Australian Government
Australian Security Intelligence Organisation

ASIO 70TH 1949 2019

ASIO submission to the Independent National Security Legislation Monitor

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

16 September 2019

Introduction

1. The Australian Security Intelligence Organisation (ASIO) welcomes the opportunity to provide a submission to the Independent National Security Legislation Monitor's Review of the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (the Act).

2. The contemporary digital landscape is characterised by increasing complexity, the ubiquitous use of encryption, and a rapid expansion in new methods of communication and communication providers. This environment has increasingly challenged the ability of ASIO to fulfill its functions under existing legislation. The new mechanisms provided under the Act allow ASIO to maintain a level of parity with respect to its operational effectiveness within this context.

3. Over 95 per cent of ASIO's most dangerous counter terrorism targets use encrypted communications. It is estimated that by 2020 all electronic communications of investigative value will be encrypted. There is no evidence that this trend will be reversed into the future. In this environment ASIO's ability to access data of security relevance has been increasingly frustrated by the same encryption that benefits society more broadly. Within this context ASIO will increasingly need to call upon the assistance of communications providers to gain access to data, and to do this in a cooperative way that does not weaken the protections that encryption offers to the benefit of all Australians.

4. Historically, ASIO has sought the technical assistance of communications providers to effectively and efficiently fulfil its functions. In recent years, the ecosystem of companies that provide communications within Australia has been disrupted by new technology, creating a heterogeneous, complex, and interdependent landscape composed of both new and existing entities. This fundamental shift in the way that communications take place has increasingly created ambiguity around the way in which ASIO should best seek assistance, and particularly assistance from non-traditional communications providers. Schedule 1 of the Act addresses this issue by providing a contemporary framework for cooperation that supports engagement with all communications providers whilst also legislating an explicit prohibition on any introduction of systemic weaknesses into the systems they support.

5. Where an appropriate legal instrument exists, the measures contained in Schedule 5 of the Act allow ASIO to compel assistance in accessing data stored in a digital format. This power is important in preventing those who threaten Australia's security from hiding their activities behind warrant-proof encryption. Schedule 5 also provides a legal framework to facilitate ASIO's access to voluntary assistance where available.

6. Computer access plays a key role in ASIO performing its intelligence collecting functions when investigating matters of relevance to Australia's security. The nature of this access continually evolves with changes in relevant technology and does not conform to one single model of operation. To best enable ASIO to perform its computer access functions within the contemporary technical environment Schedule 2 of the Act has effectively updated ASIO's powers to keep pace with technology.

7. ASIO considers the mechanisms provided by the Act are proportionate to the significant ongoing security threats faced by Australia. They allow the Organisation to exercise its investigative functions in the context of the modern digital landscape. Importantly, ASIO must conduct its activities in accordance with the Attorney-General's Guidelines (Guidelines), which are available online at *www.asio.gov.au*. The Guidelines stipulate that ASIO must conduct its activities in a lawful, timely and efficient manner, while applying the principle of proportionality—that is, the methods used to investigate a person must be proportional to the threat posed—to ensure the least intrusion necessary into an individual's privacy.

8. The Act contains significant safeguards to ensure that the rights of individuals are protected. In ASIO's view the public should hold a high level of assurance that their rights remain protected by the measures within the Act. To better explain these protections, an examination of the safeguards in place for each of the powers is outlined in this submission.

9. The trajectory of modern technology suggests that the complexities that ASIO will face into the foreseeable future will continue to necessitate access to the mechanisms provided under the Act and the operational efficiencies that they afford.

10. ASIO continues to work collaboratively with the Department of Home Affairs, our partner agencies, industry partners and the Inspector-General of Intelligence and Security (IGIS) on the implementation of the Act. We are grateful for the ongoing cooperation and assistance they have provided.

11. For each power provided to ASIO under the Act, the submission addresses whether it:

    I. contains appropriate safeguards for protecting the rights of individuals, and

    II. remains proportionate to any threat of terrorism or threat to national security, or both; and

    III. remains necessary.

Role of the Australian Security Intelligence Organisation

12. ASIO is Australia's national security intelligence service. As the nation's security service, our purpose is to protect Australia from violent, clandestine and deceptive efforts to harm its people and undermine its sovereignty.

13. ASIO's work is anticipatory in nature. We seek to identify, investigate and assess potential security threats and work with domestic and international security partners to prevent harm from occurring.

14. We deliver our purpose by focusing our efforts on three services – Counter, Shape and Build. We counter – through identification and mitigation - violent, clandestine or deceptive efforts to harm Australians and compromise Australian sovereignty, economic well-being and national security. We shape and inform efforts to foster institutional and community resilience, by providing Australian governments, law enforcement and industry with intelligence and advice to enable better decision-making in relation to security responses, policies and priorities. And we build capability across Australia's national security community by sharing our experience with partners, and leading the development of intelligence capabilities.

15. ASIO's key strategic priorities are:

- countering terrorism and the promotion of communal violence;
- countering espionage, foreign interference and malicious insiders;
- countering serious threats to Australia's border integrity; and
- providing protective security advice to government and industry.

16. We harness our expertise in security, unique intelligence collection capabilities, strong national and international partnerships and all-source intelligence analysis capabilities to provide trusted, actionable advice.

17. ASIO's role and functions are determined by law. ASIO must act lawfully, in line with the provisions of the *Australian Security Intelligence Organisation Act 1979* (ASIO Act) and other relevant legislation and guidance. ASIO must also act with propriety: our activities must be conducted effectively, efficiently, ethically and without bias.

18. ASIO is accountable to the Minister for Home Affairs, who exercises all powers and functions under the ASIO Act except those that are exercised by the Attorney-General. The Attorney-General is responsible for integrity and oversight and exercises the powers to issue ASIO warrants and authorise special intelligence operations. ASIO is also subject to parliamentary and independent oversight and scrutiny. These separate layers of accountability provide assurance that ASIO acts independently and lawfully and properly discharges its functions.

The security environment

Terrorism in Australia

19. The national terrorism threat level for Australia remains PROBABLE—credible intelligence, assessed by security agencies, indicates that individuals or groups continue to possess the intent and capability to conduct a terrorist attack in Australia. Since September 2014, when the national terrorism threat level was raised, there have been seven attacks against people and 16 major counter-terrorism disruption operations in response to potential attack planning in Australia

20. ASIO assesses that the principal source of the terrorist threat remains Sunni Islamist extremism, emanating primarily from small groups and individuals inspired, directed or encouraged by extremist groups overseas. However, individuals motivated by other forms of extremism and ideology are also present onshore.

Espionage and foreign interference

21. Foreign interference is an enduring and increasingly complex feature of the security landscape in Australia. ASIO investigations have identified foreign interference operations directed at decision-makers in government and industry, the media, members of diaspora communities and commercial investment decision-makers.

22. ASIO assesses that the current scale of foreign intelligence activity against Australian interests is unprecedented.

Operationalisation

23. The operationalisation of the Act has been underway since late December 2018, and hence our experience with the new mechanisms it provides is still relatively limited. During this time, ASIO has commenced updating, and will continue to update, our processes and systems to support the operation of the Act and reflect the outcomes of ongoing engagement with the Department of Home Affairs and the Office of the Inspector-General of Intelligence and Security (IGIS).

24. The Act has introduced an extensive accountability framework which applies to the exercise of new powers under the Act. Additional reporting and notification requirements have been introduced to ensure the exercise of powers is appropriate, proportional and necessary. Any assistance requested or compelled must relate to the performance of ASIO's functions under the ASIO Act or the exercise of ASIO's powers under relevant legislation.

25. ASIO also notes that nothing in the Act displaces the need for a warrant – any activity ASIO wishes to undertake which would otherwise have required a warrant prior to the passage of the Act, still requires a warrant today. In addition, the Act has introduced additional and specific reporting requirements to the IGIS which ASIO must adhere to.

26. The IGIS monitors ASIO's compliance with legislation, the Attorney-General's Guidelines and ASIO's own internal policies and procedures, fulfilling both an inspection and an inquiry role. The IGIS has broad-ranging investigative powers including unfettered access to review the activities of ASIO in relation to the lawfulness and the propriety of ASIO's activities. As an independent statutory office holder, the IGIS is not subject to general direction from the Prime Minister, Attorney-General or other ministers on how responsibilities under the IGIS Act should be carried out.

27. The accountability mechanisms introduced by the Act add to the existing robust oversight framework which applies to ASIO, ensuring ASIO's use of the powers afforded to it in legislation are appropriate, lawful, and conducted with propriety.

Schedule 1 of the Act

28. Schedule 1 of the Act amended the *Telecommunications Act 1997* (Telco Act) and introduced the following new powers: Technical Assistance Requests (TARs – by section 317G), which ASIO, ASIS, ASD and interception agencies can use; and Technical Assistant Notices (TANs - by section 317L) and Technical Capability Notices (TCNs - by section 317T), which ASIO and interception agencies can use.

Safeguards for TARs, TANs and TCNs

29. TARs, TANs, and TCNs have no effect to the extent (if any) that they would request or require a Designated Communications Provider (DCP) to do an act or thing for which the agency or its officers would be required to have or obtain a warrant or authorisation under a law of the Commonwealth, or a law of a State or Territory (section 317ZH *Telecommunications Act 1997* (Telco Act).

30. A request made under a TAR to do one or more specified acts or things (section 317E Telco Act), must be in connection with an eligible activity of a DCP, and must be for the purpose of ensuring a DCP is capable of giving help to ASIO in the performance of its functions, including the relevant objective of safeguarding national security. These requirements also apply to TANs and TCNs, with some differences (e.g. for TCNs, the specified acts or things must be capable of giving "listed help", which is defined in section 317T(4) Telco Act).

31. Section 317JAA of the Telco Act sets out the decision-making criteria for the giving of a TAR and provides that the Director-General must not give a TAR to a DCP unless satisfied that the request is reasonable and proportionate, and compliance with the request is practicable and technically feasible. In considering whether a TAR is reasonable and proportionate, the Director-General must, in addition to other matters, have regard to specified matters under section 317JC Telco Act including:

    - whether the request, when compared to other forms of industry assistance known to the Director-General is the least intrusive form of industry assistance so far as persons whose activities are not of interest to ASIO are concerned;
    - whether the request is necessary;
    - the legitimate expectations of the Australian community relating to privacy and cybersecurity; and
    - such other matters as the Director-General considers relevant.

    The Director-General must also have regard to these matters when issuing a TAN (section 317RA Telco Act), and the Attorney-General must have regard to these matters when giving a TCN (section 317ZAA Telco Act).

32. Further safeguards for the exercise of Schedule 1 powers include – for TARs, the DCP must be advised, orally or in writing, that compliance with the request is voluntary (section 317HAA(1) Telco Act). In relation to TANs, the DCP must be given advice relating to the DCP's obligations under whichever of sections 317ZA or 317ZB of the Telco Act are applicable, and the DCP must also be advised of their right to make a complaint about the notice to the IGIS (section 317MAA(3) Telco Act). Similar obligations apply in relation to ensuring that a DCP who has been given a TCN by the Attorney-General is advised of their obligations under the applicable section 317ZA or 317ZB (section 317TAA(1) Telco Act).

33. Before giving a TAN to a DCP, the Director-General must consult the DCP, unless the chief officer is satisfied the TAN should be given as a matter of urgency, or the DCP waives the requirement for consultation. Relatedly, a TAN (section 317MA(1C) Telco Act) or TCN (section 317TA(1C)) may not be extended without the agreement of the DCP.

34. TCNs have further safeguards including that:

- *Attorney-General must obtain Ministerial approval*: the Attorney-General must not give a TCN to a DCP unless the Attorney-General has given the Minister a written notice setting out a proposal to give the TCN and the Minister has approved the giving of the TCN (section 317TAAA(1) Telco Act). In considering whether to approve the TCN, the Minister must have regard to certain matters (section 317TAA(6) Telco Act) including the objectives of the TCN, the legitimate interests of the relevant DCP, the impact of the TCN on the efficiency and international competitiveness of the Australian telecommunications industry, and any representation that was made by the Attorney-General about the proposal to give the TCN (section 317TAAA(4) Telco Act), which may deal with whether the requirements imposed by the TCN are reasonable and proportionate.
- *Consultation with DCP:* Before giving a TCN, the Attorney-General must give the DCP a written consultation notice setting out a proposal to give the TCN and inviting the provider to make a submission on the proposed TCN, and the Attorney-General must consider any such submission received within the time limit specified on the consultation notice (a time limit specified in a consultation notice must run for at least 28 days unless urgent or impracticable or the DCP waives compliance with the requirement for a 28 day consultation notice period) (section 317W Telco Act).
- *Ability to request assessment:* A DCP who receives a consultation notice may also request an assessment by two assessors (one a security cleared technical expert and one a retired judge) of whether the proposed TCN should be given. The Attorney-General must have regard to the report provided by the assessors in considering whether to proceed to give the TCN (section 317WA Telco Act).

Prohibition on systemic weakness or vulnerability

35. A critically important safeguard that has been explicitly included within the legislation is that TANs and TCNs must not request a DCP to implement or build a systemic weakness or vulnerability into a form of electronic protection or prevent a DCP from rectifying a systemic weakness, or a systemic vulnerability, in a form of electronic protection ('systemic weakness' and 'systemic vulnerability' are defined in section 317B Telco Act).

Notification to the IGIS

36. The Director-General or Attorney-General must notify the IGIS of the revocation of a TAR, TAN, or TCN within seven days of the revocation. The IGIS must also be notified within seven days of the extension of a TAN or TCN.

37. These reporting requirements act as an additional and important safeguard ensuring that the IGIS has oversight of the exercise of all of ASIO's Schedule 1 powers.

Annual Report

38. A further safeguard is the requirement for ASIO to record in its annual report a statement confirming the number of times the total number of TARs and TANs given by the Director-General, and the total number of TCNs given by the Attorney-General during the relevant period section 94(2BA) ASIO Act).

39. ASIO considers that these legislated requirements function as effective safeguards for protecting the rights of individuals.

Proportionality

40. ASIO must conduct its activities in accordance with the Guidelines, which stipulate that ASIO must conduct its activities in a lawful, timely and efficient manner, while applying the principle of proportionality—that is, the methods used to investigate a person must be proportional to the threat posed— to ensure the least intrusion necessary into an individual's privacy.

41. The principle of proportionality is incorporated and embedded within all of ASIO's work and practices, including in relation to the exercise of any powers under the Act. ASIO also notes that the requirement to ensure the exercise of Schedule 1 powers is proportionate is explicitly required by the legislation in relation to TARs (section 317JAA (1) Telco Act), TANs (section 317P Telco Act) and TCNs (section 317V Telco Act).

Engagement with Direct Communications Providers (DCPs)

42. In addition, as set out above, the Director-General must not give a TAR to a DCP unless satisfied that the request is reasonable and proportionate, which also includes having regard to the interests of national security and law enforcement, and whether the request is necessary. A TAR may be given (section 317H(2) Telco Act) or varied (section 317JA(6) Telco Act) orally if: an imminent risk of serious harm to a person or substantial damage to property exists, the TAR or variation is necessary for the purpose of dealing with that risk, and it is not practicable in the circumstances to give or make the TAR or variation in writing. TANs may also be given or varied orally if the circumstances described above for TARs are met (sections 317M and 317Q Telco Act). This ability would allow ASIO to request or require assistance where a threat of terrorism or threat to national security might require cooperation in very short timeframes.

43. The fact that TARs, TANs, and TCNs must be in relation to listed acts or things (section 317E Telco Act), which broadly relate to providing assistance to give effect to warrants to facilitate access to services and devices, ensures the powers can only be used for specific and limited purposes. As a result this has the implicit effect of ensuring the powers are constrained and that their use is proportionate. ASIO also notes that the Act imposes an obligation on the Director-General to revoke a TAR (section 317JB(2A) Telco Act), TAN (section 317R(2) Telco Act), and for the Attorney-General a TCN (section 317Z(2) Telco Act), if satisfied that the request or notice is not reasonable and proportionate.

Industry guidance

44. ASIO considers that the explicit requirements introduced by the Act in addition to ASIO's normal practice of having due regard to proportionality in the performance of its functions ensure Schedule 1 powers remain proportionate to any threat of terrorism or threat to national security.

Necessity

45. Legislation that supports ASIO's ability to meaningfully engage with Australia's communications providers will remain essential to ASIO fulfilling its function of investigating matters of relevance to security. Schedule 1 of the Act provides a vehicle to allow this engagement with both traditional and non-traditional communications providers to be undertaken, while balancing the interests of ASIO, the DCPs and the Australian public.

46. The importance of ASIO working cooperatively with DCPs has grown significantly with the advent of ubiquitous encryption. Within this context ASIO will increasingly need to call upon the assistance of DCPs to gain access to data, and to do this in a cooperative way that does not weaken the protections that encryption offers to the benefit of all Australians.

Schedule 2 of the Act

47. Schedule 2 of the Act amended Part III of the ASIO Act and provided ASIO with additional powers under its existing computer access warrant regime (primarily section 25A of the ASIO Act, but also under sections 27A (Foreign intelligence collection warrants) and 27E (Identified Person Warrants) of the ASIO Act).

48. Broadly, the new powers enable ASIO to: alter data in a computer or communication in transit, intercept a communication passing over a telecommunications system, and the ability to temporarily remove a computer or thing from premises (and concealing such a fact if required).

Safeguards

49. All ASIO warrants are issued by the Attorney-General (except questioning and questioning and detention warrants, which are issued by an Issuing Authority).

50. The amendments made by Schedule 2 of the Act maintain the existing and appropriate safeguards for protecting the rights of individuals. For example, section 25A computer access warrants are only to be issued by the Attorney-General if he or she is satisfied that there are reasonable grounds for believing that access to data held in a computer (the *target computer*) will substantially assist the collection of intelligence in accordance with the ASIO Act in respect of a matter that is important in relation to security. Such a warrant must meet the relevant legislative requirements and thresholds which ensure that the computer access is targeted toward specified things and is appropriate in the circumstances.

51. The new powers which permit the removal of a computer or thing for the purpose of concealing the fact that anything has been done under the warrant or the interception of a communication (sections 25A(8), 27A(3C) ASIO Act), are part of the things that may be specified in the warrant and that the Attorney-General considers appropriate in the circumstances. Similarly, the Attorney-General or Director-General is only to give an authorisation to use the new powers under an identified person warrant if satisfied, on reasonable grounds that doing those things under the warrant would substantially assist the collection of intelligence relevant to the prejudicial activities of the identified person (section 27E(4) ASIO Act). The new powers may only be exercised for the purpose of doing anything specified in the warrant (or authorisation under an identified person warrant) in relation to the *target computer*, and are subject to any restrictions or conditions specified in the warrant.

52. The Act also included specific prohibitions in relation to each new power under Schedule 2, specifying that the relevant subsections do not authorise the doing of a thing that is likely to materially interfere with a communication in transit, or the lawful use by other persons of a computer (unless necessary to do one or more of the specified things), or cause any other material loss or damage to other persons lawfully using a computer. In addition, if a computer or another thing is removed under a power, it must be returned when no longer prejudicial to security, or within a reasonable period. Anything done to conceal the fact that anything has been done under the warrant must be undertaken either while the warrant is in force, within 28 days after it ceases to be in force, or at the earliest time after that 28-day period at which it is reasonably practicable to do so.

53. Schedule 2 of the Act also made amendments to subsection 24(4) of the ASIO Act, to make clear that the new provisions under section 25A, section 27A and section 27E are within the definition of 'relevant device recovery provisions' for the purposes of section 24. This provides a safeguard against the arbitrary exercise of the range of activities permitted by the new provisions (concealment of activities, concealment of access, temporary removal of a computer or other things) by requiring the person or class of persons exercising these powers to be approved by the Director-General personally.

Warrant reporting

54. For each warrant issued by the Attorney-General, the Director-General is required to provide to the Attorney-General a written report on the extent to which action taken under the warrant has assisted ASIO in carrying out its functions. Additionally, if ASIO uses the new powers under sections 25A(4) or (8), 27A(3C), or 27E(2) or (6) (for example, the power to temporarily remove a computer or thing for the purpose of concealing the fact that anything has been done under the warrant) the Act requires the warrant report to include details of anything done that materially interfered with, interrupted or obstructed the lawful use by other persons of a computer or other electronic equipment, or a data storage device.

55. If, as at the end of a prescribed post-cessation period of a warrant (the three-month period beginning immediately after the warrant ceased to be in force, and each subsequent three-month period) it is likely that a post-cessation concealment activity will be done in connection with the warrant the Director-General must give the Attorney-General a written report on the extent to which the activity will assist ASIO in carrying out its functions.

IGIS inspection of warrants

56. The IGIS conducts regular inspections of ASIO warrants, on a sampling basis, and performs regular inspections of ASIO activities as part of its oversight function. The IGIS may also conduct detailed inquiries.

57. The IGIS is also able to consider any complaints received from persons affected by, or otherwise involved in, the exercise of ASIO's powers.

Proportionality

58. The warrant powers introduced under Schedule 2 of the Act assist ASIO in the performance of its functions, but remain proportionate.

59. The existing legal framework for the issuing of ASIO warrants provides robust assurance, accountability and oversight mechanisms. As noted above, every ASIO warrant must meet strict legal thresholds and requirements and (aside from questioning and questioning and detention warrants) must be issued by the Attorney-General.

60. Noting that some new powers have been introduced to enhance the operational effectiveness of ASIO's computer access warrants, this necessarily makes those new powers subject to the same strict and rigorous accountability and oversight framework that applies to all of ASIO's warranted activities. The removal of a computer or thing (for concealing the fact that anything has been done under the warrant) is an intrusive measure, but the power is limited to specific purposes, and by a requirement to return the computer or thing once the purpose has been achieved. The Act constrains the purposes for which ASIO may use information intercepted under these new powers, consistent with Parliament's intention for intercept warrants to be subject to high thresholds.

Necessity

61. Methods of computer access must evolve to match changes in both the target technology and the operational environment, and do not conform to one single model of operation. ASIO considers that the new powers in Schedule 2 of the Act provide an update to ASIO's computer access warrant regime necessary to keep pace with technology.

62. The new mechanisms provided under Schedule 2, have enhanced the operational effectiveness of ASIO's computer access warrant regime within the current technical context. There is no reason to anticipate a change in the nature of our operations such that these mechanisms will not continue to provide significant benefit into the future.

Schedule 5 of the Act

Safeguards

63. Schedule 5 of the Act amended Part III of the ASIO Act, providing ASIO with the power to request persons or bodies to engage in conduct to assist ASIO in the performance of its functions, and receive civil immunity for those actions, provided specific conditions are met (section 21A ASIO Act), and a power to request the Attorney-General to make an order requiring a specified person provide assistance in relation to data held in a computer or data storage device (section 34AAA ASIO Act).

Section 21A

64. Section 21A enables ASIO to request a person or body engage in conduct where the Director-General is satisfied, on reasonable grounds, that the conduct is likely to assist ASIO in the performance of its functions. ASIO can request assistance but has no powers of compulsion. Any person or body who receives a request from ASIO under section 21A can choose not to comply.

65. ASIO notes that provided the criteria set out in section 21A is met, a person or body will not be subject to any civil liability for, or in relation to conduct they engage in that is likely to assist ASIO in the performance of its functions. This conferral of civil immunity provides individuals or bodies with assurance that they have legal protection for the activities they undertake to assist ASIO.

66. Importantly, a request can only be made under section 21A where the Director-General is satisfied on reasonable grounds that the conduct is likely to assist ASIO in the performance of its functions, and the conduct does not involve a person/body committing an offence against a law of the Commonwealth or a State or Territory, and the conduct does not result in significant loss of, or serious damage to property. Accordingly, the type of assistance that can be provided under section 21A is necessarily limited and subject to clear and important constraints.

67. Furthermore, the conferral of civil immunity can only apply where the person engages in conduct in accordance with the request.

68. In the event that a person's rights are affected such that the 21A request would result in an acquisition of property otherwise than on just terms then the legislation explicitly provides that the Commonwealth is liable to pay a reasonable amount of compensation to the person (section 21A(10) ASIO Act). Where a reasonable amount cannot be agreed then the person has the right to institute proceedings in the Federal Court of Australia (section 21A(11) ASIO Act).

Annual Report

69. ASIO is required to include a statement in its annual report of the total number of requests made under section 21A (section 94(2BC) ASIO Act).

Notification to IGIS

70. As a further safeguard in relation to the use of section 21A requests, ASIO is obliged to notify the IGIS within seven days of making a request for assistance under section 21A of the ASIO Act. This acts as an important safeguard and ensures each and every use of this power is subject to oversight by the IGIS (section 21A(3A) ASIO Act).

Section 34AAA

71. A section 34AAA order allows the Director-General to request the Attorney-General to make an order requiring a person to provide information or assistance to ASIO that is reasonable and necessary to allow ASIO to access, copy or convert data held in computers or data storage devices. As such, this means a section 34AAA order can only apply to a computer or data storage device already accessible to ASIO pursuant to a warrant or authorisation.

72. Section 34AAA of the ASIO Act also contains appropriate safeguards for protecting the rights of individuals. The Director-General can only request that the Attorney-General make a section 34AAA order requiring a person to provide any information or assistance which is reasonable and necessary to allow ASIO to do a limited list of things specified in section 34AAA(1).

73. A section 34AAA order can only be made by the Attorney-General if the Attorney-General is satisfied, that:

- there are reasonable grounds for suspecting access by ASIO to data held in, or accessible from, the computer or data storage device will substantially assist the collection of intelligence in accordance with the ASIO Act in respect of a matter that is important in relation to security (section 34AAA(2)(b));
- the specified person is reasonably suspected of being involved in activities that are prejudicial to security, or meets other conditions set out in section 34AAA(2)(c); and
- the specified person has relevant knowledge of certain technical matters set out in section 34AAA(2)(d).

Some differences apply to foreign intelligence collection warrants under section 27A of the ASIO Act (section 34AAA(2)(a)).

74. Any request to the Attorney-General by the Director-General seeking a section 34AAA order must be accompanied by a statement setting out the particulars and outcomes of all previous requests (if any) relating to the person specified in the current request (section 34AAA(3C) ASIO Act). This acts as an additional safeguard.

75. Section 34AAA also includes a requirement that where the Director-General is satisfied that the grounds on which an order is made cease to exist, then the Director-General must inform the Attorney-General, as soon as practicable, that the grounds cease to exist. The Attorney-General must revoke an order if satisfied that the grounds on which the order was made have ceased to exist (section 34AAA(3D)-(3E) ASIO Act).

76. If an order is made under section 34AAA, the Director-General's warrant report to the Attorney-General under section 34 of the ASIO Act must also include details of the extent to which compliance with the order has assisted ASIO in carrying out its functions.

Annual Report

77. ASIO is required to include a statement in its annual report of the total number of requests made under section 34AAA (section 94(2BC) ASIO Act).

Proportionality

78. The ability to request persons or bodies assist ASIO voluntarily under section 21A provides ASIO with an additional mechanism to respond to a threat to national security. It is crucial that ASIO has the ability to rely on different options when responding to varying threats.

79. A request for assistance under section 21A may only be made orally if the Director-General is satisfied that: the request should be made as a matter of urgency, or making the request in writing would be prejudicial to security, or making the request in writing would be prejudicial to the operational security of ASIO.

80. Given section 34AAA orders can only apply to a computer or data storage device already accessible to ASIO pursuant to a warrant or authorisation, this ensures the use of this power can only be used in certain circumstances.

Necessity

81. ASIO operates in a contemporary environment that is characterised by continually evolving technology and ubiquitous encryption. Under these circumstances, ASIO will increasingly need to call upon the assistance of others in order to fulfil its functions. The new mechanisms provided under Schedule 5 of the Act allow ASIO to engage voluntary support where available, and compel assistance under circumstances where it is deemed necessary to do so.

82. Given the mechanisms provided under Schedule 5 are largely technology agnostic it is reasonable to expect that they will continue to provide an enhancement to ASIO's operational efficiency, even as technology changes.

Conclusion

83. ASIO views the Act to be an essential enabler of its ability to stay abreast of the technical developments that might otherwise render its powers ineffective. The mechanisms the Act introduced have offered significant utility to date, and ASIO continues to make operational use of these capabilities.

84. ASIO considers that the powers afforded to ASIO under the Act and where applicable, the related warrants under which the powers may be executed contain appropriate safeguards for protecting individuals' rights and are proportionate.

85. Evidence suggests that the complexities that ASIO will face into the foreseeable future will continue to necessitate access to the mechanisms provided under the Act and the operational efficiencies that they afford.

86. ASIO intends to continue to work in close collaboration with the Department of Home Affairs, partner agencies, industry partners and the IGIS on the continued implementation and refinement of the powers and mechanisms provided by the Act.