REFLECTIONS OF A FORMER INSPECTOR-GENERAL OF INTELLIGENCE AND SECURITY

Dr Vivienne Thom*

In this paper I will explain why intelligence and security agencies require a specialised oversight agency and how the office provides assurance that intelligence agencies act properly, and will close by setting out some challenges for the future for oversight.

Why does the intelligence community require particular oversight?

If any of you have an interaction with a government agency such as Centrelink, the Australian Tax Office (ATO) or a law enforcement agency, you will usually know what is happening. You will know how to make a complaint, you will know your rights to review, you will know when you can complain to the Ombudsman or seek review by a tribunal. You will know what information is collected about you and how you can seek access to it.

But as a general rule you will not know if you have become of interest to an intelligence agency. You will not know what is done with any data or intelligence information which might have been gathered about you. Generally, intelligence agencies are not subject to the Freedom of Information (FOI) regime and the agency might not return your phone calls or e-mails.

Individual liberties and human rights are best achieved in a secure society and there are good reasons why intelligence agencies should have some exemptions. But these agencies cannot be completely without external scrutiny.

In the last two years or so the Parliamentary Joint Committee on Intelligence and Security (PJCIS) has conducted a number of inquiries into reforms of national security legislation. The Committee's reports have consistently stressed that any extra powers given to the intelligence agencies must always be balanced by appropriate safeguards for the privacy of individuals. In other words, the current view is that agencies will only be given additional powers – or be allowed to retain the ones they already have – if there is a rigorous oversight regime in place. The answer requires going back 30 years or so to understand the history of why the office of the Inspector-General of Intelligence and Security (IGIS) was established.

Ten of those years can be summarised in one sentence. The Murphy Raid, the 'Combe-Ivanov affair' and the 'Sheraton Hotel incident', as they became known in the 1970s and 80s, fuelled a perception that the intelligence agencies were running out of control. (The descriptors 'raid', 'affair' and 'incident' are fair indicators that these were notorious events.)

Next followed the significant reforms to the Australian Intelligence Community (AIC) that arose from the ensuing Hope Royal Commissions.

---

* Dr Vivienne Thom's term as the Inspector-General of Intelligence and Security came to an end on 30 June 2015. She was formerly Deputy Commonwealth Ombudsman and the Chief Executive Officer of the Australian Mint.

As Hope noted:

> .. any secret service poses problems for democracy. If not properly controlled such organisations easily become a law unto themselves or political tools of the government. With this capacity for misuse they represent at least a potential menace to the values they are intended to protect.

The position of the IGIS was an important part of Hope's legacy and was intended to address these concerns that these agencies were not sufficiently under ministerial control, not subject to enough scrutiny, and were being improperly caught up in domestic politics.

The role is independent; the Inspector-General is a statutory officer, the office is part of the Prime Minister's portfolio but not part of the Department of the Prime Minister and Cabinet. It has separate appropriation and appoints its own staff. The IGIS is not subject to direction from the Prime Minister or other ministers on how duties are to be carried out.

The IGIS is required to look beyond matters of strict legality and comment on propriety. The IGIS Act does not provide a definition of the term 'propriety'. I found this to be a good thing. While administrative law experts might angst over the difference between judicial and merits review the IGIS has scope to look at almost anything under 'propriety'

In a recent report the NZ IGIS had a good definition. She said:

> The standard of propriety encompasses whether the agency acted in a way that a fully informed and objective observer would consider appropriate and justifiable in the circumstances.

The key part here is that the IGIS must be fully informed and objective: this is not the same as the pub test. The IGIS must have a good understanding of the national security environment and of relevant intelligence and risks.

Earlier in 2015, Duncan Lewis, the head of ASIO explained:

> ASIO's role is to investigate and provide advice on threats to Australia's national security. In doing this work, we are very mindful of the importance of using the least intrusive method of collection, proportionate to the level of threat.

This test of proportionality applies to all of the intelligence agencies and the IGIS looks to ensure it is applied. For example, in inspections the office reviews ASIO's authorisations and access to telecommunication data to ensure that the level of intrusion is proportionate to the level of threat.

While the test of propriety is broad there are limits to the role of the IGIS: it is generally not the function of the IGIS to comment on government policy. There have been calls to examine alleged payments to people smugglers or allegations about spying for treaty negotiations. Setting aside any questions of legality and propriety about these allegations, there are also fundamental issues here of government policy, and on that the IGIS is silent. The type of oversight activity I am talking about is compliance with laws and government policy. It is generally not whether the policy itself is a good idea.

The office also looks at human rights issues

There has been some recent media coverage on the question of the passage of information to foreign authorities about Australian foreign fighters.

Intelligence agencies cannot only work with friendly democracies. Dangerous threats often come from dangerous people in dangerous places. If an agency receives credible

intelligence that might save lives, they need to act. They would normally want to share the intelligence with a foreign authority if that authority is in a position to act on it.

But they also have a duty to do what they can to ensure that a partner service will respect human rights. If they hold back and do not pass on that intelligence, lives may be lost that could have been saved. This is a real, constant, operational dilemma.

It is not only the possibility of torture that is relevant to human rights questions. Australia and its intelligence agencies are involved in military conflicts where the laws of armed conflict can also apply.

What is the role of the IGIS in these human rights issues? The office reviews the relevant policy guidance provided to agency staff and, in practice, how agencies manage the risks when making decisions relating to exchanging intelligence information with foreign authorities.

Inquiries

The IGIS can conduct inquiries using coercive powers – often referred to as 'Royal Commission' powers. Oral evidence can be compelled and taken on oath or affirmation. The IGIS can require the production of records and access agency premises.

The IGIS can initiate inquiries— sometimes as a result of a complaint - or matters can be referred by a Minister or the Prime Minister.

The subject matters can be broad: in my term the Prime Minister referred the matter of the actions of Australian government agencies in relation to the arrest and detention in Pakistan, Egypt, Afghanistan and Guantanamo Bay of Mr Mamdouh Habib.

In other inquiries I looked at:

- allegations of inappropriate vetting practices by the Defence Security Authority;
- the management of the case of a particular Egyptian irregular maritime arrival who was the subject of an Interpol red notice; and
- the provision of weapons and the training in and use of weapons and self-defence techniques by the Australian Secret Intelligence Service.

Complaints

The office also receives and investigates complaints from members of the public. The largest number by far is the time taken by the Australian Security Intelligence Organisation (ASIO) to conduct security assessments for visas but there is also a fair spread of other complaints. For example, complaints about the behaviour of officers during the execution of ASIO search warrants. In investigating such complaints IGIS staff might interview officers or view video recordings

Integrity of assessments

The IGIS also looks at the assessment agencies — are they objective and independent?

In 2004 Philip Flood conducted an inquiry that arose partly as a result of a concern that intelligence assessments about weapons of mass destruction in the period prior to commencement of hostilities in Iraq may not have been sufficiently independent or robust.

Flood recommended that IGIS should conduct periodic reviews of the statutory independence of the Office of National Assessment to provide assurance that it is free from political interference.

This has now been extended to the Defence Intelligence Organisation (DIO) and ASIO. The office asks the following questions:

- Do assessments show any actual evidence of bias?
- Are they fairly based on the sources and reference material?
- Do they ignore inconvenient material?
- Are the topics selected properly or is there influence to ignore problematic areas?

The IGIS also looks at the foreign intelligence agencies. These agencies generally require ministerial authorisation to collect intelligence on an Australian person. It is natural that any such request will seek to be persuasive when it sets out how a person is involved in activities that are, or are likely to be, a threat to security. It will summarise intelligence about activities and affiliations and, on the face of the documents, the case will usually be convincing. But it is necessary, although difficult and time-consuming, for IGIS staff to look at the raw information behind the document to determine whether such an assessment is actually fair, accurate and balanced. Has it left out exculpatory or contradictory material? Does it overestimate the confidence in a particular conclusion? Does it note that some intelligence cited might be dated or overtaken by other events? Does it set out any risks to the safety of the individual where relevant? Clearly the office cannot do this for all assessments but it is a worthwhile exercise for key or contentious assessments.

We have learned a lot recently about how to conduct this type of analysis from our examination of the full and rigorous reports of the Independent Reviewer of Adverse Security Assessments.

Increasing role of the office – a challenge and opportunity

As the functions and powers of the agencies have expanded so too has the role of the IGIS.

I have already mentioned the amendments to the IGIS Act following the Flood inquiry, but when ASIO's questioning and detention warrants were introduced in 2003 a legislated safeguard was that the IGIS can attend questioning sessions and any concern raised must be considered.

And there have been many more recent changes to agency powers including

- The introduction of identified person warrants which devolves some decision making from the Attorney-General to officials – whose decisions are subject to IGIS scrutiny.
- Changes in computer access warrants to cover systems and networks and allow disruption. This will require technical expertise to oversight.
- Amendments to allow ASIO officers to use force against a person during the execution of a warrant. Concerns about this were raised in committee stage and as a safeguard the legislation now requires ASIO to notify the IGIS if such force is used against a person. This new provision will require oversight of training arrangements as well as investigation of any instances where force is used.
- Amendments to the telecommunications interception and access act include a new role for the IGIS in relation to journalist source warrants – commencing in October. The IGIS must receive a copy of the warrant, and the PJCIS must receive a copy of any IGIS inquiry or inspection of such a warrant, and can request a briefing from the

IGIS. This provision is quite a departure from existing arrangements and might suggest a greater role in the future for the PJCIS.

Special intelligence operations

A good example of a new ASIO power that requires particular oversight is the power to conduct 'special intelligence operations' .This new scheme allows the Attorney-General to give ASIO staff and other people limited immunity from Australian law in relation to particular operations.

The purpose is to allow ASIO to gain close access to sensitive information via covert means. Such operations can involve engaging and associating with those who may be involved in criminal activity, and so has the potential to expose ASIO employees to criminal or civil liability including, for example, membership, training or funding a terrorist organisation.

At committee stage I commented that the scheme has limited reporting requirements and oversight would be required during the life of such operations. The bill was subsequently amended to ensure that the IGIS is notified of such operations from their commencement and can monitor accordingly.

Section 35P of the ASIO Act 1979 is the provision in the scheme that has attracted a lot of media attention and is currently the subject of an Independent National Security Legislation Monitor review.

Generally it provides that a person commits an offence if they disclose information relating to a special intelligence operation. The purpose is to protect sensitive information and the identity and safety of ASIO employees and sources.

One criticism of the provision is that it would have a chilling effect on media reporting and prevent public scrutiny of ASIO operations. There was also concern that an intelligence operation would be declared a 'special intelligence operation' (SIO), in the terms of s 35P, just so that these secrecy provisions would apply.

The actual provision is not actually concerned with the legality or propriety of the conduct of ASIO per se so its operation is not directly within the IGIS's remit. But the IGIS will be required to provide assurance that requests for SIOs are made for proper purposes and not just to invoke these additional secrecy offences.

Credibility and reputation

An ongoing dilemma for intelligence oversight is the matter of credibility and reputation. Unlike ombudsmen and most anti-corruption bodies, intelligence oversight bodies cannot generally publish comprehensive inquiry reports or data about inspection regimes. It is a necessary feature of intelligence work that to make investigations public could compromise operations or capabilities, prejudice security, damage Australia's relations with other countries and endanger lives.

But in my view as much of this work as can be made public should be made public so as to build and maintain confidence in intelligence oversight. Every year I had robust discussions with agencies about what could go in the IGIS annual report. Agencies argued forcefully for adverse material to be omitted and I needed to remind them that public embarrassment about maladministration was not in itself prejudicial to security.

The IGIS Act 1986 also has perhaps the tightest secrecy provisions of any oversight body. The extent of secrecy goes beyond national security considerations. The IGIS cannot confirm or deny whether a particular person has made a complaint or what the subject matter of the complaint is – even to a court.

In response to a complaint about an overt activity, for example a complaint about the execution of an ASIO search warrant, the office can usually provide details of both the investigation and any outcome to the complainant. But, in responding to a complaint about a covert activity, the office does not confirm whether or not the activity took place. This means that such complainants are rarely satisfied. And in some cases it may only serve to confirm in their minds otherwise unfounded suspicions.

This can be frustrating and does not build public confidence in the oversight regime — particularly when the complainant is a parliamentarian or a journalist and the allegation is the subject of ongoing media attention.

A number of recent media articles have questioned the effectiveness of the IGIS. In the absence of evidence to the contrary it is perhaps unsurprising that most media commentators seem to assume that any government office is generally inept!

So, for example, Geoffrey Robertson QC commented in light of an allegation about the Australian Signals Directorate (ASD):

> We are sliding into an Orwellian world where the state can hoover up any electronic communication. Australia has a statutory guardian of the security services, an Inspector-General, but we have not heard a squeak from her. What is the point of her office if she remains silent over such a failure of intelligence?

I have also seen the inevitable but hardly original: 'the watchdog needs a guide dog'— the IGIS is blind to agency faults, or 'the watchdog is a lapdog'—that is, too close to the agencies.

It is difficult to rebut these criticisms without being able to provide comprehensive public reports.

The future

So where does this take us? The IGIS is but one part of the oversight regime. The agencies are also subject to ministerial authorisations and directions. The PJCIS generally examines the administration and expenditure of all AIC agencies and has a role in examining counter-terrorism legislation and the listing of terrorist organisations. The Independent National Security Legislation Monitor (INSLM) is of course part of the framework, as is the Australian National Audit Office (ANAO) and the independent reviewer of adverse security assessments.

There have been a number of calls for changes to strengthen oversight arrangements. For example, last year the then Senator John Faulkner published a thoughtful paper titled *Surveillance, Intelligence and Accountability: an Australian Story* suggesting that a serious examination of the effectiveness of oversight of the AIC is long overview.

In particular, he suggested a PJCIS with more flexible membership, greater powers and resources, including the capacity to generate its own inquiries – in line with US and UK committees. He also suggested better coordination with the IGIS including providing inquiry reports to the committee, and oversight responsibility for the counter-terrorism elements of

the Australian Federal Police (AFP). This would be a significant shift for a committee that has traditionally had a limited role.

It is my view that the current system of oversight does not have serious structural deficiencies: the office of the IGIS currently has the powers, resources (particularly with the recent increases in funding) and expertise to carry out its role effectively. In my experience intelligence agencies do not systemically misuse their powers. But nevertheless controversy and suspicion persists. A recent commentator has noted that notwithstanding any harm to foreign relations or national security caused by the Snowden leaks; the real damage was the loss of public confidence in intelligence agencies.

The IGIS was established as a result of public concerns about the powers of intelligence agencies and the necessary secrecy that attaches to their activities. I acknowledge that 30 years later those critics are even more vocal but, in my view, that does not mean that the office has failed to achieve its purpose; rather, that the need for the IGIS is stronger than ever.