Submission No 185

Inquiry into potential reforms of National Security Legislation

Name: Dr Vivienne Thom

Organisation: Inspector General of Intelligence and Security

Inquiry into potential reforms of national security legislation

Submission to the Parliamentary Joint Committee on Intelligence and Security

Dr Vivienne Thom
Inspector-General of Intelligence and Security

23 August 2012

Contents

Executive summary

The terms of reference for this inquiry set out a range of high-level proposals to ensure that Australian law enforcement, intelligence and security agencies are equipped to effectively perform their functions and cooperate effectively given the advances in technology, the changes to the ways that technology is used, and the need for increased cooperation between agencies.

This submission acknowledges these challenges and supports the need for the legislation to be reformed to ensure that it meets current and future requirements. The submission focuses on the requirement to address the needs of national security while ensuring that any response is proportional to the threat, safeguards the privacy of individuals, and includes effective accountability and oversight regimes.

The submission highlights the following issues that arise from the proposals:

1. Proposals to simplify, streamline or reduce administrative burdens must be examined closely to ensure that any proposals to standardise tests and thresholds for the use of powers take into account the nature of each of these powers and the level of intrusiveness. While having a single test might be administratively convenient it could allow the use of more intrusive powers where less intrusive ones are appropriate.

2. 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.

3. Proposals that effectively transfer the level of decision-making from ministerial level to within an agency need to consider appropriate reviews within the agency, provide for independent scrutiny and consider external reporting requirements.

4. Proposals to increase the retention or sharing of data and personal information need to take account of the security, record-keeping and destruction requirements that are necessary to safeguard privacy and ensure that there is adequate oversight in place.

5. The proposal for ASIO to conduct authorised operations needs to ensure an appropriate balance between the requirement to protect sensitive national security information with the benefits of independent authorisation and detailed oversight and public reporting.

The Office of the Inspector-General of Intelligence and Security will continue to review activities of intelligence and security agencies to ensure that that each agency acts legally and with propriety, complies with ministerial guidelines and directives, and respects human rights. The proposed reforms are not insignificant and continuing proper oversight will be essential if Parliament and the public are to be assured that agencies use these powers appropriately. Although current funding for the office is adequate, the proposed reforms would require additional funding for the office to continue to perform its role effectively.

Background

Role of the Inspector-General of Intelligence and Security

The Inspector-General of Intelligence and Security (IGIS) is an independent statutory officer who reviews the activities of the agencies which collectively comprise the Australian Intelligence Community (AIC):

- Australian Security Intelligence Organisation – ASIO
- Australian Secret Intelligence Service – ASIS
- Defence Signals Directorate – DSD
- Defence Imagery and Geospatial Organisation – DIGO
- Defence Intelligence Organisation – DIO
- Office of National Assessments – ONA.

The Office of the IGIS is situated within the Prime Minister's portfolio and reports to the Special Minister for State for the Public Service and Integrity for administrative purposes; however, the IGIS is not subject to general direction from the Prime Minister, or other Ministers, on how responsibilities under the IGIS Act should be carried out.

The primary role and functions of the IGIS are set out in sections 8, 9 and 9A of the *Inspector-General of Intelligence and Security Act 1986* (the IGIS Act). This Act provides the legal basis for the IGIS to conduct inspections of the AIC agencies and to conduct inquiries, of varying levels of formality, as the need arises.

The overarching purpose of these activities is to ensure that each AIC agency acts legally and with propriety, complies with ministerial guidelines and directives, and respects human rights. A significant proportion of the resources of the office are directed towards on-going inspection and monitoring activities, so as to identify issues, including about the governance and control frameworks within agencies, before there is a need for major remedial action.

The inspection role of the IGIS is complemented by an inquiry function. The IGIS has own motion powers to investigate matters and conduct inquiries in addition to considering requests from Ministers and complainants. In undertaking inquiries the IGIS has strong investigative powers including the power to obtain information and can require any person to answer questions and produce relevant documents, take sworn evidence, and enter agency premises. IGIS inquiries are conducted in private because they almost invariably involve highly classified or sensitive information, and the methods by which it is collected.

Although the primary focus of the IGIS relates to the activities of the AIC agencies, an amendment to the legislation made in late 2010 allows the Prime Minister to request the IGIS to inquire into an intelligence or security matter relating to any Commonwealth agency. This provision has been used twice.

Basis of this submission

In general, it is not the role of the IGIS to comment on current or proposed government policy. However, there are some matters on which I have particular experience because of my oversight of the activities of the AIC. This experience may assist a body such as the Parliamentary Joint Committee on Intelligence and Security (the Committee) in considering legislative proposals. It follows then that my comments are focused on are whether the proposals:

- have proper accountability and oversight mechanisms
- pose risks to legality or propriety
- are consistent with human rights
- address issues that I am aware of through my examination of agency operations.

I have a particular interest in whether proposed policies place sufficient weight on maintaining the privacy of individuals, and whether proposals reflect the concept of proportionality – that is, that the means for obtaining information must be proportionate to the gravity of the threat posed and the likelihood of its occurrence. As the exercise of agency powers will in the vast majority of cases not be apparent to the subject, and as they are by their nature often highly intrusive, these powers should only be considered for use when other, less intrusive, means of obtaining information are likely to be ineffective or are not reasonably available.

I have complete access to all documents of the AIC agencies and am often proactively briefed about sensitive operations. It is my expectation that AIC agencies will be forthright in briefing me on any legal and propriety issues that arise in operational planning or activity. This familiarity with agency operations and capabilities also allows me to give my views about some of the challenges outlined in the discussion paper.[1]

My comments are necessarily limited to the agencies and type of activities that I oversight. I cannot comment on these proposed legislative amendments insofar as they relate to the activities of law enforcement agencies, or the impact upon the telecommunications sector.

In addressing the terms of reference and commenting on the proposals, this submission also sets out some of the current oversight arrangements that are in place.

While this submission mentions some international comparisons these are indicative only as I have not conducted a comprehensive comparison.

This submission is structured to address the terms of reference by addressing each piece of legislation in turn. Numbers in the headings align with the numbering in the terms of reference (ToR). Relevant parts of the discussion paper are cross referenced.

[1] *Equipping Australia against emerging and evolving threats*, http://www.aph.gov.au/Parliamentary_Business/Committees/House_of_Representatives_Committees?url=pjcis/nsl2012/additional/discussion%20paper.pdf, accessed 14 August 2012

Telecommunications (Interception and Access) Act 1979

ToR 1 – Strengthening the safeguards and privacy protections under the lawful access to communications regime in the *Telecommunications (Interception and Access) Act 1979*.

This would include the examination of:

a. the legislation's privacy protection objective
b. the proportionality tests for issuing of warrants
c. mandatory record-keeping standards
d. oversight arrangements by the Commonwealth and State Ombudsmen

The discussion paper suggests that it may be timely to revisit whether the privacy framework within the *Telecommunications (Interception and Access) Act 1979* (TIA Act) remains appropriate. It proposes 'reviewing the current checks, balances and limitations on the operation of interception powers will ensure that the privacy needs of contemporary communications users are appropriately reflected in the interception regime'.[2] The paper does not set out specific proposals as to how this is to be achieved.

The discussion paper notes that community views about access to communications may have changed along with their use and expectations of technology.[3] It is certainly true that many in the community share personal data including their current location, email content, photographs, data of personal contacts, personal interests and buying patterns. It is not clear to what extent this sharing is conscious. In my view, it would not be appropriate to extrapolate from this behaviour to conclude that there is any diminished interest in the community about privacy issues and the desirability of having limits on government collection of information. It is clear to me from complaints to my office that there is still widespread concern in the community about covert, albeit lawful, access to personal information by intelligence and security agencies and the recording and communication of that information.

In light of this, any changes to the current system of checks, balances and limitations would require compelling arguments and should be given very serious consideration.

The paper also states that consideration is being given to 'introducing a privacy focused objects clause that clearly underpins this important objective of the legislation and which guides interpretation of obligations under the Act'.[4]

Although the primary objective of the TIA Act is to prohibit interception of telecommunication or access to stored communication except in certain prescribed and regulated circumstances, the range of exceptions has grown and, if the proposals in the discussion paper are accepted by Parliament, the ways in which interception can occur will continue to expand. A privacy-focused objects clause may address this apparent imbalance and ensure that the legislation is interpreted with the emphasis on protecting communications and privacy rather than facilitating exemptions.

The terms of reference also contemplate examining the proportionality tests for the issue of warrants. As discussed under ToR 2(b) below, any proposal to rationalise the types of warrants or

[2] Discussion paper, page 23
[3] Discussion paper, page 23
[4] Discussion paper, page 23

align thresholds will need to be examined carefully to ensure that it does not compromise proportionality tests or privacy objectives.

The discussion paper addresses record keeping and accountability obligations for law enforcement agencies.[5] These agencies are required to keep records relating to documents associated with the warrants issued and particulars relating to warrant applications and each time lawfully intercepted information is used, disclosed, communicated, entered into evidence or destroyed.

Chief officers of law enforcement agencies are required to report to the Attorney-General on the use and communication of intercepted information and the Attorney-General must table a statistical report in Parliament. The Commonwealth Ombudsman oversights the use of TIA powers by Commonwealth law enforcement agencies and reporting requirements are set out in the TIA Act.

The oversight regime for ASIO is not specified in the TIA Act but, in practice, my office oversights ASIO's use of TIA powers under the inspection function in the IGIS Act. To assist the Committee in understanding the way this oversight occurs I have summarised the current inspection regime below:

Warrant related papers are examined so that we may be properly satisfied that:

- the intelligence or security case that ASIO has made in support of the application is soundly based and that all necessary legislative requirements have been met
- the individuals identified in each warrant are actually identical with, or closely linked to, persons of security interest (this is particularly relevant where a 'B-Party' telecommunications interception warrant is being sought[6])
- appropriate internal and external approvals for the request have been obtained
- the Director-General of Security has identified in writing those individuals who may execute the warrant, or communicate information obtained from the warrant
- written reports to the Attorney-General on the outcome of executed warrants are factual and provided in a timely manner
- the activity concerned did not begin before, or continue after, the period authorised by the warrant
- in the small number of cases where unauthorised collection has occurred, that prompt and appropriate remedial action has been undertaken.

In addition to our regular warrants inspections OIGIS staff undertake spot audits of ASIO's interception management systems. The purpose of these checks is to gain independent assurance that ASIO's collection activities are only occurring in accordance with the terms of a relevant warrant and related investigative authorities.

If any issues with warrants are identified, they are raised with the Director-General of Security to ensure that appropriate action is taken. Where appropriate I can also advise the Attorney-General of any concerns. I also include a summary of inspection activity in my

[5] Discussion paper, pages 25-26

[6] A so-called 'B-party' warrant allows ASIO to access the services of associates of persons of security interest see s. 9(1)(b) of the TIA Act

annual report. Generally the standard of warrant materials is very high and the error rate is low.[7]

Comprehensive record-keeping in ASIO is essential to ensure ASIO complies with the legislation and to enable effective oversight. Any proposal to change the record-keeping regime must consider the accountability requirements.

ToR 2 – Reforming the lawful access to communications regime.

a. reducing the number of agencies eligible to access communications information

I have no comment on this proposal.

b. the standardisation of warrant tests and thresholds

The discussion paper refers to four warrants for law enforcement agencies to access the content of communications and the types of offences for which a warrant can be obtained. The paper does not give much detail in relation to ASIO warrants, stating that 'ASIO's ability to intercept communications supports its functions relating to security'[8]. ASIO can currently obtain two types of telecommunication interception warrants from the Attorney-General to further its security functions: a telecommunications service warrant and a named person warrant.[9] These can include authority to intercept 'B-party' services.[10] ASIO can also obtain three types of warrants that relate to foreign intelligence including a service warrant and a named person warrant.[11] ASIO warrants automatically authorise access to stored communications.[12] Senior ASIO officers can authorise access to existing or prospective data.[13]

The tests and thresholds for each of the current ASIO warrants vary, corresponding to the intrusiveness of the warrant. For example a named person warrant is only available where a service warrant would be 'ineffective'[14] and a 'B-party' warrant is only available where ASIO has exhausted all other practicable methods or interception would not otherwise be possible.[15]

In my 2010-11 annual report I noted that, in respect of 'B-Party' warrants:

> In the course of our warrant inspections during 2010–11, OIGIS staff accessed and reviewed every 'B-Party' warrant which ASIO obtained. On the basis of these activities I am satisfied that this type of warrant continues to be used sparingly, and only where the special circumstances of each case dictated that it was appropriate and necessary.[16]

Broadly speaking, requests for warrants (other than B-Party warrants) to intercept communications in pursuit of ASIO's security function need to explain why the interception is *necessary* and why it *is*

[7] Inspector-General of Intelligence and Security Annual Report 2010-2011, pages 27-29
[8] Discussion paper, page 24
[9] See ss. 9 and 9A of the TIA Act
[10] A so-called 'B-party' warrant allows ASIO to access the services of associates of persons of security interest
[11] See s. 17(1)(e) of the ASIO Act and ss. 11A, 11B and 11C of the TIA Act.
[12] See s. 109 of the ASIO Act
[13] This 'data' does not include the content of a communication. See ss. 175 and 176 of the TIA Act
[14] See ss. 9A(1)(c) and 11B(1)(b)(iii) of the TIA Act
[15] See s. 9(3) of the TIA Act
[16] Inspector-General of Intelligence and Security Annual Report 2010-2011, page 28

reasonably suspected that the individual being targeted is engaged, or likely to be engaged, in activities prejudicial to security.[17] For access to data the threshold is only that it be *in connection with* ASIO's function.[18]

By way of comparison, the threshold that needs to be met in the UK is that a proposed activity under a warrant needs to be *necessary* in the interests of national security and the conduct *proportionate* to what is sought to be achieved[19]. In Canada the judge issuing the warrant must be satisfied the warrant is *required* to enable investigation of a threat to security and that other investigative procedures have been tried and failed or are unlikely to succeed.[20] In the US interception is only conducted under court orders and, amongst other things, for the Federal Bureau of Investigations to obtain a warrant to intercept communications the judge must be satisfied that a particular serious offence is, or is about to be, committed, the court also plays a role in the ongoing supervision of the warrant.[21]

Any proposals to standardise security warrant tests and thresholds must take into account the nature of each of these warrants and the level of intrusiveness. A single test could allow the use of more intrusive powers where less intrusive ones are appropriate.

ToR 3 – Streamlining and reducing complexity in the lawful access to communications regime.

a. simplifying the information sharing provisions that allow agencies to cooperate
b. removing legislative duplication

The discussion paper suggests that simplifying the current information-sharing provisions would support co-operative arrangements between the agencies and that further consideration could be given to the ways in which information sharing amongst agencies could be facilitated.[22] There is no specific discussion of how this proposal would affect ASIO. I am not aware of specific legislative impediments to ASIO sharing information with other agencies that I oversight but I would note that any proposal to increase the sharing of information between agencies should address the security, record-keeping and destruction requirements that are necessary to safeguard privacy.

ToR 4 – Modernising the TIA Act's cost sharing framework

a. align industry interception assistance with industry regulatory policy
b. clarify ACMA's regulatory and enforcement role

I have no comments on these proposals.

ToR 8 – Streamlining and reducing complexity in the lawful access to communications

a. creating a single warrant with multiple TI powers

Having multiple sets of warrant applications for a single investigation is administratively inconvenient for ASIO and does not necessarily provide the Attorney-General with a clear view of

[17] See ss. 9(2)(b)and 9A(2)(c) of the TIA Act
[18] This 'data' does not include the content of a communication. See ss. 175(3) and 176(4) of the TIA Act
[19] See ss. 5(2) and (3) of the Regulation of Investigatory Powers Act 2000 (UK)
[20] See s. 21 of the Canadian Security Intelligence Services Act (R.S.C, 1985, c. C-23)
[21] See for example Electronic Communications Privacy Act (18 USC ch 119)
[22] Discussion paper, page 25

the totality of proposed activities. Any proposal to streamline this and give the Attorney-General a better picture of the situation is worthy of consideration but issues of proportionality and levels of authorisation will need careful consideration.

My understanding is that currently ASIO could legally combine multiple warrant applications into a single 'bundle' for the Attorney-General to consider. However, as discussed under ToR 2 above, there are currently different thresholds and tests depending on the intrusiveness of what is proposed. The warrant application bundle would need to set out how each test was satisfied so that the Attorney-General could make a decision about the use of each warrant type.

One interpretation of the proposal in the discussion paper could be that the Attorney-General is to be asked only to agree broadly to 'interception' against a particular individual, group or premises for a specified period and to then allow the Director-General of Security or a delegated ASIO officer to decide what form that interception should take during the warrant period (including whether B-Party interception is appropriate). I note that a 'named person warrant' currently allows the Director-General of Security to add or remove services from interception coverage during the life of the warrant to enable interception of communications made by or to the specified individual.[23] Any proposal to effectively further transfer the level of decision making from Ministerial level to within an agency needs to ensure that appropriate reviews take place within the agency, make allowance for independent scrutiny and consider external reporting requirements.

If such a proposal was implemented my office would monitor whether the use of the more intrusive powers increased with time.

It is also not clear how ToR 8 combines with ToR 14 (characteristic-based interception) and whether characteristics would also be able to be varied without reference to the Attorney-General.

ToR 9 – Modernising the Industry assistance framework

a. Implement detailed requirements for industry interception obligations
b. extend the regulatory regime to ancillary service providers not currently covered by the legislation
c. implement a three-tiered industry participation model

I have no comments on these proposals.

ToR 14 – Reforming the Lawful Access Regime

a. expanding the basis of interception activities

I understand this reform to be proposing what is described in the discussion paper as a warrant regime that is 'focused on better targeting the characteristics of a communication that enable it to be isolated from communications that are not of interest'.[24]

My understanding is that the proposal would not actually enable agencies to collect communications that they cannot currently legally collect under a warrant or a combination of service, device and named person warrants. However the proposed scheme would enable the

[23] See ss. 9A and 11B of the TIA Act
[24] Discussion paper, page 25

warrant to be specific about particular characteristics of communications to be provided and thereby potentially oblige the carriers to sort those from other telecommunications traffic that could be covered by the existing warrants. I am also advised that ASIO considers the proposal would be administratively more efficient than having to potentially obtain a combination of other warrants; I have no reason to doubt this.

A key issue to be considered in this proposal is whether the warrants would be limited to interception based on the 'characteristics' described in the initial warrant (similar to a service warrant) or whether ASIO would itself be able to vary the warrant to add or remove 'characteristics' (similar to a named person warrant). If the proposal is for the latter then there needs to be certainty as to the parameters within which 'characteristics' can be added.

In the UK, for example, the relevant agency can vary the 'characteristics' upon which interception for national security purposes is undertaken but each warrant is limited to interception against one person or premises.[25] My understanding is that in the US and Canada the court order authorising the interception is to specify the person or premises and can be made by reference to a 'type of communications' but these 'types' cannot be later unilaterally be varied by the agency.[26]

If the proposed warrant is not limited to a specified person or premises and allows ASIO to add and remove 'characteristics' during the life of the warrant it would substantially change the balance between what is currently decided by the Attorney-General and what is within the authority of the Director-General of Security. Such a change should take into account the need for effective internal and external review and consider reporting requirements. If the proposed change was limited to interception against a specified person it would be more akin to the current named person warrants. [27]

A further issue is the technological capacity to actually undertake this type of 'characteristic'-based interception – including whether the carriers should be responsible for collecting, processing and delivering the communications of interest or whether the agencies should be permitted to collect and retain large amounts of information in order to find the communications of interest. It is outside my area of focus to comment on the technology, cost or burden sharing aspects of the proposal. However I would expect to see any regime include appropriate measures to ensure that the content of communications which were not the specific target of the warrant were not retained longer than necessary for 'sorting' and to ensure that such information is kept secure.

One of the important accountability and oversight requirements of the current regime is the requirement that ASIO provide a report to the Attorney-General after the expiration or revocation of each warrant. The report must include details of the telecommunications service to or from each intercepted communication was made as well as the extent to which the warrant has assisted ASIO

[25] See ss. 8(1) and 10(6) of the Regulation of Investigatory Powers Act 2000 (UK)

[26] See for example s. 21 of the Canadian Security Intelligence Services Act (R.S.C, 1985, c. C-23) and Electronic Communications Privacy Act (18 USC ch 119). However note that this submission is not based on a detailed study of the relevant overseas legislation

[27] Named person warrants can currently allow the Attorney-General to authorise interception of communications made to or from any service used by the specified person (see for example s. 9A(1)(b)(i) of the TIA Act). During the life of such a warrant the Director-General can add or remove any such services from interception coverage. However the Director-General cannot currently add a service used by a third person without a specific B-Party warrant nor can the Director-General add or remove services to be intercepted based only on proximity to a location.

in carrying out its functions.[28] This measure would be particularly important in maintaining oversight and accountability of any discretion to add new characteristics for interception.

ToR 15 – Modernising the Industry assistance framework

a. establish an offence for failure to assist in the decryption of communications
b. institute industry response timelines

I have no comments on these proposals.

c. tailored data retention periods for up to 2 years for parts of a data set, with specific timeframes taking into account agency priorities, and privacy and cost impacts

This office has an interest in the amount of information retained by ASIO and the security of that information. However, I do not have a role in relation to what information is retained by carriers. In relation to the retention of data by ASIO the 2009-10 IGIS annual report noted:

> Our interest in ASIO's retention and destruction of data arises from the Attorney–General's Guidelines which were issued to ASIO by the then Attorney–General, the Hon. Philip Ruddock MP, in October 2007 (the 2007 Guidelines). These guidelines replaced earlier guidance issued by the then Attorney–General, the Hon. Michael Duffy MP, in December 1992 (the 1992 Guidelines).
>
> Around the time that the 2007 Guidelines were issued, [the then IGIS] commented that while he was supportive of many of the changes, the office would take a close interest in ASIO's information management governance framework, with a particular focus on what data ASIO retains or destroys in future inspections.
>
> This is a difficult issue because the real significance of some (but not all) data may only become apparent when it is correlated with other data which becomes available subsequently. At the same time, ASIO is required to comply with Ministerial Guidelines which preclude ASIO from retaining high volumes of data, including significant data holdings which prove to have no relevance to organisational objectives.
>
> The 1992 Guidelines contained an express prohibition on so–called 'speculative data matching' which does not appear in the 2007 Guidelines. Instead, the 2007 Guidelines are more permissive as to what data ASIO may collect, including as 'reference' data, although this is subject to the general limitation that material be 'relevant to security'.
>
> Data sets are only one element of the information which ASIO collects. In relation to other material there is also the question of what should be done with individual records over time, particularly data which proves not to be, or to no longer be, relevant to security.
>
> Clause 11.2 of the 2007 Guidelines state that: *Where an inquiry or investigation concludes that a subject's activities are not, or are no longer, relevant to security, the records of that inquiry or investigation shall be destroyed under disposal schedules agreed to between ASIO and the National Archives of Australia.*
>
> There is a requirement on broadly similar lines in the *Telecommunications (Interception and Access) Act 1979* for intercepted material (section 14), and in the *Australian Security Intelligence Organisation Act 1979* in relation to certain records obtained under warrant (sections 31 and 34ZL).

[28] See s. 17(1) of the TIA Act

> The challenge continues to be to ensure that ASIO performs its functions to full effect and within the legislative framework.[29]

I continue to monitor ASIO's data retention and destruction policies and practices. OIGIS staff also undertake spot audits of ASIO's interception management systems. The purpose of these checks is to gain independent assurance that ASIO's data collection and retention activities are only occurring in accordance with the terms of a supporting special powers warrant and related investigative authorities.

It is not clear from the discussion paper what safeguards will be put in place if carriers have an increased obligation to retain data. In our inspection work we note that most errors relating to telecommunication intercept occur as a result of service provider error:

> During 2010–11 this office either identified, or had brought to our attention by relevant ASIO staff, nine instances in which an error had occurred in the course of telecommunications interception activities … Of these nine errors two were directly attributable to ASIO and seven occurred as the result of actions which relevant telecommunications service providers either took or failed to take.
>
> While any mistake or error is regrettable, it is important to clearly recognise that most of the errors we identified were not directly within ASIO's control ...
>
> In some of the cases where a problem was identified, a combination of technical, product delivery and administrative errors in preparation for, or subsequent to, the execution of these warrants led to collection occurring against persons who were not the intended target of these warrants, or the potential existed for such collection to occur.
>
> In one instance intercepted material which was intended to be delivered to ASIO was misdelivered to a law enforcement agency which had simultaneously obtained telecommunications warrants on the same person of interest.
>
> In several other instances appropriate preliminary checks had been undertaken by ASIO to properly identify the telecommunications services being used by persons of interest only for that information to subsequently be found to be inaccurate.
>
> In at least one case the telecommunications service which ASIO wished to intercept was disconnected in the period between when subscriber checks were undertaken and when the warrant was issued. Although ASIO should have received advice from the telecommunications service provider that the targeted service had been disconnected, this advice was not provided. After a quarantine period during which the service in question was not allocated, it was then reallocated to an individual with no connection to any matters of security interest.[30]

I note that the number of errors is low compared to the number of service intercepted and that despite best efforts administrative and technical errors will almost inevitably occur. But these observations do highlight the need for safeguards to be put in place if the obligations placed on carriers are increased.

[29] Inspector General of Intelligence and Security Annual Report 2009-2010, pages 18-19
[30] Inspector-General of Intelligence and Security Annual Report 2010-11, page 28

Australian Security Intelligence Organisation Act 1979

ToR 5 – Amending the ASIO Act to modernise and streamline ASIO's warrant provisions

a. to update the definition of 'computer' in section 25A

The discussion paper sets out the difficulties of the current provision and suggests amending the legislation 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'.[31]

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.

My understanding is that the 'mischief' that the proposed change is seeking to overcome is much narrower than the potential breadth of the proposal in the discussion paper. I am advised that the 'mischief' arises where a warrant is executed on a specific premises and the subsequent search reveals not only the computer system that was expected to be found but also additional computers that are not in some way connected to the computer system specified in the warrant. [32] The circumstances may be such that ASIO believes it is likely that the individual of security interest may have saved relevant information on the separate computer or computer systems as well as those originally covered by the warrant. In this scenario it would be administratively more convenient for ASIO to be able to obtain access to all such computers without having to obtain further warrants (which may be impractical in the time available).

The drafting of any specific legislative proposal should be able to address this type of issue without a disproportionate increase to the scope of the existing warrant powers.

a. Enabling warrants to be varied by the AG, simplifying the renewal of the warrants process and extending duration of search warrants from 90 days to 6 months.

Variation of warrants

The discussion paper notes that there is currently no provision to vary a warrant and that a new warrant is required when there is a 'significant change in circumstances'.[33] (The paper does not canvass whether s. 33(3) of the *Acts Interpretation Act 1901* applies, a provision which would generally allow a decision maker to vary an instrument that they have made.)

I note that the Attorney-General can always issue a new warrant where they consider it appropriate to do so. Further, if the 'significant change in circumstances' amounts to 'the grounds on which the warrant was issued have ceased to exist' then s. 13 of the TIA requires that the Attorney-General be advised forthwith and interception discontinued thereby contemplating that a new warrant would be required to continue interception.

---

[31] Discussion paper, page 41

[32] Warrants can currently authorise access to more than one computer or device where those computers form part of one system (see s. 25A and the definition of a 'computer' in s. 22 of the ASIO Act)

[33] Discussion paper, page 41

Duration of warrants

The discussion paper suggests extending the maximum duration of a search warrant from 90 days to six months to be consistent with other types of warrants and to provide operational benefits as there have been some instances where ASIO was unable to execute the warrant within 90 days.[34] I note that the maximum duration of a warrant was increased from 28 days to the current 90 days in 2005.[35]

In my view, it would be unusual, with the exception of one type of search, for ASIO to not be able to execute a search warrant of a premises within 90 days. 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.

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.

Noting ToR 11(a) (establishing a named person warrant for multiple ASIO Act powers) 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.

Renewal of warrants

The paper proposes a renewal process instead of a new warrant being required in instances where there has been no change to the intelligence case.[36] The paper notes that currently 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 change to either, and the assessment of the intelligence case remains unchanged'.[37]

Section 30 of the ASIO Act would seem to require ongoing monitoring of the intelligence case and need for the warrant. Section 30 requires that if 'the Director-General is satisfied that the grounds on which the warrant was issued have ceased to exist, the Director-General shall forthwith inform the Minister accordingly and take such steps as are necessary to ensure that action in pursuance of the warrant (other than the recovery of a listening device or tracking device) is discontinued'.

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.

---

[34] Discussion paper, page 42
[35] See Schedule 10 of the *Anti-terrorism Act (No. 2) 2005*
[36] Discussion paper, page 43
[37] Discussion paper, page 42

Current provisions also require ASIO to provide a report to the Attorney-General on the outcome of every warrant which is issued to it.[38] This is an important accountability step, and one that I would expect to continue if a warrant was renewed rather than a new warrant being issued.

ToR 6 – Modernising ASIO Act employment provisions:

a. providing for officers to be employed under a concept of a 'level,' rather than holding an 'office.'
b. Making the differing descriptions denoting persons as an 'employee' consistent
c. Modernising the Director-General's powers in relation to employment terms and conditions
d. Removing an outdated employment provision (section 87 of the ASIO Act)
e. Providing additional scope for further secondment arrangements

The changes relating to the 'requirement to hold an office', 'descriptors of employees in the ASIO Act', 'special provisions relating to ASIO employees' and 'modernising the Director-General's powers in relation to employment terms and conditions' appear directed at bringing ASIO employment provisions in-line with other Commonwealth government employees.[39] I have no comment on these proposals other than to note that I expect that I will continue to have general oversight of the ASIO redress of grievance procedures[40] and to deal with complaints from ASIO employees about promotion, termination, discipline and remuneration matters.[41]

The proposed change relating to secondments may significantly change what powers individuals can exercise. For example, currently an ASIS staff member 'seconded' to ASIO or who is cooperating with ASIO under a s. 13 A ISA arrangement may not undertake an activity for the purpose of producing intelligence on an Australian person without the approval of the Foreign Minister unless the staff member is on leave without pay from their 'home' agency and has been employed by ASIO. Under the proposed changes an individual might 'switch' from being an ASIS staff member, who is not permitted to produce intelligence on an Australian without ministerial authorisation, to being an ASIO staff member who is permitted to do so. Though while on 'secondment' individuals would not be able to rely on powers specific to their 'home' agency so for example ASIS staff members 'seconded' to ASIO could not carry weapons or rely on the partial immunity in s14 of the ISA.

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.

Careful consideration also needs to be given to how the proposed secondment provisions would interact with the proposed authorised operations regime (ToR 10).

My understanding is that there is no intention for 'secondments' to apply outside of Australian Government agencies (note ToR 12 – ASIO cooperating with the private sector).

[38] See s 34 of the ASIO Act
[39] Discussion paper, pages 42-43
[40] See s. 8(1)(b) of the IGIS Act
[41] See s. 8(6) of the IGIS Act

ToR 10 – Amending the ASIO Act to create an authorised intelligence operations scheme.

This will provide ASIO officers and human sources with protection from criminal and civil liability for certain conduct in the course of authorised intelligence operations.

The discussion paper states that ASIO has a requirement:

> … to covertly gain and maintain close access to highly sensitive information. This activity often involves engaging and associating closely with those who may be involved in criminal activity and therefore has the potential to expose an ASIO officer or human source to criminal or civil liability in the course of their work.[42]

An example is cited where, in the course of collecting covert intelligence in relation to a terrorist organisation, an ASIO officer or source may be open to criminal liability under the Criminal Code if they receive training from that organisation.

Intelligence and security agencies must act lawfully. It is not acceptable for agencies to operate in 'grey areas'. If Parliament decides to permit ASIO employees and sources to engage in activity that may otherwise be illegal then, in my view, there should be a carefully considered regime to regulate this.

The paper suggests that an authorised intelligence operations scheme would be 'similar to' the controlled operations scheme that operates in relation to the Australian Federal Police (AFP), the Australian Crime Commission (ACC) and the Australian Commission for Law Enforcement Integrity (ACLEI) under the *Crimes Act 1914* (Crimes Act). It is useful to briefly set out some of the key features of that scheme:

> A controlled operation is a covert operation carried out by law enforcement officers for the purpose of obtaining evidence that may lead to the prosecution of a person for a serious offence. The operation may result in law enforcement officers and other approved persons engaging in conduct that would otherwise constitute an offence. Specific and detailed external oversight and reporting mechanisms are set out in the legislation.
>
> Generally, controlled operations may be approved in the first instance by designated Senior Executive Service officers (except for major controlled operations in the AFP which must be authorised by the Commissioner or Deputy Commissioner).[43] The initial period generally cannot exceed three months. The operation may only be extended past three months up to a maximum of 24 months with the approval of a nominated member of the Administrative Appeals Tribunal (AAT).[44] This provides an independent external review of the case for an ongoing controlled operation every three months.
>
> The Chief officer of the law enforcement agency must provide detailed reports to the Minister and the Commonwealth Ombudsman.[45] The annual report of operations must be tabled in Parliament (excluding sensitive matters).

[42] Discussion paper, page 46
[43] See s. 15GF of the *Crimes Act 1914*
[44] See s. 15GT of the *Crimes Act 1914*
[45] See ss. 15HM and 15HN of the *Crimes Act 1914*

> The Commonwealth Ombudsman is required to inspect the controlled operations records of the AFP, the ACC and ACLEI at least once every twelve months.[46] The Ombudsman is required to submit a report to the Minister and the report is tabled in Parliament.[47]

The discussion paper states that any scheme for ASIO would need 'appropriate modifications'.[48] The proposal is that the Director-General of Security could issue authorised intelligence operation certificates which would provide protections from criminal and civil liability for specified conduct for a specified period (such as twelve months). The discussion paper is silent on how long any renewal could be for or what test would be applied to determine if a renewal was appropriate. Consistent with the law enforcement regime, the legislation would specify what conduct could not be authorised [49]

The ability to give itself immunity from Australian law would be a significant new power for ASIO. Engaging in activities that would otherwise be illegal carries significant risk – particularly for human sources. 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. Similarly, where such an activity was to occur outside Australia the scheme already provided for ASIS under s. 14 of the *Intelligence Services Act 2001* (the ISA) would appear relevant and the Committee may want to consider why such overseas activities could not be managed in conjunction with ASIS perhaps by way of ASIO staff and agents being made available to ASIS under the existing provisions.

I understand that there are operational impediments for ASIO in being required to operate under schemes designed for law enforcement agencies, particularly where those schemes emphasise the collection of evidence or are designed for short-term operations. I am conscious too that ASIO considers it needs to develop and maintain sources over many years.

The proposed scheme for authorised operations by ASIO is silent on the issue of independent authorisation and detailed oversight or public reporting. Notwithstanding the sensitive matters relating to national security, the Committee may want to consider whether it would be desirable to have independent external review or ministerial approval of the intelligence case at regular intervals. This external review could be provided by suitably cleared members of the AAT.[50]

The discussion paper does suggest that my office would have a role in oversight and inspection. This could be carried out under the IGIS Act but the Committee may also like to consider whether it would be preferable for the oversight and reporting regime to be set out in detail in the legislation, as is the case for controlled operations, to provide assurance that the scheme operates according to the legislation. Being notified that a scheme has been 'approved' may not necessarily be enough to maintain oversight, particularly where operations run for many years.

---

[46] See s. 15HS of the *Crimes Act 1914*
[47] See s. 15HO of the *Crimes Act 1914*
[48] Discussion Paper, page 46
[49] Discussion paper, pages 46-47
[50] Note that the *Administrative Appeals Tribunal Act 1975* (the AAT Act) and the ASIO Act make provision for the AAT to review sensitive ASIO security assessment decisions under special procedures intended to protect security – see s. 21AA of the AAT Act and Part IV, Division 4 of the ASIO Act.

Additional resources for my office could be required for my office to effectively oversight the proposed authorised operations scheme.

ToR 11 – Amending the ASIO Act to modernise and streamline ASIO's warrant provisions to:

a. 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.

As far as I am aware there is no legal reason why ASIO cannot currently 'bundle' warrant applications so that the Attorney-General is asked to authorise the use of multiple powers in relation to a specific individual at the same time. Such an arrangement would, however, require the Attorney-General to consider the threshold and case for each individual power. See my comments in respect of ToR 8(a) – single TI warrants.

The discussion paper suggests that a single warrant could be issued covering all ASIO warrant powers where the relevant legislative thresholds are satisfied rather than requiring multiple warrants for an individual.[51]

The paper does not explain how the current different legislative tests and thresholds for the issuing of different types of warrants would be reconciled in a single warrant process or whether there is an intention to effectively transfer the decision as to what powers should be exercised from the Attorney-General to the Director-General of Security. The different types of warrants involve different activities and consequently different levels of intrusiveness (see also my comments above in respect of ToR 2(b) – standard TI warrant threshold). While a standardisation of tests and thresholds may be administratively convenient I would be concerned if there was, in effect, a lowering of the thresholds without careful justification of the need to do this.

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 – see my comments in respect of ToR 2(b) and 8(a) above.

b. Align surveillance device provisions with the *Surveillance Devices Act 2004*

The discussion paper proposes aligning the surveillance device provisions in the ASIO Act with the more modern *Surveillance Devices Act 2004* to overcome impediments to cooperation with law enforcement partner agencies.[52]

While cooperation is desirable, it is not clear what the specific changes would be. Any changes must also consider external review and oversight mechanisms. I note there are substantial differences between the current ASIO regime and warrants under the Surveillance Devices Act. For example Surveillance Device Act warrants are issued by eligible judges or nominated members of the AAT.[53] There are also specific provision in the Surveillance Devices Act relating to reporting and oversight by the Ombudsman.[54]

[51] Discussion paper, page 47
[52] Discussion paper, page 47
[53] See s. of the *Surveillance Devices Act 2004*
[54] See ss. 49 to 61 of the *Surveillance Devices Act 2004*

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'[55] – then this is a more focussed proposal that does not raise propriety concerns.

c. Enable the disruption of a target computer for the purposes of a computer access warrant

The ASIO Act 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.[56] The discussion paper suggests an amendment such that the prohibition would not apply to activity that is proportionate to what is necessary to execute the warrant.

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.

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. There should be appropriate review and oversight mechanisms with particular attention to the effect of any disruption on third parties.

d. Enable person searches to be undertaken independently of a premises search

The ASIO Act does not provide specific person search powers for ASIO, although a warrant to search a premises can also specify, if appropriate, that the warrant provides the 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 security matters. This needs to be specified in the warrant.[57]

The discussion paper states that 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. The paper proposes addressing 'the existing limitation' by enabling ASIO to request a warrant to search a specified person. [58]

It seems that the current provisions consider the search of the person as incidental to the search of the premises. A proposal to introduce a warrant to search a specified person is not an extension of the existing power to search premises but is rather a proposal to introduce a new class of warrant. This will require careful consideration of the restrictions and conditions that should apply.

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.

---

[55] See s. 22 of the ASIO Act
[56] Discussion paper, page 48
[57] See s. 25 of the ASIO Act
[58] Discussion paper, page 48

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, were possible, such searches are undertaken by law enforcement officers who have specific training in this regard.

e. Establish classes of persons able to execute warrants

The discussion paper proposes that the Direct-General of Security should be able to specify a class of person to execute a warrant rather than named individuals. 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 ToR 11(d) there may be cases where the best qualified officers to conduct a particular search are law enforcement officers.

ToR 12 – Clarifying ASIO's ability to cooperate with the private sector.

The discussion paper proposes amending s 19(1) of the ASIO Act to avoid any doubt about ASIO's ability to cooperate with the private sector.[59]

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.

ToR 13 – Enabling ASIO to refer breaches of section 92 of the ASIO Act to authorities

I have no comment on this proposal.

ToR 17 – Amending the ASIO Act to modernise and streamline ASIO's warrant provisions:

a. Using third party computers and communications in transit to access a target computer under a computer access warrant

The discussion paper proposes amending the ASIO Act to enable a third party computer or communication in transit to be used by ASIO to lawfully access a target computer.[60]

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.[61] This appears to be an appropriate safeguard.

[59] Discussion paper page 49
[60] Discussion paper, page 50
[61] See s. 9(3) of the TIA Act

b. Clarifying that the incidental power in the search warrant provision authorises access to third party premises to execute a warrant

The discussion paper proposes 'clarification' of the scope of the powers incidental to the execution of a search or computer warrant in respect of entry to a third party's premises.[62]

Any such change must ensure that the impact on the third party, including privacy implications as well as the potential for any damage to property, is considered carefully. If this entry is pre-planned – for example as access to a premises – it could be specified and authorised in the warrant documentation.

My understanding is that the operational driver behind the proposed amendment is to allow for an unplanned or unforseen emergency exiting by ASIO officers who are covertly executing a warrant. This limitation could to be set out in the legislation.

c. Clarifying that reasonable force may be used at any time during the execution of a warrant, not just on entry.

The current drafting of the ASIO Act suggest that the use of force is limited to authorisation of entry measures.[63] The discussion paper suggest that 'the provisions relating to the use of force are not limited in such a way' and proposes an amendment to 'correct' this is a 'drafting anomaly'.[64]

It is not clear whether this is in fact a 'drafting anomaly' but, in any event, to broaden the use of force to include *all* warranted activities could enable ASIO to use force in conducting person searches.

My understanding is that the policy intention behind the proposed amendment relates only to secondary use of force by ASIO officers against 'things' when conducting premises searches. For example force may be required to initially get through the front door and further force may be needed to, for example, open a locked drawer. I understand that there is no intention to authorise ASIO officers to use force to conduct person searches.

From time to time my office has received complaints about searches of premises. This is a highly intrusive activity and I will continue to monitor ASIO's activities in this regard.

d. Introducing an evidentiary certificate regime.

I have no comments on this proposal

[62] Discussion paper, page 50
[63] See, for example, heading above s. 25(7) of the ASIO Act
[64] Discussion paper, page 50

Intelligence Services Act 2001

ToR 7 – Clarifying the DIGO's authority to provide assistance to approved bodies.

The discussion paper proposes amendments to DIGO's function under s. 6B(e) of the ISA to ensure that DIGO has clear legislative support to undertake its geospatial and imagery related functions, and include an express reference to specialised imagery and geospatial technologies.[65]

I do not need to comment on what might have been the original parliamentary intention or whether there is actually any ambiguity in the current legislation, but I will note that I have no propriety concerns with the view that DIGO should be able to provide Commonwealth and State authorities and other approved bodies, assistance in relation to the production and use of all imagery and geospatial products or assistance with the use and application of specialised imagery and geospatial technologies. 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 ISA to any disclosure of intelligence about an Australian person, regardless of which function the intelligence was collected under.

ToR 18 – Amending the *Intelligence Services Act 2001*

The ministerial authorisations scheme ensures appropriate ministerial oversight of the most sensitive functions of the foreign intelligence agencies including setting out the limited circumstances in which it is permissible for those agencies to undertake an activity for the specific purpose of producing intelligence on an Australian person. Two changes are proposed.

a. 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.

The first change concerns the addition of a new provision which would allow the Minister to authorise the production of intelligence on an Australian person who is, or is likely to be, involved in intelligence or counter-intelligence activities.[66] The proposed change is consistent with the structure of existing approval mechanisms. I have no propriety concerns with the proposed change. Oversight of the use of such a provision could be managed in the same way that this office inspects the exercise of other actions based on similar approvals by the relevant Minister.

b. Enable the Minister of an agency under the ISA to authorise specified activities which may involve producing intelligence on an Australian person or persons where the agency is cooperating with ASIO in the performance of an ASIO function pursuant to a section 13A arrangement. A ministerial authorisation will not replace the need to obtain a warrant where one is currently required.

ASIO collects intelligence relevant to 'security'.[67] ASIS collects intelligence about the capabilities, intentions or activities of people or organisations outside Australia.[68] While the statutory functions

[65] Discussion paper, page 44
[66] Discussion paper, pages 51-52
[67] See s. 17(1)(a) of the ASIO Act
[68] See ss. 6(1)(a) and (b) of the ISA

of ASIO and ASIS overlap significantly, the mechanisms to ensure ministerial control over the production of intelligence on Australian persons differ substantially.

ASIO can collect intelligence about an Australian of security interest who is 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.[69] This means that, in some instances, the level of protection for the privacy of individual Australians may depend on which agency is collecting the intelligence. 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.

The discussion paper does not specify what types of 'activities' could be approved, whether they may only occur overseas, which minister(s) would give the approval, how long the approval would be for, or on what basis it could be approved or renewed. However, my understanding is that intention is that the Minister for Foreign Affairs could issue authorisations to 'pre-approve' ASIS conducting an 'operation' that may involve collecting intelligence on any Australian provided that activity is being done for the purpose of assisting ASIO.

If an 'activity' is to be defined by reference to a particular operation there would be scope for the approvals to become quite broad. As a result it is possible that such authorisations could, in effect, become an almost blanket approval for ASIS, like ASIO, to produce intelligence on Australian persons for any purposes relating to security without further specific approval. Indeed, unless a broad range of activities were pre-approved and renewed on an ongoing basis the current difficulties with delay in obtaining an authorisation may continue.

I note that the proposal does include a reference to the need to obtain an individual ministerial authorisation where it could be sought. While, in principle, this is a good idea and seeks to maintain some of the current system of safeguards, it may have unintended consequences that could result in a continuation of current operational issues and make the scheme difficult to effectively oversight.

The existing threshold for a ministerial authorisation in security related cases is that the Minister must be satisfied that an individual is, or is likely to be, involved in an activity that is, or is likely to be, a threat to security.[70] This is not a high threshold. However my experience is that the cases that ASIS usually pursues are the more serious ones which go well above this threshold.

If the proposal requires a ministerial authorisation to be sought at renewal whenever this relatively low threshold is met, ASIS will need to ensure that each time an 'activity authority' is renewed every case is assessed to determine whether, for each individual, the legal threshold for an individual authorisation has been met. ASIS would have to stop collecting intelligence while an authorisation is obtained at the exact time it is assessed that the individual is of potential security interest. This problem may be particularly apparent where the individual comes to attention only towards the end of the authorisation period.

[69] See ss. 8(1)(a)(i) and 9(1A)(b) of the ISA. Note that in any case if the activity was in Australia and required a warrant it could not be undertaken by either agency in the absence of a warrant. This includes, for example, if ASIO was to obtain intelligence about an Australian who is overseas by intercepting the calls made by that person to another person in Australia via the Australian telecommunications network.

[70] See s. 9(1A)(a)(iii) of the ISA

It is possible that the problem of the inconsistency of legal frameworks outlined above could be addressed in a different way that might lead to a more consistent outcome. For activities inside Australia all of the agencies are currently bound by the common standard that requires ministerial approval (in the form of a warrant) or some other form of approval under legislation (for example, an authority to collect telecommunications data) for particularly intrusive activities. The Committee might want to consider whether this standard should be maintained to protect the privacy of *Australian persons* wherever they are. It may be appropriate to require that any intelligence or security agency that is undertaking an activity for the purpose of producing intelligence on an Australian person overseas should obtain the equivalent to the approval that ASIO would require if the activity was conducted in Australia (so for example Ministerial level approval for actions that would require a warrant and equivalent approvals for other actions that ASIO needs to have authorised under legislation).

So, for example, under such a scheme if DSD was to intercept the communications of an Australian person outside Australia a ministerial authorisation might be required. If ASIS or ASIO was to use a listening device to collect intelligence on an Australian outside Australia a ministerial authorisation might be required. However, if ASIS or ASIO was to ask an agent what they know about an Australian person who may be allegedly involved in terrorist activity or to task an agent to try to find out if any Australian persons are present at a terrorist training camp, specific ministerial authorisation would not be required.

My office would be required to monitor any changes to ministerial authorisation requirements and to continue to pay very close attention to any activity against an Australian person. In both my 2009-10 and 2010-11 annual reports I have noted that there is overall a very high level of compliance by the agencies with ministerial authorisation and warrant requirements.

b. Enable ASIS to provide training in self-defence and the use of weapons to a person cooperating with ASIS.

Currently ASIS cannot provide training in the use of weapons to individuals who are not ASIS staff members. This restricts joint training exercises. The discussion paper proposes amendment to allow ASIS to cooperate in training with law enforcement and military personnel as well as a limited number of approved overseas authorities.[71]

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.

[71] Discussion paper, page 54

Telecommunications Act 1997

ToR 16 – Amending the Telecommunications Act to address security and resilience risks

1. Amending the Telecommunications Act to address security and resilience risks posed to the telecommunications sector. This would be achieved by:
   a. by instituting obligations on the Australian telecommunications industry to protect their networks from unauthorised interference
   b. by instituting obligations to provide Government with information on significant business and procurement decisions and network designs
   c. Creating targeted powers for Government to mitigate and remediate security risks with the costs to be borne by providers
   d. Creating appropriate enforcement powers and pecuniary penalties

I have no comments on these proposals