Inquiry into comprehensive revision of the *Telecommunications (Interception and Access) Act 1979*

Submission to the Senate Legal and Constitutional Affairs References Committee

Dr Vivienne Thom
Inspector-General of Intelligence and Security

February 2014

Executive Summary

The terms of reference for this inquiry focus on a range of issues to be addressed by a comprehensive revision of the *Telecommunications (Interception and Access) Act 1979* (TIA Act). The terms of reference have regard to relevant recommendations made by the Parliamentary Joint Committee on Intelligence and Security (PJCIS) in its May 2013 report *Inquiry into Potential Reforms of Australia's National Security Legislation*.

This submission acknowledges these challenges and supports the need for the TIA Act to be reformed to ensure that it meets current and future requirements. The submission focuses on the requirement for telecommunications interception and access 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 Office of the Inspector-General of Intelligence and Security will continue to review the telecommunications interception and access activities of ASIO to ensure that it acts legally and with propriety, complies with ministerial guidelines and directives, and respects human rights.

The proposed reforms are not insignificant and, as the PJCIS has noted and recommended, continuing proper oversight will be essential if Parliament and the public are to be assured that agencies use these powers appropriately. If the Senate Legal and Constitutional Affairs Committee (the Committee) proposes changes that increase the role of the Office of the Inspector General of Intelligence and Security, it might also consider the consequential resource impact on the Office, noting that IGIS must sustain its other legislated roles as well.

Background

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[1]
- 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 currently has twelve staff. The IGIS is not subject to general direction from the Prime Minister, or other relevant Ministers, on how responsibilities should be carried out.

The overarching purpose of the activities of the IGIS 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.

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 ASIO. This experience may assist the Committee in the current inquiry. My comments are focused largely on 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 ASIO's operations.

This submission is structured to address the relevant recommendations from the PJCIS inquiry report, as referred to in point b. of the Committee's terms of reference for this inquiry.

[1] The 2013 Defence White Paper announced changes to the names of the Defence Signals Directorate and the Defence Imagery Geospatial Organisation to the Australian Signals Directorate and Australian Geospatial-Intelligence Organisation respectively. At the time of writing this submission these changes had not been incorporated into legislation.

Submission addressing the recommendations relating to the TIA Act from the PCJIS *Inquiry into the Potential Reforms of Australia's National Security Legislation*

Recommendation 1

The Committee recommends the inclusion of an objectives clause within the *Telecommunications (Interception and Access) Act 1979*, which:

- **expresses the dual objectives of the legislation –**
  ⇒ to protect the privacy of communications;
  ⇒ to enable interception and access to communications in order to investigate serious crime and threats to national security; and
- **accords with the privacy principles contained in the *Privacy Act 1988*.**

Although the primary objective of the Act is to prohibit interception of telecommunications or access to stored communications except in certain prescribed and regulated circumstances, the range of exceptions has grown and may continue to expand.

An objectives clause along the lines proposed recognises the need to balance the privacy of users of the telecommunications services in Australia with ASIO's investigative requirements for security and foreign intelligence purposes. The privacy principles in the *Privacy Act 1988* would provide a useful benchmark reflecting community expectations.

Recommendation 2

The Committee recommends the Attorney-General's Department undertake an examination of the proportionality tests within the *Telecommunications (Interception and Access) Act 1979* (TIA Act). Factors to be considered in the proportionality tests include the:

- **privacy impacts of proposed investigative activity;**
- **public interest served by the proposed investigative activity, including the gravity of the conduct being investigated; and**
- **availability and effectiveness of less privacy intrusive investigative techniques.**

The Committee further recommends that the examination of the proportionality tests also consider the appropriateness of applying a consistent proportionality test across the interception, stored communications and access to telecommunications data powers in the TIA Act.

The IGIS has a particular interest in whether proposed changes 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.

The exercise of ASIO's TIA powers will, almost always, not be apparent to the subject. Further, the use of ASIO's powers is not usually subject to scrutiny by a court or through legal processes as can often occur for law enforcement agencies. As ASIO's use of TIA powers is 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.

Any proposal to apply a consistent proportionality test will need to be examined carefully to ensure that it does not compromise privacy objectives.

Recommendation 3

The Committee recommends that the Attorney-General's Department examine the *Telecommunications (Interception and Access) Act 1979* with a view to revising the reporting requirements to ensure that the information provided assists in the evaluation of whether the privacy intrusion was proportionate to the public outcome sought.

Relevant 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.

ASIO's use of TIA powers are not included in the Attorney-General's report to Parliament. The Attorney-General's Department could consider whether the public reporting regimes of similar organisations overseas might provide useful models of alternative reporting approaches.

The oversight regime for ASIO is not specified in the TIA Act. 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.

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)[2]
- 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, including through carrier error, prompt and appropriate remedial action has been undertaken.

Warrant related papers are examined *after* the Attorney-General has authorised the activity. If any issues with warrants are identified, they are raised with the Director-General of Security to ensure that remedial action is taken and that processes are reviewed to prevent future errors. Where appropriate I can also advise the Attorney-General of any concerns. I also include a

[2] 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

summary of inspection activity in my annual report. Generally the standard of warrant materials is high and the error rate is low.

Comprehensive recordkeeping in ASIO is essential to ensure ASIO complies with the legislation and to enable effective oversight. Any proposal to change the recordkeeping regime should enhance accountability requirements.

Recommendation 4

The Committee recommends that the Attorney-General's Department undertake a review of the oversight arrangements to consider the appropriate organisation or agency to ensure effective accountability under the *Telecommunications (Interception and Access) Act 1979*.

Further, the review should consider the scope of the role to be undertaken by the relevant oversight mechanism.

The Committee also recommends the Attorney-General's Department consult with State and Territory ministers prior to progressing any proposed reforms to ensure jurisdictional considerations are addressed.

I can comment only on the oversight arrangements of the use of TIA powers by ASIO. If any revision led to an increased role for this office, additional resources could be required for the Office to continue performing this and other existing oversight roles effectively.

Recommendation 5

The Committee recommends that the Attorney-General's Department review the threshold for access to telecommunications data. This review should focus on reducing the number of agencies able to access telecommunications data by using gravity of conduct which may be investigated utilising telecommunications data as the threshold on which access is allowed.

I note that this recommendation seems to relate to law enforcement agencies only. I have no comment on this recommendation.

Recommendation 6

The Committee recommends that the Attorney-General's Department examine the standardisation of thresholds for accessing the content of communications. The standardisation should consider the:

- **privacy impact of the threshold;**
- **proportionality of the investigative need and the privacy intrusion;**
- **gravity of the conduct to be investigated by these investigative means;**
- **scope of the offences included and excluded by a particular threshold; and**
- **impact on law enforcement agencies' investigative capabilities, including those accessing stored communications when investigating pecuniary penalty offences.**

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. These can include authority to intercept 'B-party' services. ASIO can also obtain three types of warrants that relate to foreign intelligence, including a service warrant and a named person warrant. ASIO security function warrants automatically authorise

access to stored communications. Senior ASIO officers can authorise access to existing or prospective data.[3]

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 and a B-party warrant is only available where ASIO has exhausted all other practicable methods or interception would not otherwise be possible.

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 reasonably suspected* that the individual being targeted is engaged, or likely to be engaged, in activities prejudicial to security. For access to data the threshold is only that it be *in connection with* ASIO's function.[4]

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.[5] 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.[6] In the US interception is only conducted under court orders. For the Federal Bureau of Investigations to obtain a warrant to intercept communications the judge must be satisfied that a particular serious offence has been, or is about to be, committed. The court also plays a role in the ongoing supervision of the warrant.[7]

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.

Recommendation 7

The Committee recommends that interception be conducted on the basis of specific attributes of communications.

The Committee further recommends that the Government model 'attribute based interception' on the existing named person interception warrants, which includes:

- **the ability for the issuing authority to set parameters around the variation of attributes for interception;**
- **the ability for interception agencies to vary the attributes for interception; and**
- **reporting on the attributes added for interception by an authorised officer within an interception agency.**

In addition to Parliamentary oversight, the Committee recommends that attribute based interception be subject to the following safeguards and accountability measures:

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

- **attribute based interception is only authorised when an issuing authority or approved officer is satisfied the facts and grounds indicate that interception is proportionate to the offence or national security threat being investigated;**
- **oversight of attribute based interception by the ombudsmen and Inspector-General of Intelligence and Security; and**
- **reporting by the law enforcement and security agencies to their respective Ministers on the effectiveness of attribute based interception.**

I understand this recommendation aims to enable better focussing on targeting the characteristics of a communication that enable it to be isolated from communications that are not of interest. If implemented appropriately this could serve to improve the protection of privacy. Possible attributes include, but would not be limited to, the time or location of a communication, or a unique identifier for the service or account.

My understanding is that the proposal would not actually enable an agency to collect communications it cannot currently legally collect under a single warrant or a combination of service, device and named person warrants. However the proposed scheme would enable the 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). A proposal for the latter would require definition 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.[8] My understanding is that in the US and Canada the court order authorising the interception is required 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.[9]

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.[10]

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

[9] 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

[10] 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

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, but I would note that any significant change to the current regime could, at least initially, result in more errors by carriers. 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 would not be retained longer than necessary for 'sorting', to ensure that such information is kept secure, and to provide for appropriate levels of oversight for carriers.

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 which each intercepted communication was made, as well as the extent to which the warrant has assisted ASIO in carrying out its functions. This measure would be particularly important in maintaining oversight and accountability of any discretion within ASIO to add new characteristics for interception.

Recommendation 8

The Committee recommends that the Attorney-General's Department review the information sharing provisions of the *Telecommunications (Interception and Access) Act 1979* to ensure:

- **protection of the security and privacy of intercepted information; and**
- **sharing of information where necessary to facilitate investigation of serious crime or threats to national security.**

I am not aware of specific legislative impediments to ASIO sharing information with other AIC agencies, but I would note that any proposal to increase the sharing of information between agencies would need to address the security, record-keeping and destruction requirements that are necessary to safeguard privacy.

Recommendation 9

The Committee recommends that the *Telecommunications (Interception and Access) Act 1979* be amended to remove legislative duplication.

I have no comment on this recommendation.

Recommendation 10

The Committee recommends that the telecommunications interception warrant provisions in the *Telecommunications (Interception and Access) Act 1979* be revised to develop a single interception warrant regime.

---

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.

The Committee recommends the single warrant regime include the following features:
a single threshold for law enforcement agencies to access communications based on serious criminal offences;

- **removal of the concept of stored communications to provide uniform protection to the content of communications; and**
- **maintenance of the existing ability to apply for telephone applications for warrants, emergency warrants and ability to enter premises.**

The Committee further recommends that the single warrant regime be subject to the following safeguards and accountability measures:

- **interception is only authorised when an issuing authority is satisfied the facts and grounds indicate that interception is proportionate to the offence or national security threat being investigated;**
- **rigorous oversight of interception by the ombudsmen and Inspector-General of Intelligence and Security;**
- **reporting by the law enforcement and security agencies to their respective Ministers on the effectiveness of interception; and**
- **Parliamentary oversight of the use of interception.**

This recommendation is directed to providing a single warrant regime with a single threshold for law enforcement agencies. It is not clear how this recommendation would apply to the use of TIA powers by ASIO.

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 the totality of proposed activities. Any proposal to streamline this and give the Attorney-General a better picture of the situation is worth pursuing 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 at the moment there are 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.

I note that the recommendation contains the safeguard that the issuing authority (the Attorney-General in the case of ASIO) must be satisfied that the facts and grounds indicate that interception is proportionate to the national security threat being investigated.

The Attorney-General might be requested 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). This would effectively transfer the level of decision making from Ministerial level to within ASIO. Any such proposal would need 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 have an interest in whether the use of the more intrusive powers increased with time.

Recommendations 11 – 17

These recommendations relate to telecommunications providers. I have no comments on the recommendations.

Recommendation 18

The Committee recommends that the *Telecommunications (Interception and Access) Act 1979* (TIA Act) be comprehensively revised with the objective of designing an interception regime which is underpinned by the following:

- **clear protection for the privacy of communications;**
- **provisions which are technology neutral;**
- **maintenance of investigative capabilities, supported by provisions for appropriate use of intercepted information for lawful purposes;**
- **clearly articulated and enforceable industry obligations; and**
- **robust oversight and accountability which supports administrative efficiency.**

The Committee further recommends that the revision of the TIA Act be undertaken in consultation with interested stakeholders, including privacy advocates and practitioners, oversight bodies, telecommunications providers, law enforcement and security agencies.

The Committee also recommends that a revised TIA Act should be released as an exposure draft for public consultation. In addition, the Government should expressly seek the views of key agencies, including the:

- **Independent National Security Legislation Monitor;**
- **Australian Information Commissioner;**
- **ombudsmen and the Inspector-General of Intelligence and Security.**

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

I note this recommendation recognises both the importance of clear protection for the privacy of communications as well as the need for robust oversight. I support the explicit requirement for consultation with my office and will cooperate actively if the revision proceeds as proposed.

If any revision proposed an increased role for this office, additional resourcing would be required to perform this oversight role effectively.