4

Australian Intelligence Community Legislation Reform

4.1 The Attorney-General's Department (AGD) discussion paper notes that the security environment in which Australia's intelligence agencies operate 'is continually evolving and becoming increasingly diversified'. This evolution and diversification in turn requires these intelligence agencies to adapt, and as such the discussion paper argues that:

> ...it is imperative that these agencies are appropriately equipped with the necessary statutory powers to uphold Australia's vital national security interests.[1]

4.2 The Attorney-General's Department and agencies within the Australian Intelligence Community have identified a number of practical difficulties with the legislation governing the operation of those agencies.

4.3 As such, the discussion paper canvasses a number of reforms to the *Australian Security Intelligence Organisation Act 1979* (ASIO Act) and the *Intelligence Services Act 2001* (IS Act). According to the discussion paper, these reforms are necessary to:

> ...maintain the intelligence gathering capabilities of the Australian intelligence agencies, ensuring they remain able to adeptly respond to emerging and enduring threats to security. Proposed reforms seek to continue the recent modernisation of security legislation to ensure the intelligence community can continue to meet the demands of government in the most effective manner.[2]

---

1 Attorney-General's Department, *Equipping Australia against emerging and evolving threats*, Discussion Paper, July 2012, p. 40.

2 Attorney-General's Department, *Equipping Australia against emerging and evolving threats*, Discussion Paper, July 2012, p. 40.

4.4 The proposed reforms fall into three broad categories:

- Matters the Government wishes to progress: changes to ASIO's warrant provisions; changes to ASIO Act employment provisions; and clarifying the authority of DIGO.
- Matters the Government is considering: amending the ASIO Act to create an authorised intelligence operations scheme; further changes to ASIO's warrant provisions; and clarifying the ability of ASIO to cooperate with private sector actors.
- Matters on which the Government seeks the views of the Parliamentary Joint Committee on Intelligence and Security (the Committee): further changes to ASIO's warrant provisions; ministerial authorisations for Australia's foreign intelligence agencies to produce intelligence on Australian citizens; and ASIS cooperation with overseas authorities on self-defence and weapons training.

Proposals the Government wishes to progress

ASIO Act – Computer access warrants

4.5 The Terms of Reference for this inquiry incorporate three separate issues relating to computer access warrants. One issue is a matter that the Government wishes to progress, a second is a matter that the Government is considering and the third is a matter that for which the Government expressly seeks the Committee's views. In this report, the three issues will be dealt with together because of their common subject matter.

4.6 Section 25A of the ASIO Act currently allows the Director-General of Security to request the Attorney-General to issue a computer access warrant. The Attorney-General may issue the warrant if satisfied that there are reasonable grounds for believing that access to data held in a particular computer will substantially assist the collection of intelligence in respect of a security matter.

4.7 Computer access warrants authorise ASIO to do things specified by the Attorney-General in relation to a particular computer, subject to any restrictions also specified by the Attorney-General.

4.8 The ASIO Act currently allows the Attorney-General to specify the entering of premises, the use of computers, telecommunications facilities, other electronic devices and data storage devices for the purpose of obtaining data that is held on the target computer and, if necessary, adding, deleting or altering other data in the target computer if it is necessary to obtain the data.

4.9 A warrant issued under section 25A empowers ASIO to copy any data that appears to be relevant to the collection of intelligence, as well as do anything that

is reasonably necessary to conceal that any action has been done under the warrant.

4.10 However, ASIO is prohibited from adding, deleting or altering other data in the target computer or doing anything that interferes with, interrupts or obstructs the lawful use of the target computer by other persons.

4.11 The Attorney-General's Department discussion paper nominates three particular changes to section 25A that would enhance its effectiveness.

References to 'computer' in section 25A

4.12 The Terms of Reference state that the Government wishes to amend the ASIO Act to update the definition of computer in section 25A. The discussion paper elaborates that the ASIO Act could be amended so that a computer access warrant may be issued in relation to a computer, computers on a particular premises, computers connected to a particular person or a computer network.[3]

4.13 Computer access warrants under section 25A of the ASIO Act are limited to obtaining data stored on '*a computer*'. A 'computer' is defined to mean 'a computer, a computer system or part of a computer system'. This means that if an individual has more than one computer which is not part of the same computer system, or data is stored on a computer network, it may be necessary for the Attorney-General to issue more than one warrant.

4.14 The discussion paper asserts that 'this is inefficient and does not increase the level of accountability around the issue of warrants'. The discussion paper further suggests that a possible solution to this issue could be to:

> …amend the ASIO Act so that a computer access warrant may be issued in relation to a computer, computers on a particular premises, computers connected to a particular person or a computer network.[4]

4.15 Mr Ian Quick identified that there may be some over-reach or ambiguity in how far removed from the target intelligence a computer could be lawfully accessed:

> Could a single warrant cover all computers at BHP headquarters? All computers at a university?[5]

4.16 Mr Quick added:

> A 'computer network' is even more worrying. How is the network defined? Everything the person could access anywhere on the internet? Everything on their 'local' (on the premises) network? Where exactly

3 Attorney-General's Department, *Equipping Australia against emerging and evolving threats*, Discussion Paper, July 2012, p. 39.

4 Attorney-General's Department, *Equipping Australia against emerging and evolving threats*, Discussion Paper, July 2012, p. 39.

5 Mr Ian Quick, *Submission No. 95*, p. 8.

> would the warrant boundaries be, given that it could be argued that the bulk of computers on the planet are on the same 'network?[6]

4.17 The Inspector-General of Intelligence and Security (IGIS) noted that:

> Computing technology and usage patterns have changed and continue to change, however the proposed response may introduce further issues. For example, the term 'computers connected to a computer network' is potentially very broad in scope. It is difficult to contemplate when it would be reasonable to access *all* computers connected to a network in the absence of further limitations. Similarly 'computers on a particular premises' could inadvertently include computers that can have no connection whatsoever with the individual of interest.[7]

4.18 Similarly, the Gilbert + Tobin Centre of Public Law argued:

> ASIO should not be able to seek a warrant to access the computers on a particular network unless there are reasonable grounds to believe that the person in relation to whom intelligence is being sought had a connection with computers other than his own on the network.[8]

4.19 The Australian Privacy Foundation argued that the ambiguity of the discussion paper meant that such changes 'may be harmless or disastrous depending on exactly what is intended'. The Australian Privacy Foundation further advised that:

> The Committee should reject outright the concept of agencies ever being permitted to perform an act that "adds, deletes or alters data or interferes with, interrupts, or obstructs the lawful use of the target computer by other persons", on the grounds that such acts pollute evidence, and enable the "framing" of suspects.[9]

Committee comment

4.20 The Committee notes the concerns that have been raised as to the authority that may be given to ASIO under the proposed changes to the computer access warrants regime. However, the Committee is of the view that giving full effect to the original intention of that warrant regime is necessary.

4.21 In an environment of rapidly evolving technology, the capability of ASIO should not be degraded by the definition of computer in the ASIO Act being obsolete. Therefore, the Committee considers that the existing definition of computer in the ASIO Act, and in particular the term "computer system", may not be sufficient to include a multiplicity of computers operating together as a network.

6 Mr Ian Quick, *Submission No. 95*, p. 8.

7 Inspector-General of Intelligence and Security, *Submission No. 185*, p. 14.

8 Gilbert + Tobin Centre of Public Law, *Submission No. 36*, p. 11.

9 Australian Privacy Foundation, *Submission No. 162*, p. 9.

In the Committee's view, computer networks should be within the definition of "computer".

4.22 The Committee understands the desire of ASIO to enable warrants to extend to all computers located on a particular premises, or connected to a particular person; however it does not consider that the issue is appropriately addressed by amending the definition of "computer" but rather by amending the warrant provisions.

Recommendation 20

The Committee recommends that the definition of computer in the *Australian Security Intelligence Organisation Act 1979* be amended by adding to the existing definition the words "and includes multiple computers operating in a network".

The Committee further recommends that the warrant provisions of the ASIO Act be amended by stipulating that a warrant authorising access to a computer may extend to all computers at a nominated location and all computers directly associated with a nominated person in relation to a security matter of interest.

Enabling the disruption of a target computer

4.23 The Terms of Reference state that the Government is considering amending the ASIO Act to modernise and streamline ASIO's warrant provisions to enable the disruption of a target computer for the purposes of a computer access warrant.

4.24 The discussion paper elaborates that subsection 25A(5) currently restricts ASIO from doing anything under a computer access warrant that adds, deletes or alters data or interferes with, interrupts, or obstructs the lawful use of the target computer by other persons. This prohibition operates regardless of how minor or inconsequential the interference, interruption or obstruction may be.

4.25 The discussion paper explains that the existing formulation of the prohibition leads to difficulties in executing computer access warrants:

> The increasingly complex nature of the global information technology environment and the use by some targets of sophisticated computer protection mechanisms can adversely impact ASIO's ability to execute a

> computer access warrant for the purpose of obtaining access to data relevant to security.[10]

4.26 The discussion paper suggests that to address those difficulties section 25A could be amended so that the prohibition does not apply to activity proportionate to what is necessary to execute the warrant.

4.27 The Law Council of Australia countered the discussion paper's assertions by highlighting the original intent of the provision that prevents ASIO from disrupting the target computer when it executes its warrant:

> Having regard to this legislative history, the Law Council questions the basis of this proposed reform in relation to sub-section 25A(5). This key provision was considered important to the community and the Parliament when it was introduced and the discussion paper does not justify its removal other than through the general statement about the global information technology environment and sophisticated computer protection mechanisms adversely impacting on ASIO's ability to execute computer access warrants.[11]

4.28 The Inspector-General of Intelligence and Security (IGIS) addressed concerns by clarifying the intent of the proposal:

> I understand that the proposal is to enable ASIO to do only what is necessary to covertly retrieve the information sought under the warrant. That is, the primary purpose of any disruption would be to avoid disclosing to the person or group under surveillance that ASIO was monitoring them. This seems to be a reasonable solution to current operational problems.[12]

4.29 The Attorney-General's Department was asked why ASIO should be allowed to disrupt a target computer if the law currently prevents such actions from being authorised. The Department expanded upon the intent of the proposal:

> This prohibition operates regardless of how minor or inconsequential the interference, interruption or obstruction may be. As this requirement is expressed in absolute terms, it can prevent ASIO from being able to execute a warrant if doing so would have even a minor or inconsequential impact, such as a temporary slowing of the computer. It could also create uncertainty if it is not possible to determine whether doing something under a computer access warrant may interfere with, interrupt or obstruct the lawful use of the computer by other persons.[13]

---

10 Attorney-General's Department, *Equipping Australia against emerging and evolving threats*, Discussion Paper, July 2012, p. 48.

11 Law Council of Australia, *Submission No. 96*, p. 66.

12 Inspector-General of Intelligence and Security, *Submission No. 185*, p. 20.

13 Attorney-General's Department, *Submission No. 236*, p. 2.

4.30 In their joint submission, the peak industry bodies the Australian Mobile Telecommunications Association and Communications Alliance expressed concern that disruption of a target computer could inadvertently lead to damage to broader telecommunications networks:

> Disruption of a target computer, or network, should be facilitated by agency mechanisms. Industry would strongly oppose any proposal for disruption mechanisms being inserted into information communications networks, communications devices, and any other publicly available applications platforms.[14]

4.31 Similarly, Telstra expressed its concern as to the involvement of telecommunications service providers:

> If such a change to legislation is contemplated, Telstra would expect that ASIO provide [service providers] with full indemnity in relation to proceedings brought by a third party in relation to this form of interception.[15]

4.32 In relation to accessing information stored in cloud computing facilities, Mr Robert Batten, submitting in a private capacity, cautioned:

> Any reform that allows interruption to service needs to be worded to be cognisant of the potentially very broad implications of such interruption, and that warrants for physical computers are becoming less relevant in the face of rapid virtualisation.[16]

Committee comment

4.33 The Committee notes the Attorney-General's Department's submission that there is a need to address difficulties that can arise in executing ASIO's computer access warrants. The Committee further notes that the ASIO Act should be amended so that the prohibition on disrupting computers does not apply to activities that would be necessary to execute the warrant.

4.34 The Committee also encourages the Government to consider including provisions in the ASIO Act that would prevent damage or cause loss to telecommunications systems operated by third parties.

4.35 The Committee agrees with the comments of the IGIS that this proposal should be framed carefully to minimise the impact on parties unrelated to the security matter:

---

14 Australian Mobile Telecommunications Association and Communications Alliance, *Submission no. 114*, p. 20.

15 Telstra, *Submission No. 189*, p. 14; see also: Mr Evan Slatyer, *Submission No. 131*, p. 1.

16 Mr Robert Batten, *Submission No. 50*, p. 10; see also Internet Society of Australia, *Submission No. 145*, p. 3.

> As this proposal could directly affect the activities of persons unrelated to security interests it would be essential to have to clearly justify the case as to why it is appropriate to affect any lawful use of the computer. The reasons would need to balance the potential consequences of this interference to the individual(s) with the threat to security.[17]

4.36 The Committee also agrees with the IGIS that there should be appropriate review and oversight mechanisms with particular attention to the effect of any disruption on third parties.

Recommendation 21

The Committee recommends that the Government give further consideration to amending the warrant provisions in the *Australian Security Intelligence Organisation Act 1979* to enable the disruption of a target computer for the purposes of executing a computer access warrant but only to the extent of a demonstrated necessity. The Committee further recommends that the Government pay particular regard to the concerns raised by the Inspector-General of Intelligence and Security.

Access via third party computers and communications

4.37 The Terms of Reference state that the Government expressly seeks the views of the Committee on amending the ASIO Act to modernise and streamline ASIO's warrant provisions by using third party computers and communications in transit to access a target computer under a computer access warrant.

4.38 As with the proposals considered above, the discussion paper attributes the increasingly difficult situation ASIO faces in executing its computer access warrants to advancements in technology. This is particularly the case where a target is security conscious and ASIO must consider 'innovative methods' to access the target computer:

> In the same way that access to a third party premises may be necessary to execute a search warrant, it may be necessary to use a communication that is in transit or use a third party computer for the purpose of executing a computer access warrant.[18]

4.39 The discussion paper proposes:

17 Inspector-General of Intelligence and Security, *Submission No. 185*, p. 20.

18 Attorney-General's Department, *Equipping Australia against emerging and evolving threats*, Discussion Paper, July 2012, p. 50.

> To overcome this problem, it may be appropriate to amend the ASIO Act to enable a third party computer or communication in transit to be used by ASIO to lawfully access a target computer. Noting that using a communication in transit or a third party computer may have privacy implications, appropriate safeguards and accountability mechanisms would need to be incorporated into such a scheme.[19]

4.40 The description of the proposal and the lack of reference to what a legislative framework for third party access might entail drew criticism:

> There is no reference to proportionality tests applicable or the need to balance any national security benefit against the cost to individual privacy.[20]

4.41 There was also criticism of the very nature of accessing the computers of people who are not directly national security targets:

> In my view, this proposal is completely unjustified. To access a third party's computer which has no connection with the target is extraordinarily broad and intrusive. These are powers usually characteristic of a police state. Adversely impacting the privacy of an individual (the third party) should only be permitted in the most extreme circumstances as a "last resort" when all other methods have been exhausted. Furthermore, the power to alter (rather than "access") a third party computer should not be permitted.
>
> Even with such safeguards and accountability mechanisms (which are not detailed in the discussion paper), I cannot support a measure that could severely diminish the privacy of individuals and could cause a chilling effect on the way that individuals communicate and use technology.[21]

4.42 The Acting Commissioner of the Victorian Privacy Commission elaborated on his comment for the Committee at a hearing. The Commissioner was asked whether this proposal would be acceptable if there were appropriate safeguards:

> It still severely diminishes the privacy of individuals. Certainly, it would need the safeguards and accountability mechanisms and it would need to be strongly argued that it met those tests of legitimacy, necessity and proportionality. But there is not even an attempt, in my view, in the discussion paper to do that.[22]

---

19 Attorney-General's Department, *Equipping Australia against emerging and evolving threats*, Discussion Paper, July 2012, p. 50.

20 Liberty Victoria, *Submission No. 143*, p. 3; see also: Mr Daniel Judge, *Submission No. 157*, p. 13; Ms Stella Gray, *Submission No. 152,* pp. 11-12; see also: New South Wales Young Lawyers, *Submission No. 133*, p. 8.

21 Office of the Victorian Privacy Commissioner, *Submission No. 109*, p. 6.

22 Dr Anthony Bendall, Acting Privacy Commissioner, Office of the Victorian Privacy Commissioner, *Transcript*, Melbourne, 5 September 2012.

4.43 The Attorney-General's Department was asked why ASIO should be empowered to 'hack' the computers of people who are not threats to security. The Department clarified that the proposal would not allow for surveillance of third party computers:

> The proposals would not involve hacking in the sense of authorising ASIO to examine the content of material. AGD notes the concerns raised in submissions to the Committee, for example from the Office of the Victorian Privacy Commissioner, that the proposal would allow surveillance of virtually unlimited services. However, the purpose of a warrant authorising the use of a third party computer would still be to access the computer of security interest, and the warrant would not authorise ASIO to obtain intelligence material from the third party computer or the communication in transit.[23]

4.44 The IGIS suggested an appropriate precedent within the *Telecommunications (Interception and Access) Act 1979* (TIA Act) that could be adapted in the ASIO Act to provide appropriate accountability safeguards, should the proposal be adopted:

> Any such change must ensure that the impact on the third party, including privacy implications as well as any impact on the security or lawful use of the third party computer are considered carefully in the approval process.
>
> Currently the TIA Act allows ASIO to obtain a warrant from the Attorney-General to intercept communications via a third party only where all other practicable methods have been exhausted or where it would not otherwise be possible to intercept the relevant communications. This appears to be an appropriate safeguard.[24]

4.45 The IGIS refers to interception warrants that are labelled 'B-Party' warrants.

4.46 The Attorney-General's Department offered further clarification of the safeguards that would limit the intrusiveness of access to third party computers and communications:

> There are a range of safeguards that already exist so that third party computers and communications in transit could only be used in limited circumstances. It is envisaged that use of third party computers and communications in transit would need to be expressly authorised by the Attorney-General when issuing a warrant. The Attorney-General's Guidelines contain requirements for ASIO to use as little intrusion into

23 Attorney-General's Department, *Submission No. 236*, p. 1.

24 Inspector-General of Intelligence and Security, *Submission No. 185*, p. 21.

> privacy as possible and for the measures used to obtain intelligence to be proportionate to the gravity of the threat (section 10.4).[25]

4.47 Mr Johann Trevaskis, submitting in a private capacity, noted additional practical questions that the Government should consider when it develops draft legislation for Parliament's consideration:

> It also raises the issue of what happens if the third party detects what is going on. The third party is unlikely to be aware of the ASIO operation. The third party may deliberately or unintentionally reveal details of it, or interfere with it. The third party, thinking his system is under attack, may actively take countermeasures. Will the third party be indemnified for any of this? If the third party becomes aware of what is going on is the third party obliged to consent to the intrusion?[26]

Committee comment

4.48 The Committee notes that there are circumstances in which it would be necessary for ASIO to access a third party computer or communication in transit for the ultimate purpose of lawfully accessing a target computer.

4.49 The Committee notes that third party access has significant privacy implications and that therefore appropriate safeguards and accountability mechanisms, such as those included in the TIA Act for 'B-Party' interception warrants, would need to be incorporated into such a scheme.

4.50 The interception of voice communications via third parties is already lawful under the TIA Act. This proposal would extend this capability under warrant to ASIO via the ASIO Act to allow it to access data through third parties. In essence, this is another case of updating the Acts to keep pace with technological developments.

Recommendation 22

The Committee recommends that the Government amend the warrant provisions of the *Australian Security Intelligence Organisation Act 1979* to allow ASIO to access third party computers and communications in transit to access a target computer under a computer access warrant, subject to appropriate safeguards and accountability mechanisms, and consistent with existing provisions under the *Telecommunications (Interception and Access) Act 1979*.

25 Attorney-General's Department, *Submission No. 236*, p. 1.

26 Mr Johann Trevaskis, *Submission No.62*, p. 11.

ASIO Act warrant proposals

4.51 The Terms of Reference and discussion paper describe three related proposals that have the potential to affect the operation of all warrant types contained in the ASIO Act. Broadly, these proposals relate to the duration, variation and renewal of ASIO warrants.

4.52 Under the ASIO Act, the Director-General of Security applies to the Attorney-General for warrants. If satisfied that all the criteria have been met and that a case has been made that special powers should be used in a particular matter, the Attorney-General may issue a warrant at their discretion.

4.53 It is important to note that those powers exercised under warrant are of an inherently intrusive nature. They include search, listening device, tracking device and computer access warrants. In the case of surveillance and computer access warrants, they are executed covertly and the persons affected might never know that they were under surveillance.

4.54 Some general observations and criticisms that cover all three related proposals were made:

> Liberty Victoria is concerned that the proposals to extend the duration and allow the renewal of warrants potentially undermine judicial scrutiny of warrants. The lack of evidence to support the need for reforms and the lack of reference to accountability measures is problematic given the highly invasive nature of search warrants.[27]

4.55 The IGIS outlined the principles that ought to underpin the ASIO Act warrants regime:

> Proposals to increase the scope of existing powers or their duration need to ensure that safeguards exist such that the extended scope or longer timeframes do not become the norm, and that the warrants are not unduly broad and are executed reasonably and in accordance with the specifics of the legislation as well as the overarching privacy and proportionality objectives.[28]

Variation of warrants

4.56 The first proposal, which the Government states it wishes to progress, would allow the variation of all types of ASIO Act warrants.

4.57 The discussion paper explains that:

> Currently, the ASIO Act does not specifically provide for a warrant to be varied if the circumstances justify such a variation. A new warrant is required in every instance where there is a significant change in

27 Liberty Victoria, *Submission No. 143*, p. 3.

28 Inspector-General of Intelligence and Security, *Submission No. 185*, p. 3.

> circumstances. A variation provision may be appropriate to ensure sufficient operational flexibility while maintaining appropriate accountability.[29]

4.58 NSW Young Lawyers argued that the existing requirement that a new warrant should be applied for when there is a change in circumstances should be retained as that is an important accountability mechanism:

> In order to maintain accountability and ensure that an existing warrant did not endure inappropriately following a significant change in circumstances, any variation of a warrant as proposed would call for a level of accountability whereby the entire basis of the warrant would be reviewed in light of present, past and altered circumstances. This level of accountability is achieved under the existing provisions.[30]

4.59 The Law Council of Australia criticised the short description of the proposal in the discussion paper as lacking detail vital for consideration:

> For example, would there be different requirements for seeking a variation of a search warrant under section 25 compared with a variation of warrant to use a listening device under section 26? Would there be different limits on the period in respect of which an existing warrant could be renewed, depending on the nature of the power to be exercised? [31]

4.60 The Attorney-General's Department was asked which warrants are intended to be varied and in what ways might those warrants be varied. The Department clarified:

> It is envisaged that a general power to vary warrants could apply to all warrants under Division 2 Part III of the ASIO Act (this proposal does not cover questioning and detention warrants). A variation might be sought if there is a relatively minor change in circumstances. For example, if ASIO had a computer access warrant relating to a particular computer and also entry to the premises in which that computer is located. If the person moved house unexpectedly, before entry to the premises to access the computer occurred, the ability to request a variation to amend the address could be appropriate, as the core grounds (to access data on the target computer) would not have changed.[32]

---

29 Attorney-General's Department, *Equipping Australia against emerging and evolving threats*, Discussion Paper, July 2012, p. 41.

30 New South Wales Young Lawyers, *Submission No. 133*, p. 7; see also: Law Council of Australia, *Submission No. 96*, p. 67.

31 Law Council of Australia, *Submission No. 96,* p. 67; see also: New South Wales Young Lawyers, *Submission No. 133,* p. 6.

32 Attorney-General's Department, *Submission No. 236*, p. 5.

4.61 The Office of the Victorian Privacy Commissioner criticised what might be a potential expansion of the activities authorised by the warrant, without recourse to the issuing authority:

> In my view, the level of variation required needs to be carefully considered and should be extremely limited. Courts are (rightly) vested with authority to grant warrants; allowing "operational flexibility" to vary a warrant could potentially allow extension of a warrant beyond what was authorised by a court.[33]

4.62 The Attorney-General's Department was also asked which officer might be vested with the authority to vary the terms of a warrant. The Department responded that it would be the Attorney-General, the original issuer of the warrant:

> Given that the Attorney-General issues warrants and their terms and conditions, it would seem appropriate that the Attorney-General should have the responsibility for approving the variation of warrants.[34]

Committee comment

4.63 The Committee notes the Attorney-General's Department contention that allowing the variation of active ASIO Act warrants is appropriate in order to ensure sufficient operational flexibility for ASIO.

4.64 The Committee is satisfied that the appropriate accountability would be maintained if any such variation was authorised by the Attorney-General.

Recommendation 23

The Committee recommends the Government amend the warrant provisions of the *Australian Security Intelligence Organisation Act 1979* to promote consistency by allowing the Attorney-General to vary all types of ASIO Act warrants.

Duration of search warrants

4.65 The second proposal that the Government wishes to progress relates to the duration of ASIO Act search warrants. The discussion paper elaborated that the maximum duration of search warrants could be increased from 90 days to six

33 Office of the Victorian Privacy Commissioner, *Submission No. 109*, p. 4; see also: Ms Stella Gray, *Submission No. 152*, p. 9.

34 Attorney-General's Department, *Submission No. 236*, p. 5.

months, making those warrants consistent with the duration of all other warrants issued under that Act.

4.66 The discussion paper's rationale for extending the duration of search warrants to six months is that:

> … [it] would provide operational benefits as the exact timing of the search may depend on a range of unknown and fluid operational factors. Indeed, there have been instances where ASIO was unable to execute a search warrant within the 90 day limit for reasons beyond its control, and a new warrant would be required.[35]

4.67 The proposal to increase the duration of ASIO Act warrants was subject to many of the same criticisms that the variation of ASIO warrants proposal received, namely that current arrangements serve to protect the interests of affected parties. The Castan Centre for Human Rights Law observed that:

> A modest additional administrative burden is a small price to pay in return for avoiding any implication, for example, that certain persons are, by default, subject to covert intelligence surveillance.[36]

4.68 Contrary to the discussion paper's rationale, Mr Daniel Nazer asserted that the efficacy of search warrants may be better served by shorter deadlines for executing searches:

> As days, weeks, or even months go by, it becomes increasingly likely that a search warrant is based on stale information. Indeed, with a deadline as long as 180 days, it is possible that an investigation might evolve to the point of exonerating a target. Thus, limited warrant durations promote privacy by ensuring that searches are conducted based on fresh, accurate information.[37]

4.69 The Attorney-General's Department was asked why the current 90 day timeframe for the execution of search warrants is inadequate. The Department explained:

> ASIO operations require careful planning, and may require a high degree of flexibility as to when warrants are executed, in order to ensure access to the intelligence information and ensure protection of ASIO officers and methodology. Searches may be undertaken covertly, which may significantly limit opportunities to execute the warrant. A warrant enabling a search to take place within a six month period would provide

35 Attorney-General's Department, *Equipping Australia against emerging and evolving threats*, Discussion Paper, July 2012, p41, p. 42.

36 Castan Centre for Human Rights Law, *Submission No. 142*, p. 4.

37 Mr Daniel Nazer, *Submission No. 110*, p. 7.

> operational benefits as the exact timing of the search may depend on a range of unknown and fluid operational factors.[38]

4.70 The IGIS shed further light on the possible rationale of extending the duration of these warrants:

> I am aware of one general category of warrants where there is sometimes difficulty executing the warrant within 90 days. To ensure the legislative response is proportionate it may be preferable to allow this particular category of search warrants to be extended rather than all search warrants.[39]

4.71 Though it was not publicly discussed what types of searches may be difficult for ASIO to execute within 90 days, the IGIS offered an alternative solution to a blanket extension of all ASIO search periods:

> If that period is extended to six months then this should clearly be set as the maximum possible duration – not the default standard for all warrants. If this provision was enacted I would monitor search warrant requests closely to see whether the duration of each warrant request was considered on an individual basis to ensure it was valid for an appropriate time, which would usually be less than six months.[40]

4.72 The IGIS finally observed that there was overlap with another proposal included in the terms of reference, the 'named person warrant' for ASIO warrants. That concept is to create an additional form of warrant that would enable all forms of special powers to be available under the ASIO Act against a particular person. That proposal was referred to the Committee as one that the Government is considering and is discussed separately below.

4.73 The IGIS observed that:

> …it may be that the policy reason behind the change from 90 days to 6 months is directed at administrative ease and consistency for such warrants. However my view is that administrative ease and consistency are, in themselves, not compelling reasons to increase warrant powers or extend their duration.[41]

4.74 The Attorney-General's Department responded to the IGIS's concern:

> As with all ASIO warrant powers, six months would be a maximum duration. It would be open to ASIO to apply for a period shorter than six months where appropriate, or for the Attorney-General to grant a warrant

38 Attorney-General's Department, *Submission No. 236*, p. 3.

39 Inspector-General of Intelligence and Security, *Submission No. 185*, p. 15.

40 Inspector-General of Intelligence and Security, *Submission No. 185*, p. 15.

41 Inspector-General of Intelligence and Security, *Submission No. 185*, p. 15.

> with a shorter duration if an adequate supporting case for the maximum duration is not presented.
>
> While it is possible for ASIO to reapply for a new warrant if it has not been possible to conduct the search within the 90 day period, if the search has not been conducted and the grounds remain unchanged, arguably seeking a fresh warrant does not significantly add accountability. The warrant, whether in force for 90 days or six months, still only authorises one search of the premises. There is also a requirement under section 30 of the ASIO Act for the Director-General to notify the Attorney-General and take steps to ensure that any action under the warrant is discontinued if the Director-General ceases to be satisfied that the grounds for it exist.[42]

Committee comment

4.75 The Committee did not receive sufficient evidence to justify the proposal that the maximum duration of search warrants be increased from 90 days to six months.

Recommendation 24

Subject to the recommendation on renewal of warrants, the Committee recommends that the maximum duration of *Australian Security Intelligence Organisation Act 1979* search warrants not be increased.

Renewal of warrants

4.76 The third proposal that the Government wishes to progress relates to the renewal of ASIO Act warrants. The discussion paper notes that when a warrant expires, which is up to 6 months for most ASIO warrants, and there remains an ongoing need to use special powers, a new warrant must be sought from the Attorney-General by the Director-General of Security. The current provisions in the ASIO Act do not enable a warrant to be extended.

4.77 The discussion paper notes that certain threats to security can endure for many years and that the threats creating the need for a significant proportion of warrants continue beyond the initial authorisation periods. This means that:

> In such circumstances, ASIO must apply for a new warrant which necessitates restating the intelligence case and completely reassessing the legislative threshold in instances where there has not been a significant

42 Attorney-General's Department, *Submission No. 236*, p. 3.

> change to either, and where the assessment of the intelligence case remains unchanged. A renewal process would provide appropriate oversight and accountability without requiring excessive administrative resources.[43]

4.78 Liberty Victoria questioned the desirability of removing the need to obtain a new warrant:

> The renewal of a warrant is not a minor matter. It extends the power of ASIO officers to interfere in the personal privacy of suspects through the interception of communications, searches of private premises, installation of listening devices, inspection of postal articles and use of tracking devices. All renewals need to be based on clear evidence of the intelligence case and reference to the legislative threshold. Such basic standards should not be regarded as "excessive" administrative requirements.[44]

4.79 Though not expressly endorsing the introduction of a renewal process *in lieu* of requiring fresh warrants when existing investigations carry on past the expiry of original warrants, the IGIS did offer comfort to the Committee that ASIO would not lower the standards expected of it when assessing which matters are investigated with intrusive powers:

> My experience is that ASIO actively monitors changes in circumstances and is generally prompt in ensuring that action under a warrant is discontinued when the grounds for a warrant have ceased to exist. My understanding is that there is no intention in ASIO to reduce the scrutiny given to the intelligence case on renewal or re-issue of warrants or the ongoing monitoring of the grounds for the warrant – these essential internal assurance processes may limit the "streamlining" benefits the proposed amendment could deliver.[45]

4.80 The Gilbert + Tobin Centre of Public Law reminded the Committee that consideration of the concept of renewing warrants should also be considered in the context of the 'named person warrant' proposal:

> We would, however, note that the criteria, especially for renewal, should not be significantly less than those for issuing a warrant in the first place. This is particularly important given the proposal to merge warrant powers into a single category of warrant. Otherwise, renewal may become

---

43 Attorney-General's Department, *Equipping Australia against emerging and evolving threats*, Discussion Paper, July 2012, p. 42.

44 Liberty Victoria, *Submission No. 143*, p. 10; see also: Castan Centre for Human Rights Law, *Submission No. 142*, p. 4; Mr M Newton, *Submission No. 87*, p. 11.

45 Inspector-General of Intelligence and Security, *Submission No. 185*, p. 15.

> a means of rolling all of the warrant powers over every six months without meaningful consideration of whether the need still exists.[46]

4.81 The Attorney-General's Department was asked what was envisaged for a renewal process for ASIO warrants and how that may differ from applying for fresh warrants. The Department replied:

> It is envisaged that a renewal process would differ by enabling ASIO to present a renewal application to the Attorney-General that focuses on why it is necessary to continue the warrant and certifies that the facts and grounds specified in the original application have not changed. A simplified renewal process would provide significant administrative efficiencies for ASIO and the Attorney-General, without reducing oversight and accountability, as the Attorney-General would still need to be satisfied that the application meets the relevant threshold.[47]

4.82 Noting community concerns raised in submissions, the Attorney-General's Department also advised:

> …that the criteria for renewal should not be significantly less than those for issuing a warrant in the first place. The Attorney-General could still have responsibility for renewing warrants, and the IGIS would also continue to have oversight of all warrant documentation. On that basis, the Attorney-General would only grant a renewal if satisfied that the legislative requirements continue to be met. In doing so, the decision to renew warrants would be focused on any change in circumstances from when the original warrant was issued and the appropriateness of continuing the warrant for a further period.[48]

Committee comment

4.83 The Committee is of the view that there is merit in making the process of obtaining authority to continue the use of intrusive powers more efficient. This could be done with a form of renewal, rather than requiring ASIO to start its application afresh.

4.84 However, the standards and thresholds for obtaining a warrant should not be lowered for the renewal of the very same warrant. The Attorney-General ought to remain satisfied, by applying the same standards, that there is a threat that requires intrusive investigation, as they were when the original warrant or warrants were issued.

---

46 Gilbert + Tobin Centre of Public Law, *Submission No. 36*, pp. 13-14.

47 Attorney-General's Department, *Submission No. 236*, p. 4.

48 Attorney-General's Department, *Submission No. 236*, p. 4.

Recommendation 25

The Committee recommends that the *Australian Security Intelligence Organisation Act 1979* be amended to allow the Attorney-General to renew warrants.

ASIO Act employment provisions

4.85 The Terms of Reference to this inquiry state that the Government wishes to progress the modernisation of the ASIO Act employment provisions. ASIO officers are employed under the ASIO Act rather than the *Public Service Act 1999*. The discussion paper notes that the provisions relating to the employment of ASIO officers do not align with the Australian Public Service framework as the ASIO Act provisions have not been updated since they were originally enacted 30 years ago.

4.86 These proposals are:

- To delete the requirement for an ASIO employee to hold an "office" within ASIO;
- Replacing various descriptors denoting employment within ASIO, with a single descriptor, 'employee', throughout the ASIO Act;
- Repealing section 87 of the ASIO Act, which relates to employees who were employed immediately before the ASIO Act's commencement in 1979, of whom there are no longer any employed; and
- Secondment provisions.

4.87 The Committee received no evidence in relation to the first three proposals, however, they appear on their face to be of an innocuous administrative character.

Proposed secondment arrangements

4.88 The Terms of Reference to this inquiry state that the Government wishes to progress amendments to the ASIO Act to 'provide for additional scope for further secondment arrangements'. The discussion paper elaborates that this proposal is to legislate secondment arrangements for ASIO officers into other agencies and for officers from other agencies into ASIO:

> In order to access specialist skills and as part of arrangements whereby ASIO works closely with other agencies, ASIO often places staff of other agencies to work within ASIO, or agrees to its staff members working in other agencies. Legal complexities can arise in making such

> arrangements because of the specified scope of the functions and powers of ASIO and the other organisation involved.[49]

4.89 The discussion paper suggests that ASIO's ability to engage with other agencies would be enhanced, and administrative difficulties could be overcome if the ASIO Act expressly enabled the secondment of staff to and from ASIO. It is also proposed that, during the secondment, a seconded staff member carries out only the functions of the host organisation in accordance with any procedures or restrictions that apply under legislation to the host organisation.[50] For instance, this would mean that an ASIO officer seconded to the AFP would act according to the laws and rules that apply to the AFP, rather than ASIO.

4.90 The Inspector-General of Intelligence and Security submitting on the secondment proposal noted that there is potential for poorly constructed secondment arrangements to create opportunities for circumventing existing statutory limitations:

> If the secondment proposal is adopted I would be looking to ensure that the changes are applied in such a way that it is clear to individual officers which agency they are undertaking an activity for and that 'secondments' are a true change in working arrangements for a reasonable period. In my view it would not be proper for such a mechanism to be used to circumvent limits placed on employees in other legislation. For example it would not be proper for an ASIS staff member to be 'seconded' to ASIO for a day or two to enable them to perform an activity that they would otherwise not be permitted to undertake. My understanding is that this is not a practice the agencies intend to adopt.[51]

4.91 The discussion paper acknowledges that there is no intention for future secondment arrangements to be used to circumvent statutory limitations on the acts that officers from particular agencies may carry out. The current requirements that allow Intelligence Services Act agencies to co-operate with ASIO would operate independently of any new secondment provisions.[52]

Committee comment

4.92 The Committee is satisfied with the creation of new secondment provisions in the ASIO Act, provided that those arrangements cannot be used for the purpose

---

49 Attorney-General's Department, *Equipping Australia against emerging and evolving threats*, Discussion Paper, July 2012, p. 43.

50 Attorney-General's Department, *Equipping Australia against emerging and evolving threats*, Discussion Paper, July 2012, p. 43.

51 Inspector-General of Intelligence and Security, *Submission No. 185*, p. 16.

52 Attorney-General's Department, *Equipping Australia against emerging and evolving threats*, Discussion Paper, July 2012, p. 41.

of officers of agencies circumventing existing safeguards and limitations that apply to their employment and conduct.

Recommendation 26

The Committee recommends that the *Australian Security Intelligence Organisation Act 1979* be amended to modernise the Act's provisions regarding secondment arrangements.

Intelligence Services Act – Clarifying the authority of the Defence Imagery and Geospatial Organisation

4.93 The Government wishes to clarify the authority of the Defence Imagery and Geospatial Organisation (DIGO). The discussion paper explains that minor amendments to subsection 6B(e) of the *Intelligence Services Act 2001* (IS Act) would ensure that DIGO has clear authority to undertake its geospatial and imagery functions.

4.94 Under the IS Act, DIGO has a number of geospatial and imagery related intelligence functions, as well as civilian functions that relate to supporting Commonwealth, State and Territory governments as well as other bodies. The discussion paper explains that minor legislative clarifications are required to ensure that DIGO has clear legislative support to undertake its geospatial and imagery related functions.

4.95 DIGO's work under its civil assistance function may involve collecting imagery and other data in relation to locations inside and outside Australia. That work is not done for the purpose of providing information about a particular person or entity. This means that is not an intelligence-gathering function but DIGO may still utilise the same sources or capabilities that it uses for intelligence collection to perform its statutory civil assistance function.

4.96 The discussion paper proposes amendments to the Intelligence Services Act to avoid any doubt that DIGO is enabled to provide Commonwealth and State authorities, and other approved bodies, assistance in relation to the production and use of both non intelligence and intelligence imagery and geospatial products.[53]

4.97 The discussion paper also proposes that the IS Act be amended to include an express power for DIGO to provide specialised imagery and geospatial technologies assistance to Commonwealth, State and Territory authorities and

53 Attorney-General's Department, *Equipping Australia against emerging and evolving threats*, Discussion Paper, July 2012, p. 45.

certain non-government bodies. This would include the use and application of specialised imagery and geospatial technologies, including geospatial web-based services.[54]

4.98 Because DIGO is an organisation that uses intelligence-gathering capabilities for both intelligence and non-intelligence functions, as well as using those capabilities to image locations within Australia and overseas, some submitters urged caution in amending the legal framework in which DIGO operates.

4.99 For example, Ms Stella Gray highlighted for the Committee that:

> This would enable ASIS, DSD and DIGO to collect intelligence on Australian citizens whenever the agencies are cooperating with ASIO in the performance of its functions. This proposal does not include any provision to prevent the abuse of power by these agencies whilst working in concert. This proposal cannot be supported with the current level of accountability it demands of these agencies.[55]

4.100 The discussion paper explains that the safeguards that prevent possible abuses of power will remain in place:

> The proposed amendments do not change the original intended operation of section 6B of the IS Act. The existing safeguards in the IS Act would remain unaffected and in place. The suggested changes involve minor clarifications to provide more certainty and practical utility. By making the legislation clearer, it would be easier for the Inspector-General of Intelligence and Security to effectively review whether DIGO is operating within its powers, and ensure accountability is maintained.[56]

4.101 The IGIS further elaborated on the protections that would prevent the risk of abuse of power by DIGO and the agencies and bodies that it may assist:

> If such assistance was also for the specific purpose of producing intelligence on an Australian person my expectation is that DIGO would continue to be required to obtain ministerial authorisation. I also expect DIGO to continue to apply the Privacy Rules made under s. 15 of the IS Act to any disclosure of intelligence about an Australian person, regardless of which function the intelligence was collected under.[57]

---

54 Attorney-General's Department, *Equipping Australia against emerging and evolving threats*, Discussion Paper, July 2012, p. 45.

55 Ms Stella Gray, *Submission No. 152*, p. 10.

56 Attorney-General's Department, *Equipping Australia against emerging and evolving threats*, Discussion Paper, July 2012, p. 45.

57 Inspector-General of Intelligence and Security, *Submission No. 185*, p. 23.

Committee comment

4.102 The Committee agrees that the IS Act should be amended to clarify DIGO's authority to assist other agencies and bodies, provided that the existing oversight and accountability mechanisms would apply.

Recommendation 27

The Committee recommends that the *Intelligence Services Act 2001* be amended to clarify the authority of the Defence Imagery and Geospatial Organisation to undertake its geospatial and imagery functions.

Matters the Government is considering

4.103 The second category of reform proposals are matters which the Terms of Reference state the Government is considering. These are proposals to amend the ASIO Act to:

- Create an authorised intelligence operations scheme;
- Create a named person warrant;
- Align the ASIO Act surveillance device provisions with the *Surveillance Devices Act 2004*;
- Allow the Director-General of ASIO to create authorisation lists for the execution of warrants;
- Clarify ASIO's ability to operate with the private sector; and
- Refer breaches of the prohibition on identifying ASIO officers to law enforcement for investigation.

Creation of an authorised intelligence operations scheme

4.104 The Terms of Reference state that the Government is considering amending the ASIO Act to create an authorised intelligence operations scheme. Such a scheme would provide ASIO officers and its human sources with protection from criminal and civil liability for certain conduct in the course of authorised intelligence operations.

4.105 The discussion paper proposes the creation of an authorised intelligence operations scheme (or controlled operations scheme) for ASIO officers, based on that currently available to certain law enforcement officers under the Crimes Act

'with appropriate modifications and safeguards that recognise the scheme would operate in the context of covert intelligence gathering investigations or operations'.[58]

4.106 Existing controlled operations provisions in Commonwealth and State and Territory laws provide for the issue of authorities which provide immunity from prosecution and indemnity from civil liability for law enforcement officers and nominated civilian participants who engage in activities that would otherwise be unlawful.

4.107 The Australian Federal Police (AFP)'s Annual Controlled Operations Report for 2010-11 notes that controlled operations can be used to uncover serious illicit and organised criminal activity such as the smuggling of drugs, firearms and persons and to disband or disrupt organised criminal syndicates.[59]

4.108 In relation to creating an analogous scheme for ASIO, the discussion paper explains that:

> An authorised intelligence operations scheme would significantly assist covert intelligence operations that require undercover ASIO officers or human sources to gain and maintain access to highly sensitive information concerning serious threats to Australia and its citizens.[60]

4.109 The discussion paper also provides that:

> Should an authorised intelligence operations regime be pursued, it will be critical that it achieves an appropriate balance between operational flexibility and appropriate oversight and accountability. Key features that may contribute to such could include:
>
> - the Director-General of Security to issue authorised intelligence operation certificates which would provide protection from criminal and civil liability for specified conduct for a specified period (such as 12 months);
> - oversight and inspection by the IGIS, including notifying the IGIS once an authorised intelligence operation has been approved by the Director-General;
> - specifying conduct which cannot be authorised (for example, intentionally inducing a person to commit a criminal offence that the person would not otherwise have intended to commit and conduct that is likely to cause the death of or serious injury to a person or involves the commission of a sexual offence against any person), and

58 Attorney-General's Department, *Equipping Australia against emerging and evolving threats*, Discussion Paper, July 2012, p. 46.

59 AFP, *Controlled Operations annual Report 2010-2011*, viewed 12 November 2012, <www.afp.gov.au/media-centre/publications/~/media/afp/html/controlled-operations-annual-report-2010-2011.ashx>.

60 Attorney-General's Department, *Equipping Australia against emerging and evolving threats*, Discussion Paper, July 2012, p. 46.

- independent review of the operation, effectiveness and implications of any such scheme, which could be conducted five years after the scheme's commencement.[61]

4.110 The potential creation of an authorised intelligence operations scheme raised a number of criticisms in submissions and at hearings.

4.111 Dr Patrick Emerton of the Castan Centre for Human Rights Law at Monash University drew an important distinction between ASIO and traditional law enforcement agencies such as police forces. Dr Emerton contended that ASIO:

> ...is not a law enforcement agency and is not accountable through the criminal trial process in the way that a law enforcement agency is, and it is therefore not governed by the very strict chapter 3 [of the *Constitution*] jurisprudence that governs the behaviour of law enforcement agencies under our constitutional law. It is in a very different constitutional position, a very different administrative position and a very different policy position, and it is essentially secret.[62]

4.112 The IGIS questioned why ASIO's existing relationships with law enforcement agencies could not be utilised to take advantage of the existing controlled operations regimes:

> I am aware that over a period of some years my office has received a small number of complaints from current and former ASIO human sources that demonstrate the complexity of the relationship. The paper does not explain why ASIO could not request the AFP or ACC to use existing powers to perform these functions, including where necessary authorising ASIO officers or sources under the existing schemes.[63]

4.113 The Attorney-General's Department was asked if ASIO would be able to rely on the AFP to conduct controlled operations on its behalf. The Department contended that it would not always be possible:

> While there might be some capacity to utilise this scheme in joint counter-terrorism investigations, ASIO security intelligence operations extend across the range of national security matters within the ASIO Act. Some operations may cover matters not normally the subject of criminal investigations, such as foreign interference. Similarly, ASIO may be involved at a stage where there would not be sufficient grounds for law enforcement to investigate the possible commission of an offence.[64]

---

61 Attorney-General's Department, *Equipping Australia against emerging and evolving threats*, Discussion Paper, July 2012, pp. 46-47.

62 Dr Patrick Emerton, Castan Centre for Human Rights Law, *Transcript*, Melbourne, 5 September 2012, p. 21; see also NSW Council for Civil Liberties, *Submission No. 175*, p. 13; Law Council of Australia, *Submission No. 96,* p. 58.

63 Inspector-General of Intelligence and Security, *Submission No. 185*, p. 18.

64 Attorney-General's Department, *Submission No. 236*, p. 6.

4.114 The Gilbert + Tobin Centre of Public Law argued that it would not be necessary to create an indemnity scheme for ASIO as it would be unlikely that ASIO officers would be prosecuted for crimes committed in the course of their duties because the Commonwealth Director of Public Prosecutions has a discretion whether or not to prosecute individuals for terrorism and other offences:

> It is highly unlikely that an ASIO officer would be prosecuted for activities done in the course of an undercover operation.[65]

4.115 The Attorney-General's Department argued that ASIO would not be able to rely on prosecutorial discretion, even where it was available:

> While a general prosecutorial discretion is available, decisions on whether to pursue a prosecution are determined on a case-by-case basis by the relevant Director of Public Prosecutions. It is not normal practice for the Director of Public Prosecutions to give advance indemnities or immunities from future prosecution. In addition, there is no equivalent mechanism to provide indemnity from civil proceedings.[66]

Committee comment

4.116 The Committee received evidence that there are occasions on which ASIO officers and sources are placed in positions where, in order to carry out their duties, they may need to engage in conduct which may, in ordinary circumstances, be a breach of the criminal law. The Committee understands that such occasions would be seldom but may from time to time arise. The Committee also understands that it will not be possible for ASIO to rely on the existing framework under which the AFP operates.

4.117 The Committee is therefore of the view that the ASIO Act should be amended to create a controlled intelligence operations scheme.

4.118 The discussion paper suggests particular restrictions, reporting and accountability mechanisms. The Committee agrees that an ASIO authorised intelligence operations scheme should be subject to strict accountability and oversight.

4.119 The Committee supports the adaptation of the procedures and safeguards in the *Crimes Act 1914* that apply to the AFP's controlled operations. This would mean that ASIO officers and agents would be exempted from criminal and civil liability only for certain authorised conduct.

4.120 The Committee expects that unreasonable or reckless conduct would not be indemnified by an authorised intelligence operation, and the ASIO officer or source would be liable for such conduct.

---

65 Gilbert + Tobin Centre of Public Law, *Submission No. 36*, p. 16.

66 Attorney-General's Department, *Submission No. 236*, p. 6.

Recommendation 28

The Committee recommends that the *Australian Security Intelligence Organisation Act 1979* be amended to create an authorised intelligence operations scheme, subject to similar safeguards and accountability arrangements as apply to the Australian Federal Police controlled operations regime under the *Crimes Act 1914*.

Named person warrants

4.121 The Government is considering amending the ASIO Act to establish a named person warrant enabling ASIO to request a single warrant specifying multiple (existing) powers against a single target, instead of requesting multiple warrants against a single target.

4.122 The discussion paper explains that:

> In approximately one third of cases, more than one ASIO Act warrant type is sought against a particular target. Under the current provisions, this requires the preparation of multiple applications, each re-casting the available intelligence case to emphasise the relevant facts and grounds to satisfy the different legislative requirements of the various warrant types, which is administratively burdensome.
>
> The same outcome could be achieved with greater efficiency and with the same accountability by enabling ASIO to apply for a single warrant covering all ASIO Act warrant powers where the relevant legislative thresholds are satisfied.[67]

4.123 As noted above, ASIO Act warrants are issued by the Attorney-General at the request of the Director-General of Security.

4.124 The different types of warrants involve different activities and consequently different levels of intrusiveness. In addition, the precise matters in respect of which the Attorney-General must be satisfied vary depending on the power to be exercised under the warrant.

4.125 The warrants are also required to specify the particular activities or things that are authorised in the particular circumstances.

4.126 The notion that the different types of warrants with their different powers could be combined into a single type raised several issues with submitters.

67 Attorney-General's Department, *Equipping Australia against emerging and evolving threats*, Discussion Paper, July 2012, p. 45.

4.127 The Castan Centre for Human Rights Law objected to the asserted benefit of reducing administrative burdens, arguing that:

> Administrative burden is a small price to pay in order to preserve a regime which creates a strong presumption against the permissibility of covert intelligence intrusion into people's affairs.[68]

4.128 The Attorney-General's Department was asked if there are any benefits, beyond administrative convenience, in creating a named person warrant that would enable all ASIO powers to be used against a single target. The Department explained that efficiency could be introduced without weakening accountability:

> The same outcome could be achieved with greater efficiency and with the same accountability by enabling ASIO to apply for a single warrant covering all powers proposed to be used against the target where the relevant legislative thresholds are satisfied. The proposal is intended to cover various warrant powers in Division 2 of Part III other than foreign intelligence collection warrants, and it would not include questioning or questioning and detention warrants.[69]

4.129 The Law Council of Australia noted that the current warrant processes require the Attorney-General to consider the use of each power separately, which allows the Attorney-General to consider the particular nature of the power to be exercised, the benefit this is likely to have to the collection of intelligence relevant to security and that:

> This type of assessment would be made significantly more difficult if a single warrant covering multiple powers were introduced.[70]

4.130 The Attorney-General's Department countered that:

> Arguably, a named person warrant could enhance the Attorney-General's assessment of the appropriateness of the use of particular powers against a single person when issuing a warrant, and whether the use of a particular power or number of powers will assist ASIO in obtaining intelligence relevant to security.[71]

4.131 The Inspector-General of Intelligence and Security (IGIS) questioned how the Government intends to reconcile the different tests and thresholds for the different warrants into a combined warrant. The IGIS further asked if there was an intention to shift the decision-making process for which powers would be exercised from the Attorney-General, to the Director-General of ASIO:

---

68 Castan Centre for Human Rights Law, *Submission No. 142*, p. 4.

69 Attorney-General's Department, *Submission No. 236*, p. 11.

70 Law Council of Australia, *Submission No. 96*, p. 70.

71 Attorney-General's Department, *Submission No. 236*, p. 11.

> While such a scheme might be administratively simpler, there is the risk that the warrant would authorise activities that were not proportionate to the threat to security and may shift the balance between what is currently authorised by the Attorney-General and what is authorised by the Director-General.[72]

4.132 The Attorney-General's Department, being aware of the IGIS' concern, explained:

> It is important to note that it is not proposed that a named person warrant would provide a blanket authority for ASIO to use any special power. The warrant would need to specify which powers are covered and the use of each power would need to be justified and meet the relevant legislative threshold. It is not intended that this proposal will weaken any of the thresholds.[73]

Committee comment

4.133 The Committee received evidence that there would be a benefit to ASIO and to the Attorney-General in being able to issue a single warrant to authorise the use of multiple powers, over one person, for the same investigatory purpose.

4.134 The Committee notes that this proposal does not intend to weaken any of the thresholds for the use of the various special powers.

4.135 The Committee has been advised that it is not proposed that a named person warrant would provide a blanket authority for ASIO to use any special power and that the Attorney-General will have to decide which particular powers will be covered by each warrant.

4.136 In classified evidence a case was made supporting the establishment of a named person warrant. While it is the preference of the Committee wherever possible not to rely on classified evidence, in this instance it has been unavoidable. While the classified evidence was sufficient to give in principle support to the proposal, the Committee believes that further examination is necessary.

72 Inspector-General of Intelligence and Security, *Submission No. 185*, p. 19.

73 Attorney-General's Department, *Submission No. 236*, p. 11.

Recommendation 29

The Committee recommends that should the Government proceed with amending the *Australian Security Intelligence Organisation Act 1979* to establish a named person warrant, further consideration be given to the factors that would enable ASIO to request a single warrant specifying multiple powers against a single target. The thresholds, duration, accountability mechanisms and oversight arrangements for such warrants should not be lower than other existing ASIO warrants.

Surveillance devices – use of optical devices

4.137 The Government is considering amending the ASIO Act to modernise the warrant provisions to align the surveillance device provisions with the *Surveillance Devices Act 2004* (SD Act).

4.138 The discussion paper notes that the ASIO Act provisions governing ASIO's capabilities with respect to electronic surveillance have not been updated to align with legislation governing the use of electronic surveillance by law enforcement. The discussion paper proposes aligning the surveillance device provisions in the ASIO Act with the more modern SD Act, which provides for warrants for the use of surveillance devices by the Australian Federal Police, the Australian Crime Commission and the Australian Commission for Law Enforcement Integrity.

4.139 The Attorney-General's Department was asked on notice for further information on the purpose of aligning the two pieces of legislation. The Department explained how the ASIO Act provisions had fallen behind the equivalent provisions for law enforcement agencies:

> For example, ASIO's ability to use optical surveillance devices is tied to its ability to use listening devices. This is a relic of the time in which the ASIO Act was first drafted. Additionally, the administrative and procedural provisions governing the use of listening and tracking devices in the ASIO Act are not aligned with provisions governing the use of surveillance devices by law enforcement. Some of the differences where alignment is proposed would be:
>
> - addressing the lack of a separate optical surveillance device warrant
> - the provision of a single surveillance device warrant
> - the ability to adapt new future technologies by allowing surveillance devices to be prescribed in regulation, and
> - clarifying that certain surveillance devices may be used in limited circumstances without a warrant (for example, the use of an optical

> device that does not involve entry onto premises without permission or interference without permission of any vehicle or thing).[74]

4.140 The Inspector-General of Intelligence and Security commented that:

> If the proposal is only to modernise the language of the ASIO Act – which for example rather confusingly includes a device for recording images within the definition of a 'listening device' – then this is a more focussed proposal that does not raise propriety concerns[75].

Committee comment

4.141 The Committee did not receive any evidence contradicting the IGIS and AGD evidence. Consequently, there is no apparent reason to doubt the desirability of aligning those two pieces of legislation.

Recommendation 30

The Committee recommends that the *Australian Security Intelligence Organisation Act 1979* be amended to modernise the warrant provisions to align the surveillance device provisions with the *Surveillance Devices Act 2004*, in particular by optical devices.

Person searches

4.142 The Terms of Reference state that the Government is considering amending the ASIO Act to enable person searches to be undertaken independently of a premises search.

4.143 The ASIO Act currently contains the power to search a premises. That power also contains a further power to search a person who is at or near the premises where there are reasonable grounds to believe that the person has, on his or her person, records or other things relevant to the security matter.

4.144 The discussion paper explains that:

> Where ASIO assess that a particular person may be carrying items of relevance to security, a search warrant relating to a particular premises must be sought. It is only on or near the premises specified in the warrant that a person may be searched. However, it is not always feasible to execute a search warrant on a person of interest while they are 'at or near' the premises specified in the warrant.[76]

74 Attorney-General's Department, *Submission No. 236*, p. 9.

75 Inspector-General of Intelligence and Security, *Submission No. 185*, p. 20.

76 Attorney-General's Department, *Equipping Australia against emerging and evolving threats*, Discussion Paper, July 2012, p. 48.

4.145 The existing limitation leads to a practical problem that:

> For example, some persons of interest employ counter-surveillance techniques such that predicting the likely timing and location at which a search would yield the desired intelligence dividend is not always possible.[77]

4.146 When answering a question about the purpose of enabling person searches to be undertaken independently of a premises search, the Attorney-General's Department gave a more detailed example of where a person search could be executed away from a specified premises:

> As noted in the discussion paper, the sort of scenario where power to search a person might be relevant is where a foreign agent is passing security relevant material to someone in a public space, such as a park.[78]

4.147 The discussion paper proposes that that problem could be addressed by enabling ASIO to request a warrant to search a specified person rather than premises so that there would be 'sufficient operational flexibility' while maintaining appropriate accountability via the warrant process.

4.148 The discussion paper also suggests that the existing safeguard that ASIO Act search warrants do not authorise a strip search or a search of a person's body cavities will remain in place.[79]

4.149 The IGIS noted that this proposal is better described, not as an extension of the existing power to search premises, but is rather a proposal to introduce a new class of warrant. The IGIS argued, therefore, that it is important to carefully consider of the restrictions and conditions that should apply to the new warrant:

> I am aware of one category of activities where ASIO currently relies on premises search warrants to achieve what is in effect a person search. While I do not have concerns about the legality of the current approach, from an oversight and transparency perspective it would be preferable for the legislation to provide a specific mechanism for person searches with appropriate limits rather than using a premises search warrant for this purpose.
>
> Care needs to be taken that those undertaking a person search have appropriate training and qualifications. To this end it may be preferable to require that, where possible, such searches are undertaken by law enforcement officers who have specific training in this regard.[80]

---

77 Attorney-General's Department, *Equipping Australia against emerging and evolving threats*, Discussion Paper, July 2012, p. 48.

78 Attorney-General's Department, *Submission No. 236*, p. 10.

79 Attorney-General's Department, *Equipping Australia against emerging and evolving threats*, Discussion Paper, July 2012, p. 48.

80 Inspector-General of Intelligence and Security, *Submission No. 185*, p. 20

4.150 The search power proposal was criticised in a number of submissions, including the acting Victorian Privacy Commissioner:

> I consider an alteration of the warrant procedure in such a fashion to be extraordinarily broad and intrusive. It would have a serious adverse impact on an individual's privacy, may unduly infringe a number of human rights and freedoms (such as the freedom from arbitrary search and seizure), and interfere with the privacy of one's home and family. In particular, despite the safeguards in place, there is a possibility of using a person search to repeatedly harass a target at multiple locations (eg work, home, in a public space etc).[81]

4.151 In response, the Attorney-General's Department explained that the person search proposal would not lead to a series of searches or the possibility of ASIO harassing suspects:

> ASIO would only be able to conduct one search per warrant and could not use the warrant to harass the target at multiple locations. This proposal is not recommending ASIO be given stop and search powers, such as those available to police in some circumstances.[82]

4.152 Liberty Victoria submitted that allowing the search of people away from pre-determined premises could be disruptive to the lives of searched people if they were to be searched in public spaces and offered that:

> While we recognise that the current 'at or near' requirement poses operational challenges, we believe that the appropriate solution lies with operational tactics, not with legislative amendment.[83]

4.153 The Castan Centre for Human Rights Law submitted that ASIO's existing search warrant power remains controversial and that search powers should only be granted to police:

> If individuals are suspected of committing criminal offences there is already ample provision under state and Commonwealth law for police officers to exercise powers of arrest and/or search. Steps should not be taken which would give ASIO even the hint of the character of a secret police force.[84]

4.154 The Gilbert + Tobin Centre for Public Law agreed that search powers are better delegated to police forces than to an intelligence agency but suggested means to mitigate their existence:

---

81 Office of the Victorian Privacy Commissioner, *Submission No. 109*, p. 5.

82 Attorney-General's Department, *Submission No. 236*, p. 10.

83 Liberty Victoria, *Submission No. 143*, p. 12.

84 Castan Centre for Human Rights Law, *Submission No. 142*, pp.4-5; see also: Law Council of Australia, *Submission No. 96*, p. 58.

> However, in the event that a separate category of person search warrant is established, ASIO searches must be accompanied by similar safeguards as apply to searches by law enforcement officers. If not, there is a risk that ASIO searches will be used as a means of circumventing the safeguards attaching to law enforcement searches.[85]

4.155 The Attorney-General's Department elaborated on the safeguards that might apply if ASIO was allowed to conduct these searches independent of particular premises:

> The existing safeguards that apply to searching a person when on a premises would also continue to apply, including:
>
> - Not authorising a strip search or a search of a person's body cavities.
> - Where practicable, the search must be carried out by a person of the same sex as the person being searched.
> - Key requirements in the ASIO Guidelines that are relevant would be the requirement of proportionality, to use the least intrusive powers where possible, and the need to have regard to the cultural sensitivities, values and mores of certain persons.
> - ASIO has internal policies, procedures and training requirements that relate to the proper conduct of searches.
> - The exercise of this power, as with all ASIO's powers, would be subject to oversight by the IGIS.[86]

Committee comment

4.156 The Committee is very mindful of the importance of maintaining the clear distinction between intelligence and law enforcement. ASIO is not a law enforcement agency; it is an intelligence agency. Its statutory charter makes this clear. The Committee has serious misgivings about whether this power would take ASIO into the realm of law enforcement and policing. As well, we note that ASIO did not, upon inquiry, press for this power.

Recommendation 31

The Committee recommends that the *Australian Security Intelligence Organisation Act 1979* not be amended to enable person searches to be undertaken independently of a premises search.

85 Gilbert + Tobin Centre of Public Law, *Submission No. 36*, p. 13. See also: Tasmanian Association of Community Legal Centres, *Submission No. 184*, p. 4.

86 Attorney-General's Department, *Submission No. 236*, p. 10.

Authorisation lists for warrants

4.157 The Government is considering amending the *Australian Security Intelligence Organisation Act 1979* (ASIO Act) to establish classes of persons able to execute warrants.

4.158 Section 24 of the ASIO Act provides that the Director-General (or senior officer authorised in writing by the Director-General for the purposes of this section) may approve certain officers and employees to execute warrants issued under Division 2 of Part III of the ASIO Act.

4.159 The discussion paper explains that the requirement to maintain a list of the individual names of employees who may be involved in executing a warrant can create operational inefficiencies for ASIO. For example, sometimes the execution of a warrant takes place in unpredictable and volatile environments and ASIO needs to be able to quickly expand the list of authorised persons.[87]

4.160 The discussion paper proposes that:

> The problem could be overcome in large part if the Director-General could approve classes of people to execute a warrant. For example, the Director-General could authorise officers of a certain level within a particular Division of ASIO. Such persons at any one time would be readily ascertainable ensuring the level of accountability is not diminished, while improving operational efficiency.[88]

4.161 The proposal to alter authorisations from specific named individuals to classes of people received limited public comment. Mr Mark Newton, submitting in a private capacity, stated:

> I have no objection to authorisation lists for warrants, provided the persons on the authorisation lists would otherwise qualify as officers and employees able to execute warrants under the current version of Division 2 of Part III of the ASIO Act.[89]

4.162 Arguing in the contrary, the Law Council of Australia was of the view that specifically naming particular officers within ASIO offered an accountability benefit:

> For the Law Council, moving beyond the existing level of flexibility to allow the Director-General to authorise a list of persons based on a certain level within a particular Division of ASIO would tip the balance too far in favour of operational efficiency, and away from the need to strictly regulate the use of these intrusive and extraordinary powers. As noted

87 Attorney-General's Department, *Equipping Australia against emerging and evolving threats*, Discussion Paper, July 2012, p. 49.

88 Attorney-General's Department, *Equipping Australia against emerging and evolving threats*, Discussion Paper, July 2012, p. 49.

89 Mr Mark Newton, *Submission No. 87*, p. 12.

> elsewhere in this submission, improving operational efficiency, while a worthy goal, is not of itself enough to justify an expansion of powers or in this case, a dilution of important safeguards.[90]

4.163 The Inspector-General of Intelligence and Security, who would be empowered to carry out that oversight function was of the view that:

> While this could be operationally effective, it would be essential for ASIO to ensure that all officers in a particular class were fully trained and understood the limits of their authorisation. As noted above in relation to [person search warrants] there may be cases where the best qualified officers to conduct a particular search are law enforcement officers.[91]

4.164 Telstra advised that telecommunications industry participants that carry out interception activities on behalf of ASIO would need to be kept advised of which individual officers fall within the proposed classes in order to ensure that the industry participants can remain fully aware of which officers are in fact so authorised:

> Telstra agrees that the classes of persons who are eligible to execute a warrant will need to be clearly defined as to what types of warrants they can authorise and under what law. Careful consideration will also need to be given to the appropriate levels of oversight and record keeping. A list of persons will then need to be conveyed to C/CSPs to reduce any risk of harm, unauthorised interception or breaches of customer privacy by persons who are not eligible to execute a warrant.[92]

Committee comment

4.165 It is not clear what benefit there is in maintaining the current requirement to specifically name ASIO officers who are authorised to execute warrants. Allowing the Director-General of ASIO to delegate those functions to a class of people appears sensible.

4.166 The Committee accepts the rationale for moving to authorising ASIO officers by position rather than specific name.

---

90 Law Council of Australia, *Submission No. 96*, p. 73; see also: New South Wales Young Lawyers, *Submission No. 133*, p. 9.

91 Inspector-General of Intelligence and Security, *Submission No. 185*, p. 21.

92 Telstra, *Submission No. 189*, p. 14.

Recommendation 32

The Committee recommends that the *Australian Security Intelligence Organisation Act 1979* be amended to establish classes of persons able to execute warrants.

Clarifying ASIO's ability to co-operate with private sector

4.167 The Terms of Reference to this inquiry state that the Government is considering amending the *Australian Security Intelligence Organisation Act 1979* (ASIO Act) to clarify ASIO's ability to co-operate with the private sector.

4.168 The ASIO Act enables ASIO to cooperate with authorities of the Commonwealth and States and Territories where it is necessary or conducive to the functions of ASIO. However, it is unclear whether the Act implies that ASIO should not cooperate with organisations outside of government.

4.169 The discussion paper explains that it is conducive to ASIO's functions to cooperate with the private sector as the private sector plays a role in Australia's national security, including by owning and operating a significant proportion of Australia's critical infrastructure. ASIO's Business Liaison Unit provides an interface between Australian business and the Australian Intelligence Community by providing security reporting that can be used for private sector risk management.[93]

4.170 Consequently, the discussion paper suggests it may be desirable to amend the ASIO Act to avoid any doubt about ASIO's ability to cooperate with the private sector.

4.171 Despite ASIO already interacting with some elements of the private sector on critical infrastructure matters, the Australian Privacy Foundation disagreed that ASIO should be able to co-operate with the private sector:

> The Committee should express serious concern about the continued trend to enlist corporations as part of the national security apparatus. All responsibilities of corporations and individuals must be explicit and clear at law and not subject to discretionary interpretation by law enforcement and national security agencies of rubbery clauses that permit or require "cooperation".[94]

4.172 Conversely, Mr Ian Quick, submitting in a private capacity, agreed as to the need for ASIO to co-operate with private sector entities:

93 Attorney-General's Department, *Equipping Australia against emerging and evolving threats*, Discussion Paper, July 2012, p. 49.

94 Australian Privacy Foundation, *Submission No. 162*, p. 10.

> There is no doubt that ASIO should be able to cooperate with the private sector, the big issue is on what basis, with what oversight, what permissions it requires (or should require) on a case by case basis, etc etc.[95]

4.173 Oversight of ASIO's co-operation with private sector entities by the IGIS would be one of the oversight mechanisms that would give the Committee comfort. Indeed, the IGIS offered as much in her submission:

> My office regularly inspects the files of ASIO's interactions with, for example, State law enforcement agencies. We also have the ability to review ASIO's cooperation with private sector entities if appropriate.[96]

Committee comment

4.174 ASIO's co-operation with private sector organisations is clearly necessary given that so much of Australia's critical infrastructure is controlled and secured by the private sector. There is a clear public interest in the Government, through its security intelligence agency, to advise on security threats to all parties that are involved in providing critical infrastructure.

4.175 The Committee offers support to amending legislation to give ASIO a clear mandate to co-operate with the private sector.

4.176 The Committee appreciates that there are issues of confidentiality likely to arise in dealing with the private sector. The Committee has an open mind as to whether those confidentiality issues should be addressed by legislation or administrative arrangements. The Committee recommends that the Government clarify the types of information that would be shared and what handling and dissemination limitations would apply in legislation. For example, creating similar limitations for co-operating with the private sector as currently exist for ASIO's co-operation with various government bodies.

Recommendation 33

The Committee recommends that the *Australian Security Intelligence Organisation Act 1979* be amended to formalise ASIO's capacity to co-operate with private sector entities.

95 Mr Ian Quick, *Submission No. 95*, p. 12.

96 Inspector-General of Intelligence and Security, *Submission No. 185*, p. 21

Identifying ASIO officers

4.177 The Terms of Reference to the Inquiry state that Government is expressly seeking the views of the Committee on Amending the ASIO Act to enable ASIO to refer breaches of section 92 of the ASIO Act (publishing the identity of an ASIO officer) to authorities for investigation.

4.178 The discussion paper explains that section 92 makes it an offence for a person to publish the identity of an ASIO officer. The offence is punishable by 12 months imprisonment.

4.179 However, section 18 of the ASIO Act limits the circumstances in which a person can communicate information or intelligence acquired through their association with ASIO. In particular, information may only be passed to law enforcement agencies in relation to a 'serious crime' (defined as an offence punishable by imprisonment exceeding 12 months).

4.180 Because the ability to pass information to law enforcement only applies if the maximum penalty for an offence *exceeds* 12 months and the maximum penalty for the section 92 offence is precisely 12 months, ASIO is therefore precluded from passing information about the possible commission of this offence to law enforcement agencies.

4.181 The Committee received limited comment on this particular proposal. Ms Stella Gray, submitting in a private capacity, objected to the existence of section 92 in its current formulation:

> Under The ASIO Act 1979 it is a serious offence to publicly identify ASIO officers or agents, which means detainees are unable to take ASIO or one of its officers to court for torture prolonged interrogation and other abuses.[97]

4.182 Similarly, Mr Mark Newton contended that the ASIO Act should be amended to allow for identifying ASIO officers in limited circumstances:

> I object to section 92 in its current form. There have been times in recent history when it would be in the public interest to identify ASIO officers, specifically those who are likely to be involved in criminal acts. I would not support any strengthening of section 92 unless and until it is amended to include a workable public interest exception.[98]

Committee comment

4.183 The Committee agrees that there is a need to allow ASIO to refer breaches of section 92 to law enforcement for investigation.

---

97 Ms Stella Gray, *Submission No. 152*, p. 8.

98 Mr Mark Newton, *Submission No. 87*, p. 12.

4.184 Regarding the idea of a public interest defence for identifying ASIO officers, the Committee foresees a significant risk in allowing for the identification of ASIO officers. Because of the inherent secrecy of ASIO's work, it is necessary to keep each officer's association with ASIO secret. If that secrecy is breached and an ASIO officer's identity is disclosed then their career is effectively finished. In some cases there may be risks to the safety of an officer due to unauthorised disclosure of their identity.

4.185 Allowing a public interest defence for disclosure of an ASIO officer's identity leads to the dilemma that an ASIO's officers identity would be disclosed with the negative consequences effective immediately. However, the public interest of exposing an ASIO officer's identity, if any, would not be determined until a much later date.

4.186 For these reasons the Committee does not support a mechanism that would allow for the disclosure of an ASIO officer's identity.

Recommendation 34

The Committee recommends that the *Australian Security Intelligence Organisation Act 1979* be amended so that ASIO may refer breaches of section 92 to law enforcement for investigation.

Matters on which the Government expressly seeks the Committee's views – ASIO Act amendments

4.187 The third category of proposals is those that the Government expressly seeks the views of the Committee. The proposals are to amend the ASIO Act to:

- Allow for the incidental entry onto premises while executing warrants;
- Clarify when force can be used in the execution of warrants; and
- The creation of an evidentiary certificates regime for some ASIO warrants.

Incidental entry onto premises

4.188 The Government expressly seeks the views of the Committee on amending the ASIO Act to clarifying that the 'incidental power in the search warrant provision authorises access to third party premises to execute a warrant'.

4.189 The discussion paper elaborates that:

> Sections 25 and 25A of the ASIO Act currently enable an officer, in the execution of a search or computer warrant, to do any thing that is reasonably incidental to the exercise of powers under that warrant. It is

> not clear whether this incidental power includes entry to a third party's premises for the purposes of executing the search or computer warrant. Additionally, it may be necessary to enter a third party premises for the purposes of installing a surveillance device. Clarification of the scope of the incidental power would assist ASIO in executing search and computer warrants.[99]

4.190 Reponses to the proposal were not welcoming. Mr Mark Newton argued against allowing for incidental entry onto premises:

> I absolutely do not support the Incidental Entry proposal. If ASIO wants to gain access to a premises, it should get a warrant. If it then becomes apparent that they need access to a different premises, they should get a different warrant. If they can't justify the second warrant, they shouldn't enter the premises. It's that simple.[100]

4.191 Similarly, NSW Young Lawyers highlighted important issues that the discussion paper did not address in the description of the proposal:

> The proposal does not specify which third parties could be covered by such a power, whether there would be limits of proximity or otherwise in this respect. The proposal does not specify whether a warrant or any other kind of formal procedure would be necessary to enable ASIO to exercise the proposed powers.[101]

4.192 The Office of the Victorian Privacy Commissioner highlighted the human rights risks that an incidental entry proposal might raise if not properly confined and authorised by law:

> Any encroachment into the privacy of a person's domicile should be treated seriously and should only occur when absolutely necessary. This is an essential principle of human rights law, mentioned in the *International Covenant on Civil and Political Rights* (Article 17), which states that no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence.[102]

4.193 The Attorney-General's Department was asked why ASIO would need an additional power to be able to enter premises that are not related to the premises of the target person. The Department explained that the intent of the proposal was to clarify the current operation of ASIO's ability to do anything that is reasonably incidental to the exercise of powers under that warrant:

---

99 Attorney-General's Department, *Equipping Australia against emerging and evolving threats*, Discussion Paper, July 2012, p. 48.

100 Mr Mark Newton, *Submission No.87*, p. 13. See also: Office of the Victorian Privacy Commissioner, *Submission No. 109*, p. 6.

101 New South Wales Young Lawyers, *Submission No. 133*, p. 8.

102 Office of the Victorian Privacy Commissioner, *Submission No. 109,* p. 6.

> When executing search warrants, it may occasionally be necessary for ASIO officers to enter third party premises to access or exit the target premises. This may be because there is no other way to gain access – such as where the target premises are in an apartment block and entry is through common areas or adjoining premises – or due to 'emergency' and unforeseen circumstances – such as when the target person unexpectedly returns to the premises during the search.
>
> The incidental power in the warrant provisions is currently relied on where it is necessary to access third party premises. However, it would be preferable to specifically deal with the circumstances that ASIO may be permitted to access third party premises, to provide greater clarity about the detail of the authorisation.[103]

4.194 The Department further explained that entry onto third party premises would authorise entry where consent could not be obtained:

> It is ASIO's practice to approach the owner of the third party premises to seek their consent to access the premises for the purposes of executing the warrant where possible. The proposed amendment is designed to ensure clear legal authority to enter a third party premises in those circumstances where doing so is necessary but where it is not possible to obtain consent to do so, including in an 'emergency' situation where access to third party premises may be necessary to avoid detection.[104]

Committee comment

4.195 The Committee shares community concerns that the existing incidental entry power might lead to arbitrary interference with an innocent person's home or property. It is not desirable that any agency should be given an unfettered discretion to intrude into places that are not the subject of lawful investigation purely because of a geographical coincidence in being located close to a premises of interest.

4.196 However, on balance, the Committee appreciates that there may be a need for incidental entry onto premises to give effect to ASIO warrants in some limited circumstances, particularly unforeseen or emergency situations.

4.197 The Committee accepts that the proposal as clarified by the Attorney-General's Department would not lead to the arbitrary interference with an innocent person's home or property as the scheme is intended to operate with requirements of proportionality and using as little intrusion into privacy as possible.

---

103 Attorney-General's Department, *Submission No. 236*, p. 8.

104 Attorney-General's Department, *Submission No. 236*, p. 8.

Recommendation 35

The Committee recommends that the *Australian Security Intelligence Organisation Act 1979* be amended to clarify that the incidental power in the search and computer access warrant provisions includes entry to a third party's premises for the purposes of executing those warrants. However, the Committee is of the view that whatever amendments are made to facilitate this power should acknowledge the exceptional nature and very limited circumstances in which the power should be exercised.

Use of force

4.198 The Government expressly seeks the views of the Committee on amending the ASIO Act to allow reasonable force to be used at any time during the execution of a warrant, not just on entry.

4.199 The discussion paper notes that the ASIO Act allows the use of force in the execution of search, computer access and tracking device warrants but that the legislative drafting of headings to those provisions suggest that force may only be used to facilitate entry to target premises. The paper notes that, contrarily, the substantive bodies of the warrant provisions are not so limited. It is suggested that technical legislative amendments may be necessary to correct those drafting anomalies.[105]

4.200 The Attorney-General's Department explained that confusion over the limits of ASIO's use of force came about as unintended consequences of amendments to other legislation:

> A number of the ASIO warrant provisions provide that ASIO may be authorised to 'use any force that is necessary and reasonable to do the things specified in the warrant' (subsections 25(7), 25A(5A), 26B(4) and 26C(4)). These provisions are found under headings relating to 'authorisation of entry measures'. In light of changes made in 2011 to section 13 of the *Acts Interpretation Act 1901*, the headings form part of the ASIO Act. However, the terms of the use of force provision are not stated so as to limit the use of force to enter the premises. At the time these subsections were inserted into the ASIO Act, in 1999 and 2005, there does not appear to have been an intention to limit the use of force to entry, as headings were specifically excluded from the Act at that time.[106]

105 Attorney-General's Department, *Equipping Australia against emerging and evolving threats*, Discussion Paper, July 2012, p. 48.

106 Attorney-General's Department, *Submission No. 236*, p. 12.

4.201 The Human Rights Law Centre in its submission argued:

> The Government's proposal to allow ASIO to use reasonable force at any time during the execution of a warrant, not just on entry, may raise concerns in relation to the right of liberty and security of person, which is enshrined in article 9 of the ICCPR.[107]

4.202 The Human Rights Law Centre further argued that to address human rights concerns about the use of force, the law should be carefully framed:

> A human rights-based approach to the use of force can be characterised as requiring the state to act in the three stages involved in the use of force:
>
> - before the use of force – putting in place systems to protect human rights and avoid or minimise resort to force, such as proper policies and training;
> - during the use of force – requiring that force be used in a proportionate way; and
> - after the use of force – ensuring that there are accountability mechanisms in place to hold agents of the state to account for their use of force.[108]

4.203 To understand the impact of this proposal the Attorney-General's Department was asked on notice about the circumstances it envisaged that reasonable force may be used during the execution of a warrant. The Department explained:

> In addition to the possible need to use force to enter a premises, it may be necessary to use force to obtain access to a locked room or locked cabinet, or to use force to install or remove a surveillance device. The proposal is intended to ensure the power to use any force that is necessary and reasonable to do the things specified in a warrant is not read down by reference to the heading and limited to entry.
>
> The existing provision requires that the use of force must be reasonable and necessary to do what is required to execute the warrant. The ASIO Guidelines requirement of proportionality and using as little intrusion into privacy as necessary are also relevant safeguards in this context.[109]

Committee comment

4.204 The Committee is of the view that ASIO's power to use reasonable force during the execution of a search warrant should extend to all of the acts undertaken for the purpose of the execution of the warrant, not just on entry to the premises. If there is any doubt about the existence of that power, that doubt should be removed. The Committee emphasises that the purpose of this proposal is not to

107 Human Rights Law Centre, *Submission No. 140*, p. 8.

108 Human Rights Law Centre, *Submission No. 140*, p. 8.

109 Attorney-General's Department, *Submission No. 236*, p. 12.

authorise the use of force against a person, but against property in order to facilitate the conduct of the search.

Recommendation 36

The Committee recommends that the *Australian Security Intelligence Organisation Act 1979* be amended to clarify that reasonable force can be used at any time for the purposes of executing the warrant, not just on entry, and may only be used against property and not persons.

Evidentiary certificates

4.205 The Government has requested the Committee's advice on whether an evidentiary certificate regime should be introduced to protect the identities of officers and sensitive capabilities of ASIO involved in the execution of warrants under the ASIO Act.

4.206 The discussion paper proposes that the evidentiary certificate regime would be similar to those which exist under the TIA Act and *Surveillance Devices Act 2004*. This would avoid the need for ASIO to rely upon public interest immunity claims or orders obtained under the *National Security Information (Criminal and Civil Proceedings) Act 2004*.

4.207 The purpose of evidentiary certificates is to protect sensitive information, sensitive capabilities and the identities of individuals from public disclosure.

4.208 The Gilbert + Tobin Centre for Public Law was of the view that evidentiary certificates would be appropriate for ASIO warrants that authorise powers that are technological in nature:

> We accept that it would be appropriate to adopt a similar evidentiary certificate regime in respect of *some* of the warrant powers in the *ASIO Act*. That is, those warrant powers which are technological in nature.[110]

4.209 Noting that evidentiary certificates are already issued under the *Telecommunications (Interception and Access) Act 1979* for the same purposes of protecting sensitive capabilities and the identities of people involved in interception activities, NSW Young Lawyers highlighted the acceptable limits that evidentiary certificates should be allowed:

> The evidentiary certificate provision(s) sought to be introduced should not be drafted in a way that prevents a defendant from challenging the

110 Gilbert + Tobin Centre of Public Law, *Submission No. 36*, p. 15. See also: New South Wales Young Lawyers, *Submission No. 133*, p. 13 and NSW Council for Civil Liberties, *Submission No. 175*, p. 17.

> accuracy of anything said or relied on in the intercepted communication. Furthermore the certificate should not operate to preclude a defendant from being able to provide evidence inconsistent with the Crown's case in respect of the interception, or indeed any evidence that would undermine a fact in a certificate. Importantly the evidentiary certificate should not operate to preclude the operation of s 137 of the Evidence Act, which would apply where the probative value of a certificate is outweighed by the unfair prejudice it would cause to a defendant. It may be that an evidentiary certificate goes to the exercise of the court's discretion in this regard, but there will be other factors influencing the exercise of the court's discretion. Although national security will be carefully considered by the court, a certificate in this context should not be able to dictate an outcome in the face of inconsistent or doubtful evidence.[111]

Committee comment

4.210 The Committee agrees that there is a legitimate need to protect the technological capabilities of ASIO when information under warrant is eventually led in evidence as part of a prosecution. Evidentiary certificates issued under the TIA Act have been proven to effectively protect capabilities without prejudicing the rights of defendants to a fair trial.

4.211 With that being said, there ought to be a limit to the extent to which those evidentiary certificates can be utilised. The Committee does not think it appropriate that ASIO evidentiary certificates be used to prove, without challenge, the material facts in question.

4.212 This would mean that evidentiary certificates could be used to prove the validity of how information was obtained, but not whether the information itself is true. It would grossly unfair to a defendant if an element of an offence would be determined by the prosecution simply issuing a certificate to that effect.

4.213 The Committee is of the view that any future amendments for an ASIO evidentiary certificate scheme should be drafted in a way such that ultimate facts are not to be the subject of an evidentiary certificate, and that the content of such a certificate would be limited to certain technical facts removed from a fact in issue before a court.

111 New South Wales Young Lawyers, *Submission No. 133*, p. 13; See also: Gilbert + Tobin Centre of Public Law, *Submission No. 36*, p. 15 and NSW Council for Civil Liberties, *Submission No. 175*, p. 17.

Recommendation 37

The Committee recommends that the *Australian Security Intelligence Organisation Act 1979* be amended to introduce an evidentiary certificate regime to protect the identity of officers and sources. The Committee also recommends that similar protections be extended to ASIO in order to protect from disclosure in open court its sensitive operational capabilities, analogous to the provisions of the *Telecommunications (Interception and Access) Act 1979* and the protections contained in the counter terrorism provisions in the Commonwealth Criminal code.

The Committee further recommends that the Attorney-General give consideration to making uniform across Commonwealth legislation provisions for the protection of certain sensitive operational capabilities from disclosure in open court.

Matters on which the Government expressly seeks the Committee's views – Intelligence Services Act amendments

4.214 In addition to the above proposed amendments to the ASIO Act, the Government also expressly seeks the Committee's views on amending the *Intelligence Services Act 2001* (the IS Act) to:

- Add a new ministerial authorisation ground to allow the investigation of a person who is, or is likely to be, involved in intelligence or counter-intelligence activities;
- Enable the Minister of an Agency under the IS Act to authorise specified activities which may involve producing intelligence on an Australian person where the Agency is cooperating with ASIO; and
- Enable ASIS to provide training in self-defence and the use of weapons to a person cooperating with ASIS.

4.215 Australia's foreign intelligence agencies, the Australian Secret Intelligence Service (ASIS), the Defence Signals Directorate (DSD) and the Defence Imagery and Geospatial Organisation (DIGO), collect intelligence in accordance with requirements set by Government and operate under the *Intelligence Services Act 2001* (the IS Act). These agencies have identified problems arising out of the operation of the IS Act, as described in the sections which follow.

Section 9 – Ministerial authorisations

4.216 The Government expressly seeks the Committee's views on amending the Intelligence Services Act to add a new ministerial authorisation ground where the Minister is satisfied that a person is, or is likely to be, involved in intelligence or counter-intelligence activities.

4.217 The IS Act imposes strict controls on the ability of ASIS, DSD and DIGO to produce intelligence on an Australian person.

4.218 The Minister responsible for each Australian foreign intelligence agency is required to direct that the agency obtain authorisation from the Minister before undertaking activities for the purposes of producing intelligence on an Australian person.

4.219 The grounds on which a foreign intelligence agency may seek a ministerial authorisation are laid out in section 9 of the IS Act and, *inter alia*, include acting for, or on behalf of, a foreign power and activities that are, or are likely to be, a threat to 'security' (as defined in the *Australian Security Intelligence Organisation Act 1979*).

4.220 The discussion paper notes that those grounds 'do not specifically cover the situation where a person is or is likely to be involved in intelligence or counter-intelligence activities.'

> A new item could be added to the list in section 9(1A)(a) of the IS Act which would allow the Minister to give an authorisation if he or she is satisfied that the person is, or is likely to be, involved in intelligence or counter-intelligence activities.[112]

4.221 The Gilbert + Tobin Centre for Public Law argued that the necessity of the proposed new ministerial authorisation ground was unclear. It was further contended that such counter-intelligence activities would fall within the existing ministerial authorisation ground of 'activities that are, or are likely to be, a threat to security'.[113]

4.222 ASIS's submission elaborated on the discussion paper and stated that the purpose of investigating a person for intelligence or counter-intelligence activities relates to operational security:

> Operational security is about the protection of the integrity of ASIS operations from the risk of being undermined by foreign and non-State adversaries such as terrorist organisations, or reliance on inaccurate or false information. It is important to the protection of individuals, maintaining the effectiveness of ASIS and other Australian intelligence

112 Attorney-General's Department, *Equipping Australia against emerging and evolving threats*, Discussion Paper, July 2012, p. 52.

113 Gilbert + Tobin Centre of Public Law, *Submission No. 36*, pp. 19–20.

and security agencies, as well as protecting Australia's international reputation.[114]

4.223 ASIS further submitted that such necessary counter-intelligence collection would not fall within any current ground for the issuing of ministerial authorisations.[115]

Committee comment

4.224 Provided that ministerial authorisations would be subject to existing approval mechanisms, the Committee recommends that a new ministerial authorisation ground be created to enable the authorisation of activities for the purpose of producing intelligence on an Australian person who is, or is likely to be involved, in activities that will, or are likely to, undermine operational integrity.

Recommendation 38

The Committee recommends that the *Intelligence Services Act 2001* be amended to add a new ministerial authorisation ground where the Minister is satisfied that a person is, or is likely to be, involved in intelligence or counter-intelligence activities in circumstances where such an investigation would not currently be within the operational authority of the agency concerned.

Section 13A – Co-operation with intelligence agencies

4.225 The Terms of Reference state that the Government expressly seeks the Committee's views on amending the IS Act to enable the Minister of an agency to authorise specified activities which may involve producing intelligence on an Australian person or persons where an IS Act agency is cooperating with ASIO in the performance of an ASIO function.

4.226 Section 13A of the IS Act allows the Australian Secret Intelligence Service (ASIS), the Defence Signals Directorate (DSD) and the Defence Imagery and Geospatial Organisation (DIGO) to obtain ministerial authorisations to allow co-operation with other bodies in the performance of those other bodies' functions.

4.227 The discussion paper explains that the purpose of amending section 13A would be to 'better meet the intention of enabling Australia's intelligence agencies to

114 Australian Secret Intelligence Service, *Submission No. 219*, p. 3.

115 Australian Secret Intelligence Service, *Submission No. 219*, p. 3.

cooperate and assist each other in the performance of each other's functions to protect Australia and Australians'.[116]

4.228 The discussion paper further notes that there are differences in the legislative regimes which apply to ASIS, DSD and DIGO under the IS Act and to ASIO under the ASIO Act when they produce intelligence on Australians.

4.229 For example, ASIO can collect intelligence about an Australian of security interest, whether that person is in Australia or overseas, based on internal approvals, whereas ASIS would in all cases require the approval of the Minister for Foreign Affairs and the agreement of the Attorney-General to do the same thing.

4.230 The Gilbert + Tobin Centre of Public Law at the University of New South Wales criticised this proposal holding that it would 'radically alter' the requirement for IS Act agencies to obtain a ministerial authorisation before collecting intelligence on Australians:

> It would amend 13A to allow the Minister to authorise ASIS, DSD or DIGO to produce intelligence on an Australian where the agency is cooperating with ASIO in the performance of an ASIO function. In essence, it would create a parallel, and significantly broader, ministerial authorisation regime for ASIS, DSD and DIGO to produce intelligence on Australians.[117]

4.231 However, the Inspector-General of Intelligence and Security (IGIS) noted in her submission that in some instances the level of privacy protection given to an Australian would depend, not on the matter being investigated or the tools used in the investigation, but on which agency was conducting the investigation. The IGIS concluded that:

> Through my experience in the oversight of the agencies I am aware of the operational difficulties and anomalies of the current regime and can see the need for change.[118]

4.232 Rather than support the discussion paper's suggestion for dealing with the inconsistent privacy protections for Australians who are of interest to both ASIO and a foreign intelligence agency, the IGIS proposed an alternative solution.

4.233 The IGIS proposed that an equivalent common standard across the IS Act and the ASIO Act be introduced to particularly intrusive activities involving the purpose of collecting intelligence on an Australian person.

---

116 Attorney-General's Department, *Equipping Australia against emerging and evolving threats*, Discussion Paper, July 2012, p. 51.

117 Gilbert + Tobin Centre of Public Law, *Submission No. 36*, pp. 20-21.

118 Inspector-General of Intelligence and Security, *Submission No. 185*, p. 24.

4.234 The solution proposed by the IGIS was also endorsed by ASIS which considered the IGIS's proposal to be 'an elegant solution'.[119]

Committee comment

4.235 The Committee in turn agrees with the IGIS alternative solution to this particular proposal. This alternative solution would ensure that the inconsistent privacy protection would be eliminated and a consistent standard across all intelligence agencies would apply.

4.236 The Committee also notes that where ASIS proposes to collect intelligence on an Australian person to assist ASIO with its functions, this would still need to be at the request of ASIO.

Recommendation 39

The Committee recommends that where ASIO and an *Intelligence Services Act 2001* agency are engaged in a cooperative intelligence operation a common standard based on the standards prescribed in the *Australian Security Intelligence Organisation Act 1979* should apply for the authorisation of intrusive activities involving the collection of intelligence on an Australian person.

ASIS co-operation on self-defence and weapons training

4.237 The Government expressly seeks the Committee's views on amending the IS Act to enable ASIS to provide training in self-defence and the use of weapons to a person cooperating with ASIS.

4.238 The IS Act was amended in 2004 to to enable ASIS staff members and agents to receive training in the use of weapons and self-defence techniques in certain limited circumstances.

4.239 ASIS is only permitted to provide training in the use of weapons to ASIS staff members and agents. The IS Act does not currently enable ASIS staff members to participate in joint training in the use of weapons with persons who are lawfully cooperating with ASIS. This applies even though ASIS staff members are authorised to use weapons to protect such persons.

4.240 To remedy this inconsistency the discussion paper proposes that ASIS would be allowed to engage in weapons training with Commonwealth, State and Territory bodies that have their own rights to carry weapons in the course of their duties.

119 Australian Secret Intelligence Service, *Submission No. 219*, p. 1.

ASIS would also be enabled to cooperate with a limited number of approved overseas authorities in the delivery of training in self-defence and weapons.[120]

4.241 The Pirate Party of Australia submitted that allowing the Foreign Minister to approve foreign bodies to receive such training 'is deeply concerning':

> This could be used to train insurgent armies, assassination squads and even terrorists. Such activities are not justified under any circumstances and is contrary to Australia's national interest. Any tool created to fight foreign enemies can be turned upon the Australian people or at minimum be justification for our enemies to adopt the same strategies against us.[121]

4.242 Similarly, the Human Rights Law Centre expressed concern that weapons and self-defence training:

> …may pose risks to right to life contained in article 6 of the ICCPR. These proposals should have regard to human rights standards on the use of force.[122]

4.243 Contrarily, ASIS's submission asserted that the current carriage of weapons by ASIS is strictly for defensive purposes in accordance with the limitations imposed by Schedule 2 of the IS Act.[123]

4.244 Similarly, the Inspector-General of Intelligence and Security noted in her submission that:

> Generally I am satisfied that the powers afforded to ASIS under Schedule 2 of the ISA are reasonable given the high threat environments in which it conducts some of its more sensitive activities, that the numbers of individuals who are authorised to use weapons is quite small and these authorisations are not being misused. I have been briefed on the need for joint training activities and have no propriety concerns with what has been proposed. If the proposed amendments are made I will monitor their implementation.[124]

Committee comment

4.245 The Committee is of the view that as ASIS officers are permitted at law to co-operate with certain agencies and use weapons and self-defence techniques to protect themselves and their partner agencies, it is reasonable for ASIS to be able to train with those same partners in the self-defence techniques and with the weapons that are intended to save their lives.

---

120 Attorney-General's Department, *Equipping Australia against emerging and evolving threats*, Discussion Paper, July 2012, p. 54.

121 Pirate Party Australia, *Submission No. 134*, p. 31.

122 Human Rights Law Centre, *Submission No. 140*, p. 8.

123 Australian Secret Intelligence Service, *Submission No. 219*, p. 3.

124 Inspector-General of Intelligence and Security, *Submission No. 185*, p. 25.

4.246 Indeed, the lack of such joint training poses an unacceptable danger to ASIS officers and agents.

Recommendation 40

The Committee recommends that the *Intelligence Services Act 2001* be amended to enable ASIS to provide training in self-defence and the use of weapons to a person cooperating with ASIS.

Concluding comment

4.247 The Committee has carefully considered each of the reform proposals. Where the Committee has recommended draft amendments be made to the *Australian Security Intelligence Organisation Act 1979* and the *Intelligence Services Act 2001,* these amendments should first be released as an exposure draft for consultation. The Government should expressly seek the views of key stakeholders, including the Independent National Security Legislation Monitor and Inspector-General of Intelligence and Security.

4.248 Consistent with the approach recommended for reform of the TIA Act in chapter two, the Committee recommends that the reforms to the AIC legislation be subject to public consultation and Parliamentary scrutiny.

Recommendation 41

The Committee recommends that the draft amendments to the *Australian Security Intelligence Organisation Act 1979* and the *Intelligence Services Act 2001*, necessary to give effect to the Committee's recommendations, should be released as an exposure draft for public consultation. The Government should expressly seek the views of key stakeholders, including the Independent National Security Legislation Monitor and Inspector-General of Intelligence and Security.

In addition, the Committee recommends the Government ensure that the draft legislation be subject to Parliamentary committee scrutiny.