Australian Government
Department of Home Affairs

Department of Home Affairs supplementary submission to the Review of the amendments made by the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018

Joint Parliamentary Committee on Intelligence and Security

6 August 2020

Table of Contents

Introduction

1. The Department of Home Affairs (the Department) welcomes the opportunity to make a supplementary submission to the Parliamentary Joint Committee on Intelligence and Security's (the Committee) review of the amendments made by the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (Assistance and Access Act).

2. The Department would like to thank the Independent National Security Legislation Monitor (the Monitor) for his consideration of the Assistance and Access Act.

3. This submission provides commentary in relation to the Monitor's recommendations to assist the Committee when considering the Monitor's findings in the context of this Review. This submission is not a Government response to the Monitor's review. The Government will carefully consider the findings made by the Monitor, and by the Committee, when it completes its third review of the Assistance and Access Act.

Recommendations of the Independent National Security Legislation Monitor

1. Recommendation 1: Anti-corruption and integrity commissions

4. The Monitor recommends that State and Territory anti-corruption commissions be included within the list of agencies empowered to give technical assistance requests, technical assistance notices, and technical capability notices.

5. This is consistent with the Parliamentary Joint Committee on Intelligence and Security's (PJCIS) interim recommendation made on 12 February 2019, in its second review of the Assistance and Access legislation. As noted in the Department's main submission to the current PJCIS review,[1] an expansion to allow Commonwealth and State anti-corruption bodies and investigative commissions to have access to the industry assistance framework is also consistent the Government's original intent in the exposure draft of the Assistance and Access Bill.

6. 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.

2. Recommendation 2: Technical assistance requests

7. The Monitor recommends no change to the capacity of relevant agencies and designated communications providers to agree technical assistance requests, other than that a prescribed form be used.

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

3. Recommendation 3: Administrative Appeals Tribunal authorisation of compulsory notices

9. The Monitor recommends that technical assistance notices and technical capability notices should be approved by a new division of the Administrative Appeals Tribunal (AAT)—to be known as the Investigatory Powers Division—in place of the current models of authorisation. The Monitor further recommends that technical capability notices require Commonwealth agencies to apply for the agreement of the Attorney-General to then apply to the AAT, though recommends that State and Territory agencies (and any Commonwealth Integrity Commission with these powers) not require the approval of the Attorney-General to apply to the AAT.

10. As noted by the Monitor, long before the reforms enacted by the Assistance and Access Act, section 313 of the Telecommunications Act has required carriers and carriage service providers to assist law enforcement and intelligence agencies. In particular, subsection 313(3) requires carriers and carriage service providers to give officers and authorities of the Commonwealth, and of the States and Territories, such help as is reasonably necessary for specified purposes.

---

[1] Department of Home Affairs' Main Submission (Submission 16) to Parliamentary Joint Committee on Intelligence and Security's Review of the amendments made by the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018*, page 6.

11. The Assistance and Access Act builds on these longstanding assistance obligations. As with the industry assistance framework in the Assistance and Access Act, agencies' requests for assistance under section 313 are internally authorised and require the assistance provider to be compensated. However, the Assistance and Access Act framework enhanced the authorisation process, elevating authorisation to agency head level in the case of TANs, and to the Attorney-General (with numerous additional safeguards) in the case of TCNs.

12. The Assistance and Access amendments ensure that there continues to be equal assistance available to agencies to overcome investigative obstacles regardless of their physical or digital nature. For example, a law enforcement agency may effect a search warrant where it is alternatively obstructed by a physical lock and a digital lock.

13. Departing from this model, a requirement to obtain separate approval by the AAT to seek industry assistance would increase the requirements that need to be met to investigate suspects who have chosen to use sophisticated technology to facilitate wrongdoing rather than physical methods.

14. One of the principles which underpins the industry assistance framework is that where offline activities can be investigated with a single warrant or authorisation, it should also be possible to investigate their online equivalents at this same legal standard. To do otherwise would be to increase the requirements that must be met solely because suspects have chosen to use technology to enable their alleged offending.

15. Detailed safeguards are included in the existing industry assistance framework to ensure use of the framework does not diminish internet, software, device or data security.

16. Industry assistance does not authorise agencies to obtain data but may facilitate access to legible forms of data which were obtained under a separate warrant or authorisation under pre-existing electronic surveillance legislation (for example interception warrants under the *Telecommunications (Interception and Access) Act 1979)*. This feature of the industry assistance framework is legislated in section 317ZH of the Telecommunications Act.

17. Electronic surveillance powers (such as interception warrants) were enacted to ensure agencies could obtain the information they need to investigate and prosecute crimes and threats to national security, under warrant or authorisation. The protections associated with the use of these powers and oversight of agencies' use support this. For example, the requirement that issuing authorities consider how the privacy of persons targeted by the powers will be affected. Technological advancements diminished the extent to which these powers, in isolation, could ensure agencies obtain legible information under these warrants or authorisations. The industry assistance framework facilitates the additional technical assistance that is likely to be required into the future to ensure information obtained under a separate warrant or authorisation is rendered legible and useful for agencies.

3.1 Comparison with the International Production Order Bill 2020

18. In his discussion of the International Production Order Bill 2020 (International Production Order Bill), the Monitor suggests that the framework in that Bill for AAT members to authorise international production orders (in particular with reference to ASIO) supports the position that AAT members should authorise technical assistance and capability notices.2

19. The International Production Order Bill's authorisation model was created to meet requirements to obtain a Clarifying Lawful Overseas Use of Data (CLOUD) Act agreement with the United States. As a result, that bill may not reflect typical authorisation processes for other Australian electronic surveillance regimes.

20. Like electronic surveillance powers, international production orders are directed at obtaining communications. The industry assistance framework in the Assistance and Access Act is not directed at obtaining communications. It is directed at seeking technical industry assistance to agencies, including assistance to access legible versions of the information found in communications obtained under a warrant. In this sense, international production orders are more comparable with electronic

[2] Commonwealth of Australia, Independent National Security Legislation Monitor, *Trust but verify: A report concerning the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 and related matters*, page 202.

surveillance warrants, and thus have been designed to mirror domestic authorisation processes to the fullest extent possible.

4. Recommendation 4: New Investigatory Powers Division of the AAT

21. The Monitor recommends that a new 'Investigatory Powers Division' be established as part of the AAT with the function of approving the giving of technical assistance notices and technical capability notices. The Monitor further recommends that this approval not be exercised *persona designata*; that is, not in the personal capacity of the AAT members, but rather as part of the AAT members' formal statutory functions.

22. The AAT may not be the appropriate body to undertake this proposed function.

23. The AAT forms part of Australia's administrative law framework, responsible for providing independent merits review of a range of administrative decisions made under Commonwealth laws. In contrast with this responsibility, the proposed function is more akin to the issuing of law enforcement warrants, currently undertaken by judicial officers and members of the AAT in their personal capacity.

24. As a primary decision-making exercise, the approval of technical assistance notices and technical capability notices would be a significant departure from the merits review function performed by the AAT. A similar function is not conferred on AAT members in their official capacity by any other piece of legislation. Therefore, the proposed Investigatory Powers Division would operate differently to any other AAT division and may require significant legislative amendments to the A*ustralian Administrative Appeals Tribunal Act 1975*, including modifying the basic objectives of the AAT and creating an entirely new function for the AAT.

25. This may create practical issues for AAT members and its administration. As each AAT division performs the same fundamental merits review function, AAT members are generally assigned across multiple divisions to efficiently manage caseloads and fluctuations in demand. Further, AAT members require training to familiarise themselves with the new legislation that confers jurisdiction on the AAT. It is questionable whether members serving in the proposed division could be similarly assigned, given the specialist skills and knowledge they would be required to have. Given the proposed function is very different to the AAT's merits review functions, the appointment of the additional members and support staff needed to discharge this function, and associated training costs, may be higher than the Monitor had anticipated.

26. Expanding the AAT with a new division for these functions would also be at odds with the decision to amalgamate the Social Security Appeals Tribunal, and the Migration Review Tribunal – Refugee Review Tribunal with the AAT in 2015. This amalgamation aimed to enhance efficiencies in merits review processes and to harmonise practices, aims which may be challenged by the conferral of these new functions of the AAT.

27. Given the differences between the current function of the AAT and the functions of the proposed new division, it is unlikely that the creation of the new division could be carried out with minimal expense as observed by the Monitor.3 Further, given there have been no TANs or TCNs to date, and agencies continue to advise they expect they will be used sparingly, the cost of establishing such a division would be large, when considered against the number of applications the new division is likely to consider each year.

5. Recommendation 5: Functions of the Investigatory Powers Commissioner

28. The Monitor recommends that a new statutory office holder, the Investigatory Powers Commissioner, be created as the head of the proposed investigatory powers division. The Monitor recommends that the Investigatory Powers Commissioner's functions should include developing and approving the prescribed forms for giving technical assistance requests, technical assistance notices, and technical capability notices, and issuing guidelines.

29. The Department has previously provided guidelines for the use of the industry assistance framework which are available on the Department's website.4

30. The Department offers no further comment on the other functions of the proposed Investigatory Powers Commissioner but refers the Committee to the above discussion regarding recommendations 3 and 4.

6. Recommendation 6: Appointment of the Investigatory Powers Commissioner

31. Please refer to the responses to recommendations 3, 4 and 5.

7. Recommendation 7: Offence threshold for industry assistance powers

32. The Monitor recommends that the definitions of *serious Australian offence* and *serious foreign offence* be amended to reflect the definition in section 5D of the *Telecommunications (Interception and Access) Act 1979* (Telecommunications (Interception and Access) Act). This would raise the offence threshold for the use of the industry assistance framework generally above the current threshold of three years' imprisonment.

33. The current offence threshold was selected to ensure that the industry assistance framework could be used to complement the range of investigative powers already available to agencies. These powers, and their respective offence thresholds, include:

    (a) telecommunications interception offences ranging, in general, from 10 penalty units[5] to seven years' imprisonment or more

    (b) obtaining stored communications offences which generally attach penalties of three years' imprisonment or more, and

    (c) surveillance devices offences with penalties of three years' imprisonment or more.

34. The Monitor's recommendation would preserve the ability to obtain industry assistance in relation to the interception of telecommunications. However, it would exclude numerous offences which may form the basis of a warrant to obtain stored communications or install a surveillance device. Many technical assistance requests have been given to support the execution of surveillance device warrants. Surveillance devices warrants carry an offence threshold of three years' imprisonment which allows many offences outside of the section 5D threshold to form the basis of an application to use a surveillance device.

35. Adopting this recommendation would increase the likelihood that law enforcement agencies will be unable to issue a technical assistance request. This recommendation would also limit the availability of industry assistance to overcome technological obstacles frustrating the use of stored communications and surveillance device warrants.

36. Further examples of particular offences from the *Criminal Code Act 1995* (Criminal Code) which meet the current threshold for industry assistance and would be excluded by the INSLM's proposal are:

- Possession or control of data with intent to commit a computer offence (section 478.3)
- Using a carriage service to menace, harass or cause offence (section 474.17)
- Associating with terrorist organisations (section 102.8)
- Dealing with property suspected of being proceeds of crime (section 400.9)

---

[4] Department of Home Affairs, *Administrative Guidance on the Use of Part 15 of the Telecommunications Act*, https://www.homeaffairs.gov.au/nat-security/files/assistance-access-administrative-guidance.pdf.

[5] Paragraph 5D(4)(a) of the *Telecommunications (Interception and Access) Act 1979* provides that a serious offence includes an offence against Part 10.2 of the *Criminal Code Act 1995* which includes an offence with a penalty of ten penalty units.

- Dealing with inherently harmful information by Commonwealth officers (section 122.1)
- Conduct by Commonwealth officers causing harm to Australia's interests (section 122.2), and
- Possessing equipment used to make identification documents (section 372.3).

37. The exclusion of many computer offences, which most commonly carry a penalty of three years' imprisonment, is particularly relevant given the importance of industry assistance to investigate those offences, and that gathering evidence of those offences will almost certainly require accessing a computer. Excluding these computer offences may undermine the purpose of the Assistance and Access Act and potentially hamper the investigation of these offences.

8. Recommendation 8: Deletion of systemic vulnerability

38. The Monitor recommends the removal of 'systemic vulnerability' as a concept in relation to industry assistance powers on the basis that this is interchangeable with 'systemic weakness' which would remain. The department notes that term 'systemic vulnerability' was originally included in addition to 'systemic weakness' based on advice from industry that this would most accurately reflect the common language used to discuss cybersecurity vulnerabilities.

9. Recommendation 9: Changes to systemic weakness

39. The Monitor recommended that the provision dealing with reserve capabilities in the prohibition against the introduction or implementation of a systemic weakness be rewritten as follows (added words in bold type):

> Subsection 317ZG(4A) Telecommunications Act: In a case where a weakness is selectively introduced to one or more target technologies that are connected with a particular person, the reference in paragraph (1)(a) to implement or build a systemic weakness into a form of electronic protection ~~includes~~ **means** a reference to any act or thing that ~~will, or is likely to, jeopardise the security of any information held by any other person~~ **creates a material risk that otherwise secure information will be accessed, used, manipulated, disclosed or otherwise compromised by an unauthorised third party**.

40. The effect of the textual changes to subsection 317ZG(4A) would not significantly alter the current operation of this prohibition, which already sets out at subsection 317ZG(4C) that the security of information is placed in jeopardy *when there is a material risk of access*. The proposed changes further expand this concept of jeopardy by extending these circumstances beyond 'access' to include when information is 'used, manipulated, disclosed, or otherwise compromised'.

41. The Monitor also recommends that *otherwise secure information* be defined to mean 'information of, any person who is not the subject, or is not communicating with the subject, of an investigation', and that *unauthorised third party* be defined to mean 'anyone other than a party to the communication, the agency requesting the relevant technical assistance request, technical assistance notice or technical capability notice and/or integrity agencies'.

42. It is unclear which communication platforms would be covered within the concept of 'communicating with the subject' in the proposed definition of *otherwise secure information*. While this may clearly include direct messages exchanged between two parties, it is unclear how this definition would apply to a person who receives a communication from a broadcast platform or open forum where the originator of the communication is not aware of all recipients. This definition may not clarify the systemic weakness prohibition in some contexts.

43. The Monitor notes this concern:

> People also communicate indirectly and in groups – for example, using Facebook posts and WhatsApp groups. So it is not just a case where Person A communicates directly with Person B; a group of people communicate directly and indirectly with each other.[6]

[6] Above n 2, page 102.

44. The proposed definition of *unauthorised third party* may create a situation where the disclosure of information obtained by an agency requesting assistance to another agency involved in an investigation is prohibited as an example of a systemic weakness, as that second agency would be an *unauthorised third party*. This is because the proposed definition excludes only the direct parties to a communication and the requesting agency itself from being an unauthorised third party.

45. This would potentially cause legitimate information sharing between agencies to become an example of a prohibited systemic weakness. As limiting information sharing between agencies is not the purpose of the systemic weakness prohibition, this would appear to be an unintended consequence of fully adopting this recommendation.

10. Recommendation 10: Changes to definitions of 'target technology' and 'electronic protection'

46. The Monitor recommends that *target technology* be defined to refer to the specific instance of the technology used by the intended target and that the definition of *electronic protection* include a list of non-exhaustive examples of things which are excluded.

47. The Department considers that the existing construction of *target technology* is already limited in this way. For example, *target technology* in respect of a carriage service is currently defined as being (section 317B Telecommunications Act):

> a particular carriage service, so far as the service is used, or likely to be used, (whether directly or indirectly) by a particular person, is a target technology that is connected with that person…

48. The second aspect of the Monitor's recommendation seeks to include non-exhaustive examples of things excluded from the definition of *electronic protection*. The Department is of the view that the definition of *electronic protection* already offers two, broad examples of what the term does cover (being authentication and encryption).

49. The Monitor suggests:

> Examples could be given to clarify whether it was intended that weakening forms of physical protection is acceptable, as this can be limited to operation on a specific instance of the technology. In this case, an example not covered by the 'electronic protection' term may be assisting to bypass tamper detection mechanisms when opening up a mobile phone to access data stored on its electronic components inside.[7]

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

11. Recommendation 11: Designated communications provider

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

12. Recommendation 12: AFP Commissioner's role in technical assistance notices

52. The Monitor recommended that the Australian Federal Police Commissioner no longer be required to approve the giving of technical assistance notices by the police force of a State or Territory, currently required by section 317LA Telecommunications Act. This is consistent with the department's previous submission to the Committee.[8] This could be extended so that the Australian Federal Police

[7] Above n 2, page 230.
[8] Above n 1, page 30-31.

Commissioner would also no longer be notified when a technical assistance notice is given by a law enforcement agency of a State or Territory.

13. Recommendations 13 – 15: Computer access warrants

13.1 Recommendation 13: Incidental interception

53. The Monitor recommends that computer access warrants continue to provide authority for agencies to engage in incidental interception. This is appropriate as the interception is not for the purposes of collecting evidence or intelligence – if authorised, it is being done incidentally, for the purpose of doing a thing specified in the warrant.

13.2 Recommendation 14: External approval for concealment activities after 28 days

54. The Monitor recommends that agencies be required to seek an additional external authorisation in order to perform an activity to conceal that a computer access warrant has been used against a target, where that activity occurs outside the 28 day period following the expiry of a warrant.

55. The current provisions provide for agencies to perform activities to conceal that a computer access warrant has been used at any time while the warrant is in force or within 28 days after the warrant ceases to be in force, or at the earliest time after that 28 day period at which it is reasonably practicable to carry out those concealment activities. A period of longer than 28 days would be required, for example, where a device used to effect a computer access warrant is moved by the target and the agency must wait an indeterminate amount of time for it to be physically relocated and recovered.

56. Making provision for concealment activities allows an agency to prevent targets learning that they are under investigation and attempting to frustrate further efforts to gather evidence of their activities. The Department would need to work with agencies to better understand the potential operational consequences of implementing this recommendation.

13.3 Recommendation 15: Return of items temporarily removed

57. The Monitor recommends that ASIO be required, by legislative amendment, to return items temporarily removed under a computer access warrant once they are no longer prejudicial to security or otherwise as soon as *reasonably practicable* – replacing the existing language of subsection 25A(4A) of the *Australian Security Intelligence Organisation Act 1979* (ASIO Act) which requires the items be returned *within a reasonable period*.

58. This recommendation would place ASIO's computer access warrant framework out of step with requirements to return seized items under other warrants available to ASIO such as search warrants under paragraph 25(4C)(b) and identified person warrants under paragraph 27D(5)(b) which require items to be retained *for only such time as is reasonable*. The Monitor's recommended language would impose a more positive obligation to return items seized under a computer access warrant than other warrants.

14. Recommendations 17 – 18: Schedules 3 and 4

14.1 Recommendation 16: Monitoring prosecutions/convictions

59. The Monitor recommends that agencies and the public continue to monitor public information concerning prosecutions and convictions stemming from the failure to comply with an assistance order under section 3LA of the Crimes Act or section 201A of the Customs Act.

60. The Department notes this recommendation, and the Monitor's intention that this will permit any trends to be discerned as more time passes.

14.2 Recommendation 17: Clarification powers do not authorise detention

61. The Department confirms that section 3LA of the *Crimes Act 1914* (Crimes Act) and section 201A of the *Customs Act 1901* (Customs Act) are not intended to authorise the detention of persons to whom

the relevant orders apply where the agency in question does not otherwise have any lawful basis to detain the person.

62. The Australian Federal Police does not use and does not consider section 3LA (which requires a 'person with knowledge of a computer or a computer system to assist access etc.') as a detention or quasi-detention power. The Australian Federal Police considers that the use of section 3LA to detain a person would not constitute a proper use of the power.

14.3 Recommendation 18: Monetary penalty be retained

63. The Monitor recommends the retention of a monetary penalty as an alternative to imprisonment for assistance orders under both section 3LA of the Crimes Act and section 201A of the Customs Act, as already included in the legislation.

15. Recommendations 19 – 23: Schedule 5

15.1 Recommendation 19: Limit the scope of ASIO assistance requests

64. The Monitor recommends that ASIO's power under subsection 21A(1) of the ASIO Act to confer civil immunity on persons or bodies in return for their assistance be limited to only the kinds of assistance that may be volunteered under subsection 21A(5). This would mean the types of assistance for which ASIO may offer civil immunity when proactively seeking assistance would be restricted to the provision of information or documents. Currently, subsection 21A(1) allows civil immunity to be offered for conduct which is reasonably likely to assist ASIO in the performance of its functions.

65. Examples of conduct for which immunity may be conferred under subsection 21A(1) include:

    (a) breach of contract,

    (b) infringement of property rights, and

    (c) other conduct which amounts to a tort.

66. The types of conduct where the conferral of civil immunity is available are effectively limited by the restrictions in paragraphs 21A(1)(d) and 21A(1)(e) to only conduct which does not amount to the commission of an offence against a law of the Commonwealth, a State or Territory, or which does not result in significant loss of, or serious damage to, property.

67. Implementing this recommendation could remove a potential incentive for external sources to cooperate with ASIO by closing an avenue to provide them with a limited civil immunity where their actions may otherwise give rise to an action against them.

15.2 Recommendation 20: Limitations on civil immunity

68. The Monitor recommends that the civil immunity available when the conditions of subsection 21A(1) or 21A(5) of the ASIO Act are met be limited to exclude immunity for conduct resulting in serious personal injury or death to any person.

69. In its existing formulation subsection 21A(1) excludes conduct that results in significant loss of, or serious damage to, property.

15.3 Recommendation 21: Director-General and Deputy to authorise voluntary assistance arrangements

70. The Monitor recommends that assistance requests under subsection 21A(1) of the ASIO Act only be issued by the Director-General of Security or a Deputy Director-General. This would limit the current situation which permits the Director-General of Security to delegate the power to issue these requests to a senior position-holder within ASIO.

71. This power is non-compulsory and cannot be used to request conduct which would constitute a criminal offence in any Australian jurisdiction. The Director-General has the power to delegate the ability to make these requests to senior position-holders within ASIO. Adopting this recommendation

may constrain the ability of ASIO to obtain assistance in a timely manner and may be a particular concern where a request must be made as a matter of urgency.

15.4 Recommendation 22: Interaction with technical industry assistance under Schedule 1

72. The Monitor recommends that subsection 21A(1) assistance requests be limited such that they cannot be used to seek assistance that could be provided under a technical assistance request. This would have the effect of preventing subsection 21A(1) being used to seek assistance when the assistance would be sought from an entity which is also a designated communications provider and where the assistance is of the same kind, class or nature as those listed acts or things set out in subsection 317E(1) of the Telecommunications Act.

73. Adopting this recommendation may frustrate ASIO's ability to issue similar assistance requests to multiple different entities simultaneously where some entities are designated communications providers and may be given a technical assistance request or notice, while others are not. This would confer different legal protections and place entities within different legal frameworks when they provide ASIO with the same type of assistance simultaneously.

74. Adopting this recommendation alongside Recommendation 19 would limit the use of subsection 21A(1) to only obtaining information or documents from a person or body who is not a designated communications provider. This would create two gaps in the capacity of ASIO to offer a limited civil immunity in return for assistance; firstly, when a party outside the definition of designated communications provider is asked to engage in conduct within the listed acts or things; and secondly, when a party within the definition of designated communications provider is asked to engage in the broader types of conduct currently available under subsection 21A(1). These gaps may impact ASIO's ability to fulfil its statutory functions.

15.5 Recommendation 23: Clarification section 34AAA does not authorise detention

75. The Monitor recommends that section 34AAA of the ASIO Act be amended to specify that it does not permit ASIO to detain subjects. Section 34AAA is not intended to authorise the detention of persons where ASIO does not otherwise have any lawful basis to detain the person. The Department does not consider the current effect of section 34AAA when exercised would amount to arbitrary detention.

16. Recommendation 24: INSLM Act

76. The Monitor recommends that the *Independent National Security Legislation Monitor Act 2010* be amended to allow the Monitor to perform future own-motion reviews of the amendments made by the Assistance and Access Act. The Attorney-General's portfolio administers the legislation relevant to this recommendation.

17. Recommendations 25 – 33: Oversight

17.1 Recommendation 25: Record and report industry assistance orders

77. The Monitor recommends that the number of industry assistance orders executed be recorded and provided to the head of the proposed new division of the AAT annually. Please refer to the responses to recommendations 3, 4 and 5 above.

17.2 Recommendation 26: Additional reporting to oversight bodies

78. The Monitor recommends that relevant agencies be required to report to their oversight bodies as to the number of industry assistance orders they have executed in that year and that (other than for ASIO) those figures be published in the annual reports of those agencies and oversight bodies.

17.2.1 Industry assistance under Part 15 Telecommunications Act

79. Law enforcement agencies are already required to publicly report on the use of industry assistance powers. This information is included in annual reports under the Telecommunications (Interception and Access) Act, which are tabled in Parliament and published on the Department's website. The Commonwealth Ombudsman may separately publish statistics in its annual report of the use of

industry assistance powers which it obtains from inspections and notifications received from the agencies it oversees. Law enforcement agencies are required to notify the Commonwealth Ombudsman when they give, vary or revoke a technical assistance request or technical assistance notice. If the Attorney-General gives, varies or revokes a technical capability notice on behalf of a law enforcement agency, they must notify the Commonwealth Ombudsman.

80. Subsection 94(2BA) of the ASIO Act requires ASIO to report to the Minister for Home Affairs on ASIO's use of the industry assistance framework as part of annual reporting. Under sections 42 and 42A of the *Intelligence Services Act 2001*, the Australian Secret Intelligence Service and the Australian Signals Directorate are required to report to the responsible Minister of the activities of those agencies each year. This information is not publicly provided to protect capability and methodology. The Inspector-General of Intelligence and Security also has the authority to review this information as part of general inspections of the powers.

81. Under Part 15 of the Telecommunications Act, ASIO must notify the Inspector-General of Intelligence and Security if it gives, varies or revokes a technical assistance request or technical assistance notice. If the Attorney-General gives a technical capability notice on behalf of ASIO, they must notify the Inspector-General of Intelligence and Security. The Australian Signals Directorate and Australian Secret Intelligence Service must notify the Inspector-General of Intelligence and Security if they give, vary or revoke a technical assistance request.

82. The Monitor also recommends that statistics on the use of industry assistance powers, including a description of the acts or things implemented, be published annually by the proposed Investigatory Powers Commissioner. Please refer to the responses to recommendation 3, 4 and 5 above.

17.2.2 Assistance orders under 3LA Crimes Act and 201A Customs Act

83. The Australian Federal Police and the Australian Border Force are not currently required to record or report their use of assistance orders made under section 3LA of the Crimes Act and section 201A of the Customs Act respectively.

84. As a matter of practice, the Australian Border Force records assistance orders executed under section 201A of the Customs Act.

85. Including a requirement to record section 3LA orders as executed may have an impact on the Australian Federal Police's investigative resourcing.

17.2.3 ASIO voluntary assistance power and assistance orders

86. ASIO is required to report its use of powers under paragraph 21A(1)(a), subsection 34AAA(2) and subsection 94(2BC) of the ASIO Act to the Minister for Home Affairs. The Inspector-General of Intelligence and Security also has the authority to review this information as part of general inspections.

17.3 Recommendation 27: Reporting on use of section 313

87. The Monitor recommends that agencies' use of section 313 Telecommunications Act be reported to the proposed new division of the AAT annually.

88. Section 313, and the Telecommunications Act overall, is administered by the Department of Infrastructure, Transport, Regional Development and Communications.

17.4 Recommendation 28: Joint oversight investigations

89. The Monitor recommends that the Commonwealth Ombudsman, the Ombudsman of any State, and Independent Commissions Against Corruption be enabled by express amendment to undertake joint investigations of the use of industry assistance powers. This is consistent with previous government amendments to provide for State and Territory inspecting agencies to perform oversight of the use of the industry assistance framework.

17.5 Recommendation 29: Redaction of Ombudsman reports

90. The Monitor recommends the removal of the Minister's ability to redact reports of the Commonwealth Ombudsman which contain information that could reasonably be expected to prejudice an investigation or prosecution, or compromise an agency's operational activities or methodologies. As the Department previously advised in its submission to this review in July 2019, a suitable alternative could be conditional vetting between the Ombudsman and agencies prior to the publication of these reports.

17.6 Recommendation 30: Disclosure of information in the national or public interest

91. The Monitor recommends that the non-disclosure provisions which govern the industry assistance framework be amended to allow Commonwealth, State, or Territory officials to disclose information when it is in the national or public interest:

> One of the major issues I encountered with public engagement in this review was the prohibition on public disclosure or discussion of the [industry assistance powers] information, outlined in Division 6 of [Part 15 of the Telecommunications Act]. While my coercive powers enabled confidential discussion of this information, I consider that the prohibitions on disclosure are overly restrictive and undermine public confidence in the use of the provisions. They even limit what I can state in this public report. Additionally, the prohibitions on disclosure extend to Commonwealth officials acting in an official capacity. This could mean that agencies are prohibited from sharing information relevant to cyber or national security with partners simply because that information falls under the broad description of [the industry assistance powers] information.[9]

92. Reviewing, and where possible relaxing, the non-disclosure provisions governing the industry assistance framework for the reasons given by the Monitor may assist with public discussion of the Assistance and Access Act amendments.

17.7 Recommendation 31: Disclosures to obtain technical advice

93. The Monitor recommends that the industry assistance non-disclosure provisions be amended to allow designated communications providers who are given a request or notice to be able to disclose information when seeking independent technical advice. The policy intention under the current legislation is for designated communications providers to be able to disclose information required to seek independent technical advice, for example, under the general administration exception provided by paragraph 317ZF(3)(a) of the Telecommunications Act or seeking authorisation from an agency to make a conditional disclosure under subsections 317ZF(14)-(16).

94. Providing a separate channel to make disclosures for this purpose may provide some benefit. However, any potential exception would need to be carefully drafted to ensure it does not allow sensitive operational or capability information to be disclosed.

95. In addition to the technical advice issue raised by the Monitor, the Department is giving consideration to the following issues related to the disclosure provisions.

17.7.1 Inconsistency in disclosure provisions

96. Section 317ZF provides exceptions to the prohibition against disclosure of information in the industry assistance framework. However, these exceptions do not allow for certain information to be disclosed to other relevant agencies. In particular, there may be inconsistency between:

    (a) the offence for *information obtained in accordance with a technical assistance request, technical assistance notice, and technical capability notice*, and

    (b) the authorised disclosures in subsections 317ZF(3) and (5)-(16) more generally, which only relate to technical assistance request, technical assistance notice, and technical capability notice information, and not information *obtained in accordance with* a technical assistance request, technical assistance notice, and technical capability notice

[9] Above n 2, page 232.

and this may cause difficulties for agencies and other users of the industry assistance framework.

97. The intention of the disclosure provisions is to ensure law enforcement and security agencies are able to cooperate, and work efficiently and consistently with designated communications providers.

17.7.2 Pathway for providers to communicate between agencies

98. Currently, where two agencies approach a provider seeking the same or similar assistance, secrecy provisions prevent the provider from discussing the separate approaches with both agencies. This creates inefficiency on both sides, as providers are required to duplicate their efforts and agencies must seek new assistance work where this work is already being undertaken on behalf of another agency.

99. The Department has consistently heard from industry members that they would benefit from a provision permitting them to notify an agency which has sought similar assistance. Similarly, agencies would benefit from a clear legislative pathway to coordinate and seek assistance by jointly giving an industry assistance request or notice to a provider.

17.7.3 Conditional disclosure inconsistency

100. The industry assistance framework's secrecy provisions provide exceptions, at subsections 317ZF(14) – (17), to the disclosure offence for industry members to make conditional disclosures of additional types of information with the approval of the chief officer of the agency which gave a relevant technical assistance notice or technical capability notice. However, these exceptions do not provide a pathway for industry members who have been given a technical assistance request to make a similar conditional disclosure. This is inconsistent with the policy intention of this provision.

17.8 Recommendation 32: Assistance orders not executed

101. The Monitor recommends that assistance orders issued to Commonwealth law enforcement under the Crimes Act or the Australian Border Force under the Customs Act "be confined to an obligation to report on the number of assistance orders *executed* each year and should not extend to the number of *applications made* to a magistrate or other issuing authority…"[10]

102. A requirement to record statistics relating to executed assistance orders may impact the investigative resources of the Australian Federal Police.

17.9 Recommendation 33: ASIO annual reporting

103. The Department notes that ASIO is already required to record the number of requests made under subsection 21A(1) and orders made under section 34AAA of the ASIO Act as part of its annual reporting requirements. This is consistent with reporting requirements for other ASIO powers and similar assistance powers available to law enforcement.

[10] Above n 2, page 232.