH is intended to prevent industry assistance powers being used in total substitution for these warrants or authorisations.
116. Subsection 317ZH(2) makes clear that any and all limitations in the Acts listed above apply to the operation of notices both within and outside Australia. This change was made in response to concerns expressed by offshore providers during industry consultation, who noted that they do not currently form part of Australia's domestic warrant framework. Subsequent changes were made to ensure that a notice cannot require a domestic or offshore provider to produce private communications or data.
117. Importantly, industry assistance powers are subject to the inherent territorial limitations of the underlying warrant. Many providers, including offshore providers, cannot be required to execute an interception warrant or disclose telecommunications data under an authorisation. Industry assistance powers do nothing to change this. Rather, they provide the opportunity for agencies to work with these providers to assist in validly executed powers (like a warrant issued to an Australian carrier).

118. This express limitation should be read in connection with the listed acts or things in section 317E. That list deliberately does not include the disclosure of personal information as a form of assistance. This intention is noted in the Explanatory Memorandum:

Technical information does not include telecommunications data such as subscriber details or the source, destination or duration of a communication for which an authorisation under the TIA Act would be required.

And:

Requirements to decrypt or remove electronic protection under this subsection cannot oblige a provider to furnish the content or metadata of private communications to authorities. Consistent with the restrictions in new section 317ZH, agencies must access communications content and data through established warrants and authorisations under the TIA Act...

119. The inability of the industry assistance powers to act as a substitute for existing warrants or authorisations means that the ability of Australian law enforcement, national security and intelligence agencies to receive communications content and data from offshore providers, like Facebook, is limited to either voluntary disclosures or information received through the mutual legal assistance process.
120. Regarding concerns that the provision is unclear to operational agencies, the Department has provided training and guidance material to agencies that details the effect of section 317ZH in plain terms. Reinforcing the purpose of industry assistance powers is to obtain technical assistance when exercising other powers, or as an end in and of itself, has been a major theme of training sessions and materials. The Department has seen no evidence of powers being exercised by agencies seeking to obtain content without the required underlying authority being in place.

### Only extant warrants

121. The Department notes the IGIS's concern that paragraph 317ZH(4)(f) provides a pathway for warrants other than extant warrants to be used to discharge the requirement of subsection 317ZH(1) before obtaining technical assistance in connection with accessing personal information.
122. Section 317ZH permits agencies to obtain assistance with interrogating personal information previously obtained under a now-expired warrant or authorisation. Personal information obtained under previous warrants is strictly controlled by the statutory regime which authorised its collection (the TIA Act or SD Act, for example) – it is permissible and necessary that this information to be used for in the course of an investigation, even after the warrant that collected it has expired. While Part 15 requests or notices can be used to facilitate assistance with interrogating this previously collected information and aid in the execution of a valid and live warrant, these requests or notices can't be used to enliven an expired warrant. Section 317ZH has the effect of preventing a TAR, TAN or TCN being in substitution of a warrant and nothing in this sections permits them to circumvent expiration requirements of an underlying warrant or authorisation.

### Possible clarification

123. The Department notes general concerns previously expressed by stakeholders in submissions to the PJCIS that the purpose of subsection 317ZH(1) may not be immediately apparent when reading the legislation and concerns that the test posed by the provision is practically impossible; requiring consideration of all laws of the Commonwealth, States and Territories.

## Prohibitions on metadata, browsing history and interception capability

124. In addition to the global protections against systemic weaknesses and obtaining personal information without additional authority, the Assistance and Access Act contains a number of explicit prohibitions against certain activities. These are contained in section 317ZGA.
125. Subsection 317ZGA(1) prevents TCNs being used to create new interception capabilities. Subsection 317ZGA(3) prevents TCNs being used to build or extend data retention requirements to new providers. Subsection 317ZGA(4) prevents TCNs being used to create capability to store the browsing history of internet users.

## Relevant objectives / purposes

126. The 'relevant objectives' – simply 'purposes' for TANs – for the use of industry assistance powers have been characterised in other previous submissions to the PJCIS as too broad. However, generally the relevant objectives are specific to the functions of the agency they concern. For example, for the Director-General of the Australian Signals Directorate (ASD) to issue a TAR, the request must relate to ASD's function of "providing material, advice and other assistance to a person or body mentioned in subsection 7(2) of the *Intelligence Services Act 2001* on matters relating to the security and integrity of information that is processed, stored or communicated by electronic means"<sup>7</sup>.
127. For interception agencies and ASIO, the relevant objectives are broader to accommodate the range of activities that would benefit from the technical support enabled by industry assistance powers. However, these relevant objectives are not arbitrarily broad and do not include all of the functions of the associated agencies.
128. Commentary on these relevant objectives suggests that the Assistance and Access Act has imposed novel, broad standards. However, the obligation on carriers and carriage service providers to give help under section 313 of the Telecommunications Act – the provision which industry assistance powers were designed to reflect – provides a broader range of purposes for which help can be provided than is possible in the Assistance and Access Act. Section 313 requires help to be given for purposes including:
  - Enforcing the criminal law and laws imposing pecuniary penalties
  - Assisting the enforcement of the criminal laws
  - Assisting the investigation and prosecution of crimes within the jurisdiction of the International Criminal Court (within the meaning of the *International Criminal Court Act 2002*)
  - Protecting the public revenue, and
  - Safeguarding national security.
129. The PJCIS Act Review also discusses the possibility of replacing the relevant objectives with judicial warrants as a precondition to exercising industry assistance powers.<sup>8</sup> This is discussed below in relation to the second term of reference: authorisation processes.

## Serious offence threshold

130. The reference to 'serious offences' as part of the relevant objectives of 'enforcing the criminal law' for domestic and foreign offences, also creates an offence threshold that limits the offences that

<sup>7</sup> Paragraph 317G(5)(c) Telecommunications Act.

<sup>8</sup> *Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018*, page 36.

may be investigated by interception agencies. 'Serious offences' is defined by section 317B as offences carrying a penalty of at least three years' imprisonment. This was introduced in response to recommendation 2 of the Advisory Report. This offence threshold sufficiently limits the availability of industry assistance powers to the investigation and prosecution of serious crimes such as terrorism, child sex offences and other severe offences such as using a carriage service to menace.

131. Calls for this threshold to be raised to five or seven years' imprisonment would place the Assistance and Access Act out of step with the warrants and authorisations it is designed to work with. Surveillance device warrants and stored communications warrants both have offence thresholds of at least three years' imprisonment. Authorisations for historical telecommunications data are bounded by the same purposes as section 313 of the Telecommunications Act without any associated term of imprisonment or pecuniary threshold. These powers have been set and defined by Parliament and actually authorise intrusion on privacy and the collection of personal data – something which Part 15 does not do. Raising the offence threshold for using industry assistance powers would prevent its use in parallel with these other investigative tools and frustrate the legislation's policy intention.

## Computer access warrants – Schedule 2

132. Schedule 2 of the Assistance and Access Act introduced provisions in the SD Act to allow for Commonwealth, State and Territory law enforcement agencies to obtain computer access warrants when investigating a federal offence punishable by a maximum of three years imprisonment or more. The threshold for obtaining a computer access warrant is proportionate as it is in line with the tests for an application for a surveillance device warrant in the SD Act.
133. The legislation also modernises computer access warrants in the ASIO Act to address operational challenges. 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.
134. As discussed in the Department's submission to the PJCIS's Bill Review<sup>9</sup>, it is almost always necessary for law enforcement and ASIO to undertake limited interception for the purposes of executing a computer access warrant. Schedule 2 amended the law to permit the interception of a communication passing over a telecommunication system, if the interception is for the purposes of doing anything specified in the computer access warrant. In other words, any interception of communications is incidental to fulfilling the computer access warrant, including the concealment of access, and cannot be used for independent evidence or intelligence collection.
135. This means that the threshold for primary interception is not altered or lowered by Schedule 2. Though the same information is collected by ASIO regardless of warrant-type, officers will require an interception warrant to deal with intercepted communications beyond what is required to give effect to a computer access warrant. The existing threshold for interception warrants is generally offences with a maximum seven years' imprisonment or more.
136. It is undesirable for an officer's ability to execute a computer access warrant to be dependent on their ability to obtain a separate telecommunications interception warrant. In some circumstances, law enforcement and ASIO may be able to obtain a computer access warrant, but cannot obtain a telecommunications interception warrant. This reduces the likelihood of a successful execution of the validly issued computer access warrant. In this instance it is appropriate for ASIO's interception

---

<sup>9</sup> *Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018*, Submission 18 page 30.

powers to be limited by express reference to the purposes or things specified in the computer access warrant.

137. This is consistent with the general exceptions to the prohibition against interception in section 7 of the TIA Act. Subsection 7(2) exempts a number of legitimate activities that require the incidental interception of communications, including ‘the interception of a communication where the interception results from, or is incidental to, action taken by an ASIO employee, in the lawful performance of his or her duties’ for the purposes of detecting whether a listening device is being used’.
138. Consistent with the existing provisions in the ASIO Act, ASIO computer access warrants are subject to strict tests and must be signed by the Attorney-General. The Attorney-General may only issue a warrant if they are satisfied that there are reasonable grounds for believing that access to data held in a computer will substantially assist the collection of intelligence in respect of a matter that is important in relation to security.

### **Telecommunications interception and entering premises**

139. Surveillance activities authorised by a computer access warrant may require the manipulation of data. Once undertaken, the manipulated data may allow nefarious actors to recognise the lawful intrusion and change their use of technology to avoid authorities. This would negatively impact ongoing operations and investigations that go to protecting national security and public safety.
140. The concealment of the execution of a computer access warrant is vital to the exercise of the powers under Schedule 2, and indeed, the existing powers under the ASIO Act and SD Act. Concealment of access is essential for preserving the covert nature of computer access warrants, and to protect law enforcement and intelligence technologies and methodologies.
141. Schedule 2 amended the ASIO Act and SD Act to ensure officers are able to enter a premises for the purpose of concealing the fact that anything has been done under a computer access warrant. The law also provides scope for law enforcement and ASIO to intercept communications for the purposes of gaining access to a premises. Any interception must be strictly related to the concealment of the execution of the warrant – in this case entering a premises. Officers may also rely on this power to retrieve a physically implanted computer access device from a computer which was required to give effect to the warrant. This structure acknowledges the importance of ensuring that agencies have the ability to determine when access to premises or to a planted device will best ensure the operation remains covert.
142. Similarly, Schedule 2 introduced provisions into the law to allow law enforcement agencies and ASIO to use interception powers to facilitate entry to a premises, including third-party premises, to remove a computer or device for the purpose of concealing access. The ability to temporarily remove a computer from the 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.
143. In both these circumstances, the interception of communications is only permitted so far as it is required – either to enter a premises for concealment purposes or to temporarily remove a device to give effect to the warrant. It is unlikely that interception powers will be used for such purposes however any limitations on this capability may disproportionately impact law enforcement agencies and ASIO.
144. 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.

### **Use of force and computer access warrants**

145. The Department's supplementary submission to the PJCIS's Act Review discussed how the use of force may be required due to the likely eventualities that officers face while executing a warrant.<sup>10</sup> 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 necessary to use reasonable force if a person is obstructing a doorway into the warrant premises and an officer needs to move past them.
146. 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.
147. However, it is a long standing practice that entry onto premises may be necessary where it would be impractical or inappropriate to intercept communications in respect of a device otherwise than by using equipment installed on specified premises. This may be due to technical reasons connected with the operation of the service or the telecommunications system of which the service is part, or because the execution of the computer access warrant, as a result of action taken by an officer of a carrier, might jeopardise the security of the investigation. Accordingly, it is reasonable and necessary to ensure that law enforcement officers undertaking these activities can do so with appropriate authorisations around the use of force.

### **Search warrants issued under the *Crimes Act 1914* and the *Customs Act 1901* – Schedules 3 and 4**

148. Schedule 3 amended the *Crimes Act 1914* (Crimes Act) to enhance the ability of criminal law enforcement agencies to collect evidence from electronic devices found during a search warrant. Specifically, these amendments modernised the existing search warrant powers and assistance orders to account for modern technology such as smart phones, cloud computing and the complexity of modern communications systems. Schedule 4 replicated these amendments in the *Customs Act 1901* (Customs Act) to ensure similar modern powers are available to the Australian Border Force (ABF).

### **Alternative methods of access and minimising the impact on the human rights of third parties**

149. Schedules 3 and 4 enhance the existing search warrant frameworks in the Crimes Act and Customs Act which permit law enforcement and the ABF to search computers in certain circumstances. Under an overt search warrant, law enforcement and the ABF can remotely access account-based data on a device and access an associated online account which reflects the nature of modern electronic communications systems and is the most efficient and forensically sound method of handling large volumes of data.

---

<sup>10</sup> *Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018*, Submission 16.1 page 7.

150. 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.
151. This matter is discussed in the Department's supplementary submission to the PJCIS Act Review.<sup>11</sup> It would be difficult for an issuing authority to have a sufficient degree of awareness of the investigative reality to properly consider alternative avenues of access when they are authorising the warrant. Therefore, it is more appropriate that the consideration of the degree of reasonableness of access to be undertaken by an executing officer, who would be sufficiently aware of other methods of access that may be available to them. Accordingly, the reasonableness requirement only permits access to third-party computers, or communications in transit, where other methods have already been considered is a sufficient safeguard.
152. The privacy of third parties is also protected by the limitations on the interference with data or communications unless it is necessary to give effect to the warrant. The warrant does not authorise the addition, deletion or alteration of other data, or the doing of anything that is likely to materially interfere with, interrupt or obstruct a communication in transit or the lawful use by other persons of a computer, unless absolutely required. Addition, deletion or alteration must not cause any other material loss or damage to other persons using a computer,
153. Further limitations are unnecessary and operationally unworkable given the transient and mobile nature of cloud communications and devices. If a computer subject to the warrant is obtained, it is feasible that a broad range of persons may have been using that computer to conduct illicit activity. This issue is discussed further in a Departmental response to the Standing Committee on the Scrutiny of Bills.<sup>12</sup>

## ASIO device access and immunities – Schedule 5

154. Schedule 5 introduced new measures into the ASIO Act to allow ASIO to seek voluntary or compulsory assistance to gain access to data. These measures provide necessary protections for persons and bodies assisting ASIO to obtain information and intelligence that may be critical for national security matters. Assistance orders are appropriately limited to ensure they are not used arbitrarily or to undermine human rights.

### *Proportionality of compulsory assistance under section 34AAA*

155. Section 34AAA sets out the criteria under which the Director-General may request the Attorney-General to make an order requiring a person to provide information or assistance that is both reasonable and necessary to allow ASIO to obtain access to data.
156. Broadly speaking there are two chief instances in which the Attorney-General can authorise the issuing of a compulsory assistance order.
157. The first is to facilitate with the fulfilment of certain ASIO warrants. These warrants are issued by the Attorney-General where he is satisfied, on reasonable grounds, that doing that thing or those things under the warrant will substantially assist the collection of intelligence relevant to the prejudicial activities of the identified person. Given this high threshold and that compulsory assistance orders

<sup>11</sup> *Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018*, Submission 16.1.

<sup>12</sup> Standing Committee on the Scrutiny of Bills, Ministerial responses number 14, 28 November 2018, page 34.

are inherently tied to these warrants, the community can have confidence that section 34AAA will be used to support only the most serious matters for ASIO.

158. The second instance is in circumstances where the Attorney-General is satisfied that access by ASIO to data held in, or accessible from, the computer or data storage device will substantially assist the collection of intelligence. In this circumstance, the Attorney-General must also be satisfied of the matters in paragraphs 34AAA(2)(c) and 34AAA(2)(d) of the ASIO Act, which are as follows:

(c) the Attorney General is satisfied, on reasonable grounds, that the specified person is:

- i. reasonably suspected of being involved in activities that are prejudicial to security; or
- ii. the owner or lessee of the computer or device; or
- iii. an employee of the owner or lessee of the computer or device; or
- iv. a person engaged under a contract for services by the owner or lessee of the computer or device; or
- v. a person who uses or has used the computer or device; or
- vi. a person who is or was a system administrator for the system including the computer or device; and

(d) the Attorney-General is satisfied, on reasonable grounds, that the specified person has relevant knowledge of:

- i. the computer, device or a computer network of which the computer, device forms or formed a part; or
- ii. measures applied to protect data held in, or accessible from the computer or device

159. This sets a high threshold for when the Attorney-General can issue an assistance order under section 34AAA. In particular, the threshold of 'prejudicial to security' limits the use of section 34AAA to the most serious matters for ASIO which can reasonably be considered capable of causing damage or harm to Australia, the Australian people, or Australian interests, or to certain foreign countries.

160. Given the seriousness of potential acts that are prejudicial to security, it is critical that ASIO be able to compel assistance from persons suspected of involvement. There are many ways in which involvement may be made out, but these should be viewed through the lens that there are many people with relevant knowledge that can ensure the discovery and safe resolution of activities that represent a material threat to the Australian public.

161. For example assistance can be sought from persons that are unintentionally acting as a conduit for activities that are prejudicial to security, or provide services to another person which enables them to conduct activities that are prejudicial to security. Limiting this provision to those that are knowingly and intentionally involved in activities that are prejudicial to security may inhibit legitimate ASIO investigations and intelligence gathering and establish a critical gap.

162. 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.

163. 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.

164. These additional oversight measures are required to ensure the assistance order achieves the relevant objectives of ASIO while maintaining consideration for the rights of the relevant person.



## PJCIS term of reference 2: Authorisation processes and decision-making criteria

### Industry assistance – Schedule 1

#### TCN approval process

165. An interception agency or ASIO may request that the Attorney-General issue a TCN. Before making such a request, the agency must follow any procedures set out in section 317S by the Attorney-General. This procedure-making provision is intended to streamline the coordination of capabilities across the Commonwealth, State and Territory agencies to ensure that TCNs are vetted by necessary agencies and personnel before being sought from the Attorney-General. At present no such procedures exist. The Department will work with the Attorney-General's Department to draft these procedures should the need arise.
166. Upon receiving a request from an agency the Attorney-General may give a provider a written notice setting out a proposed TCN, at the same time inviting the provider to make a submission on the proposal. Unless waived by the provider or truncated for an emergency, a consultation period of at least 28 days then elapses. During this period the Attorney-General must consider any submissions made by the provider on the proposal.
167. Once the necessary parties have vetted a proposed TCN and modifications have been made to accommodate the feedback of a provider as appropriate, the Attorney-General, with the approval of the Minister for Communications, can give the TCN to a provider. The Attorney-General must be satisfied the requirements are reasonable and proportionate and compliance with the TCN is practicable and technically feasible. Section 317ZAA contains an extensive list of factors which the Attorney-General must take into account when making this decision. In response to recommendation 11 of the Advisory Report, a review mechanism was introduced into in section 317WA to allow a provider to refer a proposed TCN to a legal and technical expert to assess the propriety of a TCN, particularly in relation to systemic weaknesses and vulnerabilities. Assessors are to consider whether:
- the requirements imposed by the notice are reasonable and proportionate,
  - whether the proposed TCN would contravene section 317ZG i.e. introduce a systemic weakness or systemic vulnerability,
  - compliance with the notice is practicable and technically feasible, and
  - the notice is the least intrusive measure that would be effective in achieving the legitimate objective of the notice.
168. Any report produced by the independent panel must be considered by the Attorney-General when issuing a TCN. This requirement for the Attorney-General to consider the outcomes of any report provided by the independent assessors is present in subsection 317WA(11) (for original notices) and subsection 317YA(10) (for variations). Though the decision of the independent panel is not binding on the decision of the Attorney-General, it will be greatly influential on any final outcome. A decision by the Attorney-General that is not consistent with the finding of the panel would be open to close examination in the context of an application for judicial review of the decision. A copy of the report must also be tendered to the provider and the relevant oversight body, ensuring broader awareness of the panel's findings.

169. The proposed TCN must also be approved by the Minister for Communications, who turns their mind to whether the proposal meets the Minister's criteria as legislated in subsection 317TAAA(6). This criteria includes consideration on the impact of the TCN on the competitiveness of industry and the interests of a provider. The requirement for additional Ministerial approval was introduced in response to recommendation 8 of the Advisory Report.

### Issues with the TCN approval process

170. Currently, reviews of proposed TCNs require both experts to consider and offer views over the other expert's area of expertise. This policy was implemented in accordance with recommendation 11 of the Advisory Report which requires both assessors to be satisfied that the legal and technical criteria have been met prior to the issuance of a TCN. This requirement is contained in subsection 317WA(7).
171. The Department queries whether an assessor appointed for their technical expertise is well positioned to consider the reasonableness and proportionality of TCNs. This criteria goes to the broader circumstances of the requirements, like the details and needs of national security and law enforcement operations and broader questions of personal and social impact – not potential technical impact of requirements.
172. While the requirement for both assessors to work in tandem may ameliorate this issue, the Department would like to bring it to the PJCIS's attention.

### Implementation of the TCN approval process

173. The Department has sought expressions of interest and made contact with a selection of persons with suitable qualifications to meet the legal requirements of being a technical or legal expert. The Department will continue to identify potential candidates for these positions so they may be quickly appointed if it becomes necessary to conduct an assessment of a TCN.
174. Together with the Attorney-General's Department, the Department will work to draft guidelines and put in place processes for the efficient administration of the TCN approval process. The Department has also provided comments on the development of draft guidance material for the Minister for Communications' role in approving TCNs.

### Proposals for judicial oversight of TCNs

175. The Home Affairs Portfolio supports the current approval process for TCNs. The Portfolio considers the process as currently enacted balances the interests of agencies with providers and provides a robust mechanism to determine if a TCN would create a systemic weakness. Additionally, considerable efforts have been taken to create and implement procedures for the current process to operate administratively.

### Coordination of TANs by AFP Commissioner

176. In response to recommendation 7 of the Advisory Report, the Government introduced section 317LA which requires TANs issued by State and Territory law enforcement to be subject to the approval of the Commissioner of the AFP. As set out in the Supplementary Explanatory Memorandum, the AFP's role is to focus on the reduction of duplication, enabling the exchange of relevant information across jurisdictions and advice on types and forms of assistance commonly requested, not reassessing State and Territory decision-making on TANs.
177. This amendment is currently in operation and administrative guidance has been developed (and continues to be refined) to centralise and streamline this process. The Department described this

amendment in its January 2019 submission to the PJCIS review. The below commentary builds on this.

178. In addition to recommending that all TANs be reviewed by the AFP Commissioner, the PJCIS recommended the Commissioner be required to “apply the same statutory criteria, and go through the same decision-making process, as would apply if the AFP were the original issuing authority.” The existing section 317LA provides scope for the AFP Commissioner to consider those matters they consider relevant when approving the issuing of a TAN. This includes the same matters that the AFP Commissioner would have regard to if issuing a TAN for the purposes of the AFP.
179. In consultation with the AFP and State and Territory police, the Department has become aware of concerns relating to the sovereignty of co-equal policing agencies and questions relating to the propriety of imposing federal control over an area of law administered by State and Territory authorities. These concerns could become more acute should the AFP Commissioner be *required* to consider the same criteria as the State or Territory decision-maker. This may raise serious concerns for the AFP and State and Territory agencies, including:
- requirements to share sensitive information across jurisdictions outside of joint operations
  - allowing the Commonwealth to ‘second-guess’ operational matters and decisions made by a police force in an independent jurisdiction relating to criminal matters which would overwhelming be tied to investigative imperatives and priorities within that jurisdiction
  - requiring the AFP to have intricate knowledge of State and Territory operations and expertise, and
  - uncertainty about the nature and detail of information about ongoing operations and warrants that would need to be exchanged between jurisdictions to facilitate approval.
180. The introduction of this requirement is likely to reduce the effectiveness of the powers for State and Territory police, reduce the willingness of State and Territory police to use the powers, duplicate existing requirements and create an undue resource and process burden for both the AFP and State and Territory police forces. The amendment may also have the potential impact of causing structural conflict between co-equal policing agencies within the Australian federal framework.
181. Unlike other Commonwealth powers which State and Territory police are able to use, industry assistance powers are not tied to offences in the federal jurisdiction. For example, under the SD Act, State and Territory police can apply for surveillance devices to investigate federal offences punishable by three years imprisonment or more. Other regimes under the Crimes Act allow for the use of powers tied to the investigation of federal offences or State offences with a federal aspect. In contrast, the industry assistance framework is designed to support the use of existing interception powers and other lawful means of accessing content and non-content data, including where the relevant warrant or authorisation has been executed to investigate a purely State-based criminal matter.
182. For example, section 5D of the TIA Act contains a suite of State and Territory offences. State and Territory agencies may independently apply for privacy-intrusive interception and stored communications warrants to investigate these offences. Similarly, the disclosure of telecommunications data made be independently authorised by these same agencies for the enforcement of the criminal law, including State and Territory criminal law.
183. Existing industry assistance provisions in section 313 of the Telecommunications Act (another Commonwealth administered power) do not establish a de-facto Commonwealth-level process of review for State and Territory police seeking technical help from carriers and carriage service providers.

184. Given the concerns expressed by federal, State and Territory police forces about the operation of this amendment, the Committee should consider whether section 317LA should be clarified regarding the coordination role of the AFP Commissioner. The AFP Commissioner could perform a coordination role focused on matters like:

- maintaining preferred points of contact between agencies and providers;
- reducing duplicate requests;
- enabling the exchange of relevant information across jurisdictions;
- advising on the types and forms of assistance commonly requested;
- establishing processes with providers and agencies for the efficient and effective delivery of notices; and
- ensuring consistency in application, payment and cost recovery.

185. State and Territory use of the regime would remain subject to Commonwealth scrutiny through the Commonwealth Ombudsman's oversight function and annual reporting requirements.

### **Decision-making criteria**

186. Decision-makers must not give TARs, TANs or TCNs to providers unless they are satisfied that the request or notice is reasonable and proportionate and that compliance with the request or notice is practicable and technically feasible.

### **Reasonable and proportionate decisions**

187. The legislation contains lists of criteria to determine whether a request or notice is reasonable and proportionate. These criteria apply to the decision to issue all industry assistance powers. The interpretation of these criteria will be assisted by reference to the administrative guidance for use of the powers which provides relevant considerations against each criterion.

188. The administrative guidance does not prescribe a particular weighting to these criteria in order to allow the decision-maker and provider to determine which criteria ought to take precedence in the circumstances. This prevents criteria irrelevant to the peculiar circumstances before a decision-maker being given unnecessary weight and will allow providers to argue for their interests to be prioritised by reference to particular commercial interests as these present themselves.

189. Criteria for determining if a request or notice is reasonable and proportionate provide a thorough and flexible set of considerations for decision-makers to scrutinise. The Department will continue to develop and refine its advice to decision-makers regarding the interpretation of these criteria in response to consultation with industry stakeholders through subsequent versions of the administrative guidance.

### **Practicable and technically feasible compliance**

190. Unlike the weighting exercise that occurs when considering if a request or notice is reasonable and proportionate, practicable and technically feasible compliance is concerned with real-world barriers to execution. It follows that a request or notice that is impracticable or not technically feasible will be impossible to execute.

191. Though these terms are undefined in the Assistance and Access Act, the administrative guidance – which reflects input from industry stakeholders – offers a description of when a request or notice may be impracticable or not technically feasible.



192. Practicability is described as considering the human, financial and organisational resources required to perform an assistance activity and their availability to the provider. An additional test for practicability asks if the assistance sought resembles an activity that is within the provider's typical capacity to perform. If it is, then this may also suggest that compliance is practicable. .
193. An activity is described as being technically feasible by the administrative guidance where it depends upon the operation of a capability that is within the provider's ability to utilise or, where permitted, build. An assistance request or notice will not be technically feasible when it is unclear what technical procedure would need to occur to provide the assistance or if no technical procedure exists that could produce the outcome that is sought. Technical feasibility is also limited by what is permitted within the legislation's prohibition of systemic weaknesses and other limitations.
194. Criticism of the decision-making criteria – particularly of "reasonable and proportionate" – has argued that they are subjective and present an inadequate safeguard against the bias of the decision-making towards law enforcement and security. However, the subjective test of reasonableness and proportionality is balanced by the practicability and technical feasibility criteria that, as described above, relate directly to questions of provider resources and mathematically attainable outcomes.
195. Submissions have also raised that decision-makers may not have the requisite expertise required to evaluate questions that arise in an essentially technical discussion – though agencies may indeed have personnel with technical expertise in the position of decision-maker. However, to the extent this is a concern, this would likely arise in any model of authorisation where the decision-maker is not a highly-specialised expert and is of particular concern in the case of judicial authorisation proposals (discussed below).
196. The Department has sought to bridge any gaps in the technical knowledge of decision-makers by proposing a robust regime of consultation and engagement between provider and agency that may be extended or truncated as required to gather the necessary technical information to make an informed decision. Consultation and engagement are discussed extensively in the administrative guidance developed together with industry stakeholders (and in a section below).
197. Building new capability is the situation most likely to raise concerns of technical feasibility. This is accounted for by allowing a provider to refer a proposed TCN for assessment by an independent expert. New capabilities built voluntarily under a TAR will of course only occur where a provider considers the request technically feasible. TANs do not raise similar concerns, being inherently limited to activities a provider is already capable of performing.

## Consultation and compensation

### Mandatory and recommended consultation

198. Consultation is also a legislative requirement before issuing a TAN. On this question, the administrative guidance recommends that agencies may wish to issue an administrative consultation notice – of the kind required for a TCN consultation – setting the terms of consultation and required assistance where a notice is the first TAN of its kind sent to the provider. This will ensure that assistance relationships primarily governed by TANs begin with detailed consultation and set the conditions for constructive future cooperation.
199. However, conducting this kind of consultation for subsequent TANs issued to obtain the same type of assistance – for example, converting subsequent documents to a readable format – would not necessarily be a productive use of provider or agency time and resources. For this reason, the administrative guidance suggests that later TANs of the same kind may rely on previous consultation conducted with the provider to meet the legislated consultation requirement when

appropriate. This approach will mean that providers have prior opportunity to discuss unique TANs but are not burdened with prescriptive consultation requirements for repeat assistance notices.

200. In the case of TARs, it remains appropriate that there is no legislated consultation requirement of any kind. As with concerns over determining the technical feasibility of TARs, the ultimate discretion of providers to decide to comply with a TAR ensures that sufficient consultation will occur. If a provider considers they have not been properly consulted prior to the issue of a TAR they may choose not to comply with the request. Alternatively, where a provider welcomes the issue of a TAR with minimal or absent consultation, it is appropriate they be able to make this choice.

### Ongoing engagement and revocation

201. The need to keep channels of communication open between provider and agency after assistance has been provided is covered in the administrative guidance with the concept of 'ongoing engagement'. Ongoing engagement begins after the request or notice is issued and continues until it is revoked or expires. This provides a forum for an ongoing conversation between provider and agency to continue to confer regarding the design of the assistance, address outstanding questions, and raise any unforeseen issues.
202. The existing legislation includes a requirement on decision-makers to revoke their request or notice if they are satisfied that the decision-making criteria are no longer met. Ongoing engagement provides an avenue to bring changes in circumstances that may vitiate the original decision to the attention of the decision-maker who may then be obligated to effect the revocation.

### Compensation for compulsory and voluntary assistance

203. The compensation currently available for the use of industry assistance powers has been designed to reflect the nature of the relationship between provider and agency for each type of notice and request.
204. This begins with the most flexible terms, for voluntary assistance provided under a TAR. While this potentially includes assistance of almost negligible financial consequences, the ability to contract for compensation by default allows providers to obtain more generous financial terms than may be expected at default cost recovery level. This accords with the policy intention of encouraging voluntary assistance to the greatest extent possible.
205. The default no-profit/no-loss compensation available for TANs reflects the limited assistance these notices are capable of compelling. It follows that assistance that relies upon existing technical processes should be more easily calculable and involve lower costs (including opportunity costs) than more complex kinds of assistance available under other powers.
206. For example, a TAN may be suitable to compel the conversion of data stored in a provider's proprietary format to a format readable by an agency. This would be a simple matter for the provider, relying upon a prebuilt tool, imposing little opportunity cost and easily billable by reference to administrative burden at a financially neutral rate of compensation.
207. By default, compensation for TCNs is also to be provided on a no-profit/no-loss basis of reasonable compensation. In certain situations it may be more appropriate for compensation to be determined by agreement between the provider and applicable costs negotiator – a person specified by the Attorney-General. For example where a TCN requires substantial capability development, governed by a commercial agreement, commercial terms may be afforded to the provider.
208. The legislation does allow compensation to be foregone in extraordinary circumstances where it would be against the public interest to compensate the provider. However, as both section 317ZK and the administrative guidance make clear, the threshold to satisfy this test is high and will only likely be met in very rare circumstances. For example, it may be appropriate to forgo compensation

where a provider has wilfully created a security risk, specifically designed their services for illicit use, or otherwise behaved negligently or recklessly.

### Standard contracting

209. The Department is working with relevant agencies to prepare standard form contracts to assist with the commercial side of developing assistance capabilities.

### **Statutory time limits**

210. The current approach to statutory maximum time limits on assistance powers has been developed with a view of what is appropriate. Most discussion of this issue focuses on the lack of an upper maximum limit for TARs – though an end date for TARs is required and, where unspecified, expire by default after 90 days.
211. As with prior justifications for the TAR settings, what makes this discretionary approach appropriate is the provider's ultimate ability to control whether or not to provide the requested assistance. Where a provider wishes to provide assistance for the period specified by the TAR, it is appropriate they be allowed to do so. Subject to any commercial or contract consequences, providers are also able to decide unilaterally to cease providing assistance under a TAR at a later time and, from this perspective, the end date specified by the TAR is not critical.
212. The other rights and obligations potentially modified by TARs belong to those individuals and entities whose ability to file a civil suit against a provider for an action is barred by the civil immunity associated with action taken under the TAR. Here it is important to note that TARs only provide an immunity to civil liability for providers for acts done in accordance with, or in good faith purportedly in accordance with, a request. This means that immunities created by TARs are only available while activities consistent with the request remain to be performed and, therefore, effectively cease to be available for further conduct after the activity requested has been completed regardless of whether the TAR remains in effect.
213. Therefore, where a TAR seeks very limited and specific assistance such as increasing a customer's data allowance, the range of activities that attract civil immunity are limited to a very specific action and for a very limited time. That is, after the data limit has been increased, civil immunities are not available for further activities even while the TAR remains in force.
214. Agency discussions with providers indicate that introducing a statutory maximum would make TARs less desirable to providers. This stems from the complexity a statutory limit would introduce into the ability to enter into long term contractual arrangements. A statutory limit would create uncertainty that the rights conferred by the TAR will be available for the length of the agreement because the TAR would need to be reissued once the maximum time is reached.
215. Providers are commercial entities that operate in competitive business environments. In order for a TAR to be appealing to these companies, agencies must be able to offer the certainty that their agency will support the TAR for the lifetime of any underlying commercial agreement. Providers engaging under TARs are already demonstrating a great deal of trust towards agencies. Further asking providers to trust a TAR will be reissued after a period of some years is an unreasonable burden to place on businesses already accepting a level of commercial risk that may be unacceptable in their ordinary dealings.
216. The ability for agencies to offer the required certainty to providers would be significantly diminished by a statutory limit shorter than the desired length of an underlying contractual agreement. This could create reluctance from providers to be engaged under industry assistance leading providers to prefer to be engaged through alternative industry assistance measures such as those offered by section 313 of the Telecommunications Act. These legacy arrangements do not offer the same level

of oversight and protections against the creation of systemic weaknesses as are available in the Assistance and Access Act.

217. Accountability of agencies issuing civil immunities has been an issue raised. The Department has devised administrative procedures to ensure that civil immunities do not linger after assistance activities have been completed. These include the best-practice model of 'ongoing engagement' introduced in the administrative guidance. This model provides for continuing discussion between the issuing agency and provider after the assistance has been provided, creating an avenue for the provider to raise that a TAR no longer meets the decision-making criteria. Where this occurs, the decision-maker will then revoke the TAR as required under section 317JB.
218. As an alternative to legislative changes, the Department would propose introducing administrative procedures for longstanding TARs to be reviewed by issuing agencies after they have been in effect for a set period. These procedures would ask decision-makers to check if the decision-making criteria continue to be satisfied for the TAR and, therefore, if the TAR should remain in effect.

## Centralised and efficient administration

219. The Department is working to develop and consider options to consider the way in which a central coordination office to prevent overlap between different users of industry assistance powers and provide a point of de-confliction could be developed.

## Other proposals

### Judicial approval proposals

220. In relation to the proposal to introduce a form of judicial approval, the Portfolio is of the view that the current approval arrangements strike the correct balance for using industry assistance powers and ensure that decisions are made from a position equipped to understand the security concerns confronted. Decisions under industry assistance encompass primarily technical and intelligence concerns, matters agency heads and the Attorney-General are best placed to adjudicate. As discussed above, industry assistance powers are not vehicles for evidence or intelligence collection in their own right and safeguards in the Assistance and Access Act prevent them from being used in substitution of an established warrant or authorisation. This feature provides independent oversight of the use of industry assistance powers by tying the use of these powers to independent approval to collect underlying personal information. These ongoing requirements for warrants or authorisations continue to protect against unfettered or unwarranted use of intrusive powers.
221. One proposed model of judicial approval would replace the existing 'relevant objectives', discussed earlier, with a regime of prior judicial approval to access the content being sought. However, this proposal relies on the incorrect observation that industry assistance powers are only useful to access the content of communications. This suggests a fundamental misunderstanding of the legislation.
222. Industry assistance provides a pathway to obtain technical assistance from industry to get intelligible versions of information – it is not the main pathway to obtain the content of communications. The legislation's purpose is to provide a pathway for technical assistance – not another avenue to independently obtain content or data.
223. There are circumstances where obtaining technical assistance will not indirectly interact with any warrant regime requirements, to obtain pure technical assistance. Such a warrant would be ill-conceived as technical assistance, involving no disclosure of personal information and creating no invasion of privacy does not require judicial approval.

224. Additionally, requiring a warrant as a precondition to using industry assistance would be complex in circumstances where content may be obtained by an executive authorisation – such as for prescribed ASIO powers.
225. The other model of judicial approval proposed would have judges participate in a ‘double-lock’ mechanism similar to the UK’s *Investigatory Powers Act 2016* (UK IPA) whereby assistance powers would additionally be approved by a judicial commissioner. This commissioner would consider the decision-making criteria.
226. The Department reiterates the analysis set out in previous submissions to the PJCIS<sup>13</sup> that comparisons with the UK IPA and its ‘double-lock’ approval process are superficial. The model for approving TCNs in the Assistance and Access Act which relies upon executive and ministerial decision-making is consistent with Australian practice and jurisprudence. The Assistance and Access Act also includes limitations not present in the UK law and supports surveillance powers in other legislation which contain their own safeguards rather than providing for new surveillance activities.
227. The current model of authorisation for TCNs is appropriate as it reflects the traditional ministerial decision-making practices exercised in Australian executive government. One precedent for this design is the Minister for Home Affairs’ power under the *Security of Critical Infrastructure Act 2018* to direct the owner or operator of a critical infrastructure asset to manage a risk that is prejudicial to security, including by implementing new cybersecurity measures. Another precedent is the Minister for Home Affairs’ power under section 315B of the Telecommunications Act requiring a carrier or carriage service provider to address a risk of unauthorised interference by doing, or refraining from, a specified act or thing. These decisions are similar to the decision the Attorney-General may take in issuing a TCN.
228. The UK IPA is far broader legislation than the Assistance and Access Act, encompassing not only the issue of obtaining technical assistance but the particular surveillance powers the assistance is designed to support as well. The UK IPA’s inclusion of a judicial layer of approval for so many of its powers matches the standard required at Australian law for activities such as telecommunications interception and access to content data, in most instances.
229. The current approval process for issuing a TCN under the Assistance and Access Act is considerable. For example, a TCN aimed at accessing content data in Australia could be said to carry an effective ‘triple-lock’ approval process. Access to content must be approved by obtaining the appropriate judicial warrant under the TIA Act, or other legislation. The TCN must then be issued by the Attorney-General, in contemplation of reasonableness, proportionality, practicability and technical feasibility. Finally, the TCN must be approved by the Minister for Communications, in light of separate decision-making criteria.
230. The assessment of TCNs by the appointment of an independent panel provides a potential fourth layer of review prior to the Attorney-General taking the decision to issue.

### [Requirement to first seek voluntary assistance](#)

231. The Assistance and Access Act is primarily intended to encourage cooperation between industry and Government agencies. As such, the Department advises agencies to seek voluntary pathways for cooperation in the first instance. Cooperation simplifies many of the challenges presented to the legislation’s effective operation and provides for a relationship with providers more conducive to effective assistance.

---

<sup>13</sup> *Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018*, Supplementary submission 18.2 page 5.

232. However, where a provider has previously indicated that they will only comply with compulsory assistance powers, a requirement that voluntary assistance first be sought is unnecessary. For this reason, agencies must be able to determine the appropriate assistance power in consultation with providers unencumbered by such legislative requirements.

## ASIO device access and immunities – Schedule 5

### *Director-General of ASIO and voluntary assistance under section 21A*

233. 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.
234. To provide further confidence, subsection 21A(8) allows the Director-General to give an evidentiary certificate certifying the factual basis necessitating the assistance provided. This certificate will detail the how the relevant conduct was likely to assist ASIO in the performance of its functions.
235. The Director-General also has discretion to provide civil immunities for any assistance given under section 21A. Subsection 21A(1) clearly sets out the thresholds for when civil liability immunity applies to persons or bodies:
- Has the Director-General requested the person or body to engage in certain conduct;
  - Is the Director-General satisfied that, on reasonable grounds, the conduct is likely to assist ASIO in the performance of its functions;
  - Does the conduct involve a person or body committing an offence against a law of the Commonwealth, a State or a Territory; and
  - The conduct would not result in significant loss of, or serious damage, to property.
236. These thresholds ensure that civil immunities will not preclude a person or body from being investigated or prosecuted for committing an offence in Australia, or allow for significant harm to other people.

## PJCIS term of reference 3: Enforcement provisions and immunities

### Industry assistance – Schedule 1

#### *Compliance measures*

237. The penalties associated with the compulsory assistance powers under the Assistance and Access Act have been selected to deter non-compliant behaviour from both large providers and businesses operated by sole traders or partnerships. The Department considers these penalties are proportionate to the harm dealt to the rule of law through non-compliance and the size of the provider in question.
238. The view that the offence in subsection 317ZA(2) of suborning the contravention of a TAN or TCN might criminalise giving security advice to customers does not reflect the intended operation of the legislation. For the purpose of this provision, counselling a contravention of a notice means advocating that a carrier or carriage service provider to fail with the legal obligations contained in the TAN or TCN issued on the corporate entity.
239. Persons engaged in providing security advice to businesses or customers would be acting entirely consistently with the law which, by virtue of paragraph 317ZG(1)(b), actually prevents any a TAR, TAN or TCN from being used to stop a provider from rectifying security flaws in their system. If the advice to the carrier or carriage service provider was that the requirements of a TAR, TAN or TCN would in fact create a security risk and be inconsistent with the protections in Part 15, then that would not be counselling for non-compliance with the law. This is because Part 15 makes clear that requirements to create wider security flaws and faults are incompatible with the legislation. Part 15 encourages the scrutiny and assessment of any potential security flaws through decision-making criteria, consultation requirements and review processes.
240. The intent of subsection 317ZA(2) is to prevent a person from engaging in any conduct if the person has knowledge that the conduct would contravene 317ZA(1). Conduct captured by this offence would include efforts by anyone to prevent the provider giving required technical assistance to law enforcement and intelligence agencies. Because this assistance cannot introduce a systemic weakness or vulnerability, it is unlikely that offering general information to customers to explain how to secure their data would breach this civil penalty provision.

#### The decision to pursue enforcement proceedings

241. A key objective of the Assistance and Access Act is creating a pathway for cooperation between industry and Government agencies. Voluntary assistance, that does not carry the possibility of enforcement action, is the preferred vehicle for industry cooperation. Enforcement proceedings are a course of last resort and will only be taken in situations of blatant and wilful non-compliance with a TAN or TCN.
242. The administrative guidance sets out that where an agency determines a provider is refusing to comply with an obligation to give assistance and wishes to pursue enforcement proceedings, the agency must refer the case to the Communications Access Coordinator (CAC) within the Department for consideration. The CAC would then review the agency's case, including the assistance obligations the provider has allegedly violated, alongside other materials related to the notice. The CAC may also accept representations from the provider regarding the case before reaching a decision to enforcement proceedings.

## Unauthorised disclosure of information rules and offences

243. The legislation's unauthorised disclosure rules and offences are an important bulwark against the disclosure of potentially damaging information for both providers and agencies. Industry assistance may involve the handling of sensitive commercial information that, if disclosed, could put providers at an economic disadvantage. Equally, providers may be exposed to sensitive operational information that, if disclosed, could endanger law enforcement and intelligence methodology and risk revealing details of ongoing investigations.
244. The Assistance and Access Act's strict unauthorised disclosure rules address these concerns by imposing substantial but proportionate criminal penalties for the offence of unauthorised disclosure of technical assistance request information, technical assistance notice information and technical capability notice information.
245. The administration exception to the unauthorised disclosure rules contained in paragraph 317ZF(3)(a) allows for any disclosures necessary to administer or execute an industry assistance power. This includes internal discussions within a provider or between a provider and external contractors. Individuals subject to the unauthorised disclosure rules are nonetheless expected, in these circumstances, to make disclosures to the extent necessary and as required during the course of executing an industry assistance power.
246. However, it is worth noting advice from agencies and industry that the stringency of the unauthorised disclosure rules is unduly impacting on the efficient operation of the industry assistance framework. Changes to subsection 317ZF(3) to clarify the full extent of the administration exception in the text of the legislation may be a workable amendment to address these issues – for example, to ensure that a provider who receives substantially similar requests from two different agencies, can share this information across agencies to the extent appropriate to create efficiencies and promote consistency.

## Civil immunity

247. Granting civil immunity recognises that the provision of assistance has not occurred in the ordinary business of the provider and has not been self-initiated. For this reason, it is appropriate that the provider be indemnified from civil suit arising out of their conduct in accordance with a request or notice. This desire to protect providers is the reason even purported compliance with requests and notices confer civil immunity, thus protecting providers who comply in good faith.
248. The granting of civil immunity to providers is part of the consideration undertaken by a decision-maker when deciding to issue an industry assistance power. Immunity may be particularly relevant to a decision-maker's assessment of whether an industry assistance power's issue is necessary and whether the power's issue is the least intrusive form of industry assistance available so far as persons whose activities are not of interest to the agency are concerned.
249. The scope of the consideration decision-makers must give to the associated civil immunity is proportionate to the scope of the immunity itself. As discussed elsewhere in this submission<sup>14</sup>, civil immunity is limited. Providers are only indemnified for activities done in connection with the provider's eligible activities in the course of giving help to a relevant agency to fulfil their functions. Additionally, the activity undertaken by the provider must be in accordance, or in good faith, purportedly in accordance, with the request or notice.

---

<sup>14</sup> See the discussion of proposed statutory maximums for TARs.



## Search warrants issued under the Crimes Act 1914 and the Customs Act 1901 – Schedules 3

### *Non-compliance with an assistance order*

250. Pre-existing provisions in the Crimes Act and Customs Act enabled law enforcement to compel certain persons (including owners and users of a device) to assist in providing access to data held in a device. Schedule 3 and 4 amended the law to ensure the penalties for non-compliance with an assistance order reflect the potential ramifications for the security of the community.
251. Under the previous regime, offenders frequently refused to comply with an assistance order in instances where the evidence on their device may lead to a more severe penalty than non-compliance with the order. For example, in 2016 an individual was prosecuted on 13 charges relating to the control of multiple child sexual abuse websites he used to distribute and facilitate the production of child pornography material. He received total effective sentence of 15 years and six months' imprisonment with a non-parole period of 10 years. For the offence under section 3LA of the Crimes Act, he was sentenced to six months' imprisonment, which must be considered in the context of the overall sentence.
252. Schedule 3 and 4 introduced a tiered approach to enforcement which ensures that the penalties are reflective of the gravity of non-compliance with an assistance order. The penalty for non-compliance in relation to a simple offence has been increased from two years imprisonment or 120 penalty units, to five years imprisonment or 300 penalty units, or both (see subsection 3LA(5)). Penalties in relation to simple offences in the Customs Act increased from six months imprisonment or 120 penalty units to five years imprisonment or 300 penalty units, or both (subsection 201A(3)).
253. The Assistance and Access Act also introduced a penalty for serious/aggravated offences of 10 years imprisonment or 600 penalty units, or both (see subsection 3LA(5)). It is important to note that the aggravated penalty is only available where the underlying investigation relates to a serious offence (defined as an offence attracting two years or more imprisonment) or serious terrorism offences.
254. This enforcement structure is proportionate and ensures that the penalties for non-compliance are reflective of the potential harm it may cause to innocent Australians.
255. The law also includes explicit protections for those persons that are required to provide assistance but are incapable of doing so. A person would be incapable of complying with an assistance order if, for example, the person is no longer able to provide the evidential material by virtue of not having access to the relevant device.

### Assistance orders and the privilege against self-incrimination

256. In a submission to the Bill review<sup>15</sup>, the Department addressed concerns regarding the view that assistance orders breach the privilege against self-incrimination. The amendments made by the Assistance and Access Act to raise the penalty for non-compliance with an assistance order rely on the existing rationale for the offence as it was legislated: that a compulsion to provide access to a device does not enliven the privilege against self-incrimination.
257. Assistance orders do not engage this privilege on the basis that an assistance order does not prevent a person from remaining silent, or compel a person to confess guilt, but allows a device to be searched. This is not dissimilar from a search warrant on a premises where access to the premises cannot be denied or frustrated on the basis of self-incrimination. Assistance orders do not

---

<sup>15</sup> Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018, Submission 18 page 34.

compel an individual to go into their device and disclose information or documents. It simply provides an avenue for law enforcement, national security and intelligence agencies to lawfully gain access to that device, so that a lawful search of the device may be conducted as necessary. Further, assistance orders must be judicially authorised.

258. Unauthorised disclosure of information about, or obtained under, a computer access warrant is an offence. The maximum penalty for the offence is two years imprisonment or 10 years if the disclosure endangers the health or safety of any person or prejudices an investigation into an offence.
259. The use, recording and communication of information obtained in the course of intercepting a communication in order to execute a computer access warrant is restricted. Where agencies want to gain intercept material for its own purposes, they must be issued with an interception warrant under Chapter 2 of the TIA Act.

## ASIO device access and immunities – Schedule 5

### *Civil liabilities and impact to third parties*

260. The limitations for when civil immunities can be provided for assistance under section 21A mitigates the risk of significant economic impact or harm being inflicted on third parties.
261. Section 21A cannot be used to compel a person or body to commit an offence against the laws of the Commonwealth, a State or a Territory. The assistance orders are further limited by the fact that any conduct cannot result in significant loss of, or serious damage to, property. As discussed in submissions to previous PJCIS reviews, the Department considers that these limitations are sufficiently broad to capture instances of meaningful harm, or significant loss or damage the property of other persons. As a result, civil immunities will not be provided for any assistance that falls foul of this test.
262. The assistance regime under section 21A is also voluntary in nature which means persons will not be subject to any civil penalties for non-compliance. As a result, if a person deems the requirements in an order to be unreasonable because it may cause others physical or mental harm or injury, or significant economic loss then they are within their rights to not provide the assistance requested.
263. In the event that the operation of this section results in an acquisition of property from a person otherwise than on just terms, the Commonwealth is liable to pay a reasonable amount of compensation to the person. If the Commonwealth and the person do not agree on the amount of compensation, the person may institute proceedings in the Federal Court of Australia for the recovery from the Commonwealth of such reasonable compensation as the court determines.

## PJCIS term of reference 4: Interaction with foreign laws

264. The loss of evidence and intelligence resulting from fundamental shifts in communications services and technologies is a challenge that the international community is facing as a collective. This is often referred to as the ‘going dark’ problem and has severely impacted the ability of law enforcement around the world to lawfully access communications and data.
265. Australia has been working with like-minded countries to develop a global approach to this challenge which balances the need to resolve technological impediments to lawful access with respect for human rights and fundamental freedoms. The Assistance and Access Act introduced a more effective framework to collaborate with modern technology and communications providers and enhanced existing investigatory powers, while also protecting the privacy and data security of innocent users and maintaining the security of networks and systems. Similar models have been introduced into the laws of countries such as the United Kingdom and New Zealand to better reflect the realities of the modern communications environment and the growing use of anonymising technologies such as encryption.
266. Importantly, the Assistance and Access Act does not undermine Australia’s ability to foster bilateral and multilateral relationships with other countries to better facilitate ongoing mutual legal assistance and international crime co-operation processes. The prevalence of global communications providers operating outside of Australia has impacted the ability of governments to acquire electronic evidence that may be vital to pursuing criminal investigations in a timely, efficient manner. As a result, Australia must continue to work with international partners to establish robust international co-operation arrangements to access content and data pursuant to a domestic warrant or authorisation. The Clarifying Lawful Overseas Use of Data Act (the CLOUD Act), which became a United States federal law in March 2018, allows the United States to enter into executive agreements with other countries for reciprocal access under warrant to content data held by each country’s communications service providers. An agreement between the United States and Australia under the CLOUD Act would ensure that Australian law enforcement and national security authorities could access data that is controlled by United States communications service providers and is significant for lawful Australian investigations.

## Global approaches to the ‘going dark’ problem

### *The Statement of Principles on Access to Evidence and Encryption*

267. A critical milestone in addressing the ‘going dark’ problem was the signing of the Statement of Principles on Access to Evidence and Encryption (the Statement) at a Five Country Ministerial Meeting between Australia, Canada, New Zealand, the United Kingdom and the United States in August 2018. The Statement affirmed the need for countries to implement a domestic model that facilitates cooperation between law enforcement and industry to develop lawful access solutions while maintaining human rights and the security of communications.
268. The Assistance and Access Act ensured Australia implemented key principles in the Statement, including:
- Developing a mutual responsibility between governments and industry to ensure law enforcement agencies have access to lawfully obtained content, and
  - Ensuring that assistance requested from providers is underpinned by the rule of law and due process protections.

## Interaction between the CLOUD Act and the Assistance and Access Act

269. As of the time of this submission, Australia continues to advocate to be the next country the United States enters into negotiations for a cross-border access to data bilateral agreement under the United States CLOUD Act. Bilateral agreements such as those reflected under the CLOUD Act will complement existing international crime cooperation mechanisms (such as a mutual legal assistance) and will ensure that the increasing pressures on international crime cooperation between governments does not prevent law enforcement and national security agencies timely access to communications data.
270. Assessments undertaken by the Department identify that Australia is largely compliant with the requirements for qualifying foreign governments and has not identified any conflicts between an agreement with the United States under the CLOUD Act and the Assistance and Access Act.
271. The Department understands that the drafting of the CLOUD Act was intentionally neutral on issues relating to encryption.<sup>16</sup> Agreements under the CLOUD Act concern reciprocal cross-border access to communications content data via an 'order' (e.g. a warranted process). This matter is explored further in a White Paper released by the United States Department of Justice on April 2019:

*“While CLOUD Act agreements will bring significant benefits to governments investigating or seeking to prevent serious crime, they will not solve all problems related to law enforcement’s need for timely access to electronic evidence. Notably, the agreements will not address challenges posed to law enforcement by end-to-end encryption, where decryption capability is limited to the end user. The CLOUD Act requires that executive agreements be “encryption neutral,” neither requiring decryption nor foreclosing governments from ordering decryption to the extent authorized by their laws. This neutrality allows for the encryption issue to be discussed separately among governments, companies, and other stakeholders.<sup>17</sup>*

---

<sup>16</sup> This is provided for by Sec. 2523(b)(3), Chapter 119 of title 18, United States Code: “the terms of the agreement shall not create any obligation that providers be capable of decrypting data or limitation that prevents providers from decrypting data”.

<sup>17</sup> *Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act*, April 2019.

## PJCIS term of reference 5: Interaction with intelligence agencies' other powers

272. Schedule 5 of the Act allows ASIO officers to seek voluntary or compulsory assistance to gain access to intelligence on national security matters. Section 21A protects persons and bodies providing solicited or unsolicited information or assistance that is likely to assist ASIO in the performance of its functions. Section 34AAA ensures ASIO is able to compel technical and non-technical information or assistance from a person or body who owns, operates or administers a computer or network.
273. The Department is aware of a number of concerns with Schedule 5 that have been identified by the IGIS in their evidence to the PJCIS in previous reviews. The IGIS have recommended legislative amendments to further clarify how the assistance frameworks in sections 21A and 34AAA will operate and interact with other ASIO powers. The Department will continue to work with the IGIS and relevant agencies on these matters. The Department puts forward the following general comments to clarify the intended operation of section 21A and 34AAA.

### Voluntary assistance under section 21A

#### *Interaction with ASIO warrants and authorisations*

274. Section 21A establishes a framework to protect persons and bodies from civil liability where they provide voluntary assistance to ASIO in the performance of its functions. Assistance may be provided in accordance with a request by the Director-General, or as an unsolicited disclosure of information. The intent of these measures is to ensure persons or bodies are not prevented from, or hesitant to, provide voluntary assistance to ASIO in circumstances where civil liability may arise in relation to certain conduct. Protections provided under section 21A may encourage members of the public (including bodies) to come forward with critical information that may assist ASIO to protect Australians from a serious threat to security. Additionally, section 21A improves the utility of voluntary assistance and may limit the need to utilise more intrusive powers under a warrant.
275. Voluntary assistance under section 21A is not limited and can apply concurrently with other warrants and authorisations. However, section 21A does not prevent the Organisation from having to seek authorisation or a warrant for any actions completed by the Organisation, rather than the recipient of the immunity. Unlike immunities granted under a Special Intelligence Operation (under Part III, Division 4), section 21A is not intended to cover activities that would constitute an offence (and would therefore require a warrant for that activity to be undertaken). Noting these fundamental differences section 21A operates under a different authorisation process than that of a Special Intelligence Operation. Section 21A is clearly intended to exclude any criminal activity, and any activity that would constitute a significant loss of, or serious damage to, property.
276. Section 21A provides specific exclusions from civil immunity for conduct that is against a law of the Commonwealth, a State or a Territory, and conduct that results in significant loss of, or serious damage to, property. Moreover, unlike warrants or similar authorisations, section 21A is a voluntary framework and cannot be used to compel assistance.

### Compulsory assistance orders under section 34AAA

277. Section 34AAA provides that the Attorney-General may, at the request of the Director-General, make an order requiring a specified person to provide any information or assistance that is

reasonable and necessary to allow ASIO to access data held in, or accessible from, a computer or storage device that:

- is the subject of an existing warrant or authorisation, or
- is found, removed or seized, under an existing warrant or authorisation.

278. Section 34AAA is broadly modelled on powers available to law enforcement under section 3LA of the *Crimes Act*. The power ensures that ASIO is able to work cooperatively with its law enforcement partners by ensuring greater consistency and alignment with their powers, in a way that is adapted to ASIO's functions and operating environment.

279. It is anticipated that ASIO may use an order under section 34AAA to seek certain types of assistance to access devices, including to:

- compel a target or a target's associate to provide the password, pin code, sequence or fingerprint necessary to unlock a phone that is the subject of an existing computer access warrant under section 25A of the ASIO Act, or
- compel a specialist employee of a premises subject to an existing search warrant under section 25 of the ASIO Act to assist ASIO officers to interrogate the relevant electronic database, or use the relevant software, in order to obtain a copy of particular records or files.


280. Rather than compounding upon other warrants, section 34AAA facilitates the proper execution of powers already authorised by an existing warrant. When making the order the Attorney-General specifically considers the existence and type of that warrant which ensures that the power is only used to give effect to an existing power to access data. It is likely that by considering whether the required warrant is in place, the Attorney-General would turn their mind to whether another warrant has been issued for the same purpose, and the relevant outcome, prior to issuing an assistance order. In addition to this, a request must be accompanied by a statement outlining all previous requests for an order under section 34AAA relating to the person.

## Assistance orders under sections 21A and 34AAA, and Schedule 1 powers

281. As discussed in the Department's Supplementary Submission to the previous PJCIS review of the legislation, the intended operation of the industry assistance framework in Schedule 1 and the ASIO assistance orders in Schedule 5 are distinct.

282. The industry assistance framework is a graduated approach to ensuring law enforcement, national security and intelligence agencies can seek technical advice and assistance from 'designated communications providers' to access content on lawfully obtained devices and data. This assistance is provided by entities across the communications supply chain and will usually be technical in nature. This framework is intended to help agencies adapt to modern technologies which can inhibit investigations. The ability of Schedule 1 powers to obtain non-technical information or assistance is appropriately limited by the 'listed acts or things' in section 317E.

283. Assistance provided under section 21A and section 34AAA may include, but is not exclusive to, technical assistance. Section 21A allows an officer to seek non-technical advice and broader documents or information that are not limited to a designated communications provider's eligible activities or things of a technical nature. Similarly, section 34AAA allows an ASIO officer to compel those who are able to provide technical or non-technical information or assistance for the purpose of accessing data on computer networks or devices to do so. These compulsory assistance orders are also limited to specific ASIO warrants or authorisations, or matters that are of high importance to ASIO's functions and meets the threshold of prejudicial to security.



284. An important distinction to make is that the voluntary assistance framework under section 21A and the compulsory assistance framework under section 34AAA have particular purposes and are not part of the same framework.

## PJCIS term of reference 6: Impact on industry and competitiveness

285. The industry assistance framework in Schedule 1 is designed to ensure agencies can operate in the modern technological environment without imposing an undue regulatory or financial burden on providers, and without compromising the competitiveness and reputation of industry's products and services. The legislation does not impose any standing obligations for industry, or require providers to change their operating procedures or the design of their products and services by default. Moreover, requests for assistance are subject to detailed decision-making criteria and consultation requirements designed to protect business interests, data security and have minimal impact on industry.
286. However, according to advice received from industry, the perception of the legislation has had a material impact on the Australian market and the ability for Australian companies to compete globally. Consumers, international companies and investors are concerned domestically produced or located products and services have been undermined by the legislation, and that the industry assistance framework increases the costs of doing business in Australia. To address these concerns, the Department is focussing on engaging across government, with our international partners, with industry (both domestic and international) and in public spheres more broadly to clarify and reiterate the intent and operation of the law. The Department continues to meet with impacted stakeholders including members of the technology and communications industry to work through their concerns. The Department expects that the formal administrative guidance that has been developed will also help to address misconceptions regarding the legislation by providing detailed analysis of the practical operation of key measures and reinforcing the consultative and collaborative nature of the industry assistance framework.

### Obligations

287. The industry assistance framework does not place any immediate or ongoing obligations on providers. Providers will only be required to give assistance in the event of a formal request or notice being issued which relates to their eligible activities.
288. The industry assistance framework does not require companies to fundamentally change the way they conduct their business operations in Australia. Consumers, and international providers and investors should have confidence that no provisions in the legislation will lead to significant changes to how services and products are developed in Australia. To the extent that the provisions do interact with Australian products or operations, requirements are bounded by security guarantees in the laws, consultation requirements and core decision-making criteria which reinforces the need for decision-makers to hold impact on businesses at the forefront of their mind.

### Financial compensation for assistance

289. The default position in the legislation is that providers should not absorb the reasonable costs of assistance given to the Government under the industry assistance framework. The legislation aims to ensure that providers are not unnecessarily financially impacted when meeting the requirements of an assistance request or notice.
290. Subsection 317ZK(3) states that, a provider is not expected to bear the reasonable costs of complying with an assistance request or notice. Reasonable costs refer to the costs necessary to satisfy the requirements under an assistance request or notice. Importantly, providers will not be compensated for costs that are not related to the assistance required. For example, if a provider's



expenditure is higher than necessary to satisfy an assistance request or notice, they are entitled to recover costs equivalent to the expenditure that would have been reasonable to satisfy the requirements.

291. The administrative guidance discusses the assessment undertaken to determine the reasonable costs associated with an assistance request or notice. Broadly speaking, this cost assessment is undertaken through a collaborative approach that considers the obligations on the provider. A more detailed discussion on cost assessment is set out below.
292. The legislation also provides scope for the relevant agency and provider to enter into commercial terms. For example, commercial terms may be suitable in cases where agencies require a provider to develop a large bespoke capability that would ordinarily be the subject of a significant procurement. The availability of commercial terms will give an agency the flexibility to enter into an arrangement containing both financial incentives and risk-management measures to secure satisfactory and timely performance.
293. Importantly, providers are only expected to comply with the requirements of a notice to the extent that they are capable of doing so. For example, if a provider does not have the resources, or the means to acquire the resources, to comply with requirements they will not be expected to do so.
294. Agencies may also enter into alternative cost arrangement if they are satisfied that no-profit/no-loss compliance would be contrary to the public interest. The threshold to satisfy this test is high and it is expected an agency will only be able to meet the requirements in exceptionally rare circumstances. For example, where a provider's conduct has wilfully created a security risk or specifically designed their services for illicit use. It may also be appropriate in cases where the provider subject to a notice acted recklessly or negligently in providing the required assistance and it would be inappropriate to compensate the provider.

## Cost assessment

295. The administrative guidance discusses the importance of agencies and providers determining the costs for meeting the requirements in an assistance requests or notice during the preliminary or mandatory consultation periods.
296. It is best practice for the issuing agency to request that the provider conduct a preliminary assessment on the costs for providing assistance. The provider may conduct this assessment in accordance with their own standard practices and give it to the applicable costs negotiator.
297. This assessment may include seeking cost information from external third parties where necessary, while withholding the purpose for which the external products or expertise are being costed where possible. The nature of the preliminary cost assessment will depend on the provider's business and the assistance being sought. The preliminary assessment undertaken by the provider and the operational needs of the issuing agency will then be considered during the formal cost assessment made by the applicable costs negotiator.
298. Practically speaking, agencies will consider the following aspects when undertaking a cost assessment of an assistance request or notice:
  - the complexity of assistance
  - the size and capability of the provider
  - the opportunity costs associated with providing the assistance, and
  - other matters the agency considers relevant.

299. The provider and applicable costs negotiator should reach an agreement as to costs, having regard to both assessments. If an agreement cannot be reached an arbitrator, approved by both parties, may be appointed to determine an alternative rate of compensation (see below).

## Arbitration

300. If the provider and agency cannot agree on the terms and conditions of compliance with a notice, an arbitrator, approved by both parties, may be appointed to resolve the dispute.
301. In the event providers and agencies cannot agree on the appointment of an independent arbitrator, the Australian Communications Media Authority (ACMA) or the Attorney-General will appoint an arbitrator to determine the terms and conditions under subsections 317ZK(5)–(14). This mechanism is consistent with the method for resolving disputes on the terms and conditions of existing industry assistance under section 314 of the Telecommunications Act.

## Decision-making criteria and consultation requirements

302. The industry assistance framework is supported by strong limitations and safeguards and the risk that proposed requirements have unintentional and disproportionate impacts on a provider is mitigated by consultation requirements and decision-making criteria. These ensure that the objectives of a formal assistance request or notice are balanced appropriately with the interests of the provider.
303. Prior to issuing a notice, the decision-maker for an agency must be satisfied that the requirements in a proposed notice are reasonable and proportionate. In determining the reasonableness and proportionality of a notice, the decision-maker must turn their attention to a number of matters including the legitimate interests of the provider. This requirement means that agencies will take into account any adverse business or financial consequences to the provider in meeting the proposed requirements in a notice.
304. As detailed in the administrative guidance, the preliminary and mandatory consultation periods provide an opportunity for the provider to formally raise any issues for the decision-maker's consideration, including whether the requirements impact their business operations or will require a fundamental change to their product development.
305. Given the gravity of TCNs, the approval of a notice is subject to the Attorney-General and the Minister for Communications. The involvement of the Minister for Communications provides another avenue for the communications industry to have their concerns properly considered.

## Australian products and services are secure

306. The industry assistance framework is designed to maintain and protect the security of networks and devices. The legislation expressly prohibits activities that would undermine cyber security on a systemic level and excludes conduct that would inadvertently make the communications of the general public or business community less secure. Agencies cannot require a company to:
- jeopardise information security, including by doing things that would increase the risk of hacking;
  - weaken electronic protections applied across a range of services or devices (e.g. end-to-end encryption);
  - refrain from patching a weakness; or

- build decryption capabilities.
307. These safeguards rule out the construction of law enforcement keys or so-called 'exceptional access' systems.
308. The law has review processes to assess whether a security risk is present. Notably, providers are able to seek independent review of the technical and legal parameters of a proposed TCN to determine if compliance with the notice would cause a security risk. Providers are also able to seek judicial review of the decision to issue a notice if they believe compliance with that notice will create a security risk in their products or service.
309. Further, just because a business may be in a position to assist agencies through Part 15, this does not mean that the data they hold will be accessible by Government authorities. An underlying warrant or authorisation, tied to an investigative and subject to additional thresholds and approval processes (including prior judicial oversight) must be present to access personal information. In many cases, Australia's warrant regime will not extend to the broader scope of designated communications provider as defined in section 317C.

## Requests for assistance are served on the corporate entity

310. Domestic and international providers have raised concerns that assistance requests will be served on their individual employees unbeknownst to the provider, and that employees will be unable to discuss the assistance requests within their organisation, as required. This concern is unfounded in the legislation and has been clarified in the administrative guidance. However the Department is also considering other ways to address this issue.
311. The intention of the industry assistance framework is to allow agencies to seek assistance from an entity that meets the definition of a 'designated communications provider' in section 317C of the Act. In other words, the intent and operation the framework is for agencies to seek assistance from an organisation, company or corporate entity itself and not from an individual in their capacity as an employee.
312. Practically speaking, agencies are likely to contact an employee of a 'designated communications provider' when formally issuing a request for assistance. In this sense, the employee is a representative of the entity to whom the assistance request must be directed. Subsection 317ZF(3)(a) allows information about assistance to be disclosed for the purpose of administering or executing a notice are relevant. This ensures employees are able disclose information within an organisation for the purpose of actioning assistance.
313. Importantly, the Act's provision for civil penalties against individuals is not intended to apply to employees of a non-compliant company. If a provider does not comply with their assistance obligations, any enforcement action that may be undertaken will apply to the enterprise. Penalties for individuals in the legislation are for the purpose of potential enforcement proceedings against sole-traders and individuals acting in their own legal capacity.
314. The IGIS and Commonwealth Ombudsman have oversight of all requests and notices. In the event a request is issued (improperly) to an individual within a company, the relevant oversight body would be able to highlight and act upon this instance of non-compliance with the legislation and administrative guidance.

## Communications material

315. The Department is leading the development of communications material to clarify the intended operation of the industry assistance framework. According to advice received from industry,

companies lack a clear understanding of the obligations in the legislation, and have concerns regarding the potential impact the industry assistance framework may have on product development and their current operating procedures. Some industry providers are reporting that these concerns have also caused investors to re-evaluate engaging with the domestic communications and technology markets.

316. A significant proportion of these concerns stem from misconceptions regarding the intent and operation of the industry assistance framework. The purpose of the Department's communications material is to:

- accurately communicate the intended purpose and effect of the legislation;
- address the core concerns of industry and investors; and
- provide practical examples for how the key measures and safeguards will operate, and the potential impact on different stakeholders.

317. As discussed above – and as the communications material will reiterate, the industry assistance framework does not:

- impose any standing obligations on industry;
- require business practices or product development to change;
- undermine the security of devices or networks;
- allow for the construction of decryption capabilities or so-called 'backdoors';
- require companies to jeopardise information security for innocent users; or
- require employees of companies to work in secret without their employer's knowledge.

318. The communications material being developed by the Department includes:

- factsheets for investors and industry;
- frequently asked questions; and
- practical examples on the operation of the Act.

319. The Department has been developing communications products in consultation with those Commonwealth agencies and departments that have an ongoing engagement with the technology and communications industry or relevant interest in the legislation. This includes the Attorney-General's Department, Department of Communications and the Arts, Department of Industry, Innovation and Science, Australian Trade and Investment Commission (Austrade), Department of the Prime Minister and Cabinet, ASIO, ACIC, AFP, Defence Portfolio, and Department of Foreign Affairs and Trade.

## PJCIS term of reference 7: Reporting obligations and oversight measures

320. As discussed in the Department's supplementary submission to the Act review<sup>18</sup>, a number of amendments have been made to meet recommendations 4, 5 and 12 of the Advisory Report concerning oversight. These amendments were developed in consultation with oversight bodies, and are intended to strengthen the IGIS and the Ombudsman's oversight of the powers and significantly refine independent scrutiny across all Schedules in the legislation. The Department refers to that supplementary submission for a more detailed discussion of how recommendations 4, 5 and 12 of the Advisory Report have been addressed.
321. The Department will continue to work with the oversight bodies and relevant agencies on resolution of these outstanding issues – whether this involves administrative guidance, procedures or, if required, consideration of legislative amendments.

### Commonwealth Ombudsman

322. The Department continues to be aware of the Commonwealth Ombudsman's recommendation that the Home Affairs Minister's power to redact Ombudsman reports into the operation of the Assistance and Access Act under subsection 317ZRB(7) be removed. This power was created to protect the sensitive information of industry engagement from unintentional public disclosure. The AFP has raised concerns regarding the need to continue to protect sensitive information from public disclosure in the event of a legislative amendment to remove this power.
323. The Department understands an alternative to the Minister's redaction power may be to undertake conditional vetting between the Ombudsman and agencies prior to publication. This will leverage the constructive relationships shared by law enforcement agencies and the Ombudsman.
324. As discussed earlier in this submission, any requests for additional resourcing for the Commonwealth Ombudsman will be considered by the Government through standard processes.

### Inspector-General of Intelligence and Security

325. The Department is also continuing to work with the IGIS to address outstanding concerns through a variety of legislative and non-legislative solutions.
326. As discussed earlier in this submission, any requests for additional resourcing for the IGIS will be considered by the Government through standard processes.

---

<sup>18</sup> Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018, Submission 16.1 page 2.

## Conclusion

327. The passage of the Assistance and Access Act was a critical step towards ensuring Australia's law enforcement, national security and intelligence agencies can operate effectively in the evolving technological environment. Where traditionally most communications were carried over domestic landlines, today over-the-top providers dominate the telecommunications landscape with most transmissions originating from a mobile or internet-connected device. Australians now rely on sophisticated and portable devices such as mobile phones and anonymising technologies to securely engage on digital platforms. These rapid changes in communications technology eroded agencies' ability to rely on existing investigatory powers provided for in legislation decades ago.
328. The Assistance and Access Act builds on the pre-existing telecommunications and surveillance law framework to equip agencies to face this challenge. The Act provides agencies with the necessary tools and powers to ensure they can continue to discharge their lawful functions to protect the Australian community. Key measures in the legislation, including the industry assistance framework in Schedule 1, have been used by agencies to overcome technological impediments to legitimate investigations.
329. The Department has engaged extensively across the Commonwealth, the States and Territories, and with industry to develop guidance material to ensure the powers in the legislation are used as intended and with respect to the important safeguards and oversight measures. The Department will continue its efforts, working with Commonwealth colleagues, to implement the legislation.
330. International companies and investors looking to engage in the domestic market should have confidence that the legislation establishes no standing obligations on industry, and does not, or indeed cannot, undermine the security of products and devices.
331. The Assistance and Access Act is supported by strong safeguards and oversight measures that protect business interests and the privacy of Australians, maintains the security of the digital ecosystem and ensure the powers are exercised responsibly.
332. The operation of the Assistance and Access Act to date indicates that overall, the current key settings afford an appropriate balance between the operational needs of agencies, the protection of civil liberties and the interests of providers. However the Department and the broader Portfolio will continue to monitor this closely, including through engagement with the INSLM and PJCIS reviews, ongoing engagement with oversight bodies, and with the communications and technology industry.