Intelligence Services Amendment (Establishment of the Australian Signals Directorate) Bill 2018

Submission to the Senate Foreign Affairs, Defence and Trade Legislation Committee

The Hon Margaret Stone
Inspector-General of Intelligence and Security

09 March 2018

Introduction

The Inspector-General of Intelligence and Security (IGIS) is an independent statutory officer who reviews the activities of the Australian intelligence agencies including the Australian Signals Directorate (ASD). This submission is intended to provide the Senate Foreign Affairs, Defence and Trade Legislation Committee (the Committee) with information about the current oversight of ASD by the IGIS and the expected impact of the changes proposed by the Intelligence Services Amendment (Establishment of the Australian Signals Directorate) Bill 2018 (the Bill) on that oversight.

Key points

The key points made in this submission are as follows.

- The Inspector-General does not have any significant concerns about the proposed amendments.
- The current regime of inspections of ASD activity by the IGIS will continue largely unaffected by the proposed amendments.
- IGIS will gain jurisdiction for employment related complaints by ASD staff. Under the proposed amendments ASD staff, like ASIS and ASIO staff, will not have access to review mechanisms available under the *Public Service Act 1999.*
- The proposed new ASD function relating to cybercrime is consistent with the current framework of the *Intelligence Services Act 2001* and IGIS will be able to oversee this new function including through review of ministerial authorisations.
- The proposed new function enabling ASD to protect specialised technologies will be subject to existing laws except in the limited circumstances where the immunity in s14 of the Intelligence Services Act applies.
- The proposed expansion of ASD's 'network defence' function is unlikely to raise oversight issues, these activities are done with the knowledge and consent of the relevant network operator. The annual reporting to IGIS on significant relationships will assist with oversight.

Role of the Inspector-General of Intelligence and Security

The IGIS is an independent statutory officer who reviews the activities of the Australian intelligence agencies:

- Australian Security Intelligence Organisation (ASIO)
- Australian Secret Intelligence Service (ASIS)
- Australian Signals Directorate (ASD)
- Australian Geospatial-Intelligence Organisation (AGO)
- Defence Intelligence Organisation (DIO)
- Office of National Assessments (ONA).

The Office of the IGIS is currently situated within the Prime Minister's portfolio. The IGIS is not subject to direction from the Prime Minister, or other ministers, on how responsibilities under the *Inspector-General of Intelligence and Security Act 1986* (IGIS Act) should be carried out. The Office currently has 16 staff.

The IGIS Act provides the legal basis for the IGIS to conduct inspections of the intelligence agencies and to conduct inquiries of the Inspector-General's own motion, at the request of a Minister, or in response to complaints.

The overarching purpose of the IGIS's activities is to ensure that each intelligence agency acts legally and with propriety, complies with ministerial guidelines and directives, and respects human rights.[1] A significant proportion of the resources of the office are directed towards ongoing 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. IGIS staff have access to all documents of the intelligence agencies and the IGIS is often proactively briefed about sensitive operations.

The inspection role of the IGIS is complemented by an inquiry function. In undertaking inquiries the IGIS has strong investigative powers, including the power to 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. Conducting an inquiry is resource intensive but provides a rigorous way of examining a particular complaint or systemic matter within an agency.

The Inspector-General also receives and investigates complaints and Public Interest Disclosures about the Australian intelligence agencies. These come from members of the public and from current and former staff of the agencies.

Changes to IGIS office

The government has announced that the Office of the IGIS will be moved to the Attorney-General's portfolio in a forthcoming machinery of government change. The move of the IGIS is expected to coincide with the movement of ASIO out of the Attorney-General's portfolio and is subject to the passage of relevant legislation.[2]

In response to the recommendations of the *2017 Independent Intelligence Review* the government has recently announced that the jurisdiction of the IGIS will be extended to include the intelligence functions of the Home Affairs Department, the Australian Federal Police, the Australian Criminal Intelligence Commission and Australian Transaction Reports and Analysis Centre. Resources for the IGIS will be increased to allow the office to sustain a full time staff of 55 and to allow the agency to move to new premises.[3]

---

1 See s 8 of the *IGIS Act* in relation to the general jurisdiction of the IGIS.

2 Parliamentary Joint Committee on Intelligence and Security, *Advisory Report on the Home Affairs and Integrity Agencies Legislation Amendment Bill 2017*, 26 February 2018, p. 5 at [1.25]-[1.28]. The Government has referred to these changes as 'phase 2' of the machinery of government changes in relation to the establishment of the Home Affairs portfolio (phase 1 occurring on 20 December 2017).

3 Senator the Hon James McGrath, *Portfolio Additional Estimates Statements 2017-2018, Prime Minister and Cabinet Portfolio*, 1 February 2018, pp. 33-40, especially at p. 33.

Current IGIS oversight of ASD

The IGIS office undertakes regular inspections of ASD activities and occasional inquiries. The most recent IGIS annual report included an unclassified summary of one inquiry into ASD and the results of ongoing inspection activity. Relevant extracts from the 2016-17 IGIS annual report area at Attachment A.

ASD has an internal compliance team and the productive and professional relationship between that team and IGIS staff is essential to effective oversight. ASD cooperates fully with IGIS inspections and inquires. The Inspector-General also values the candour of the Director of ASD in bringing matters of potential concern to her attention promptly.

Changes to ASD – impact on oversight

The proposal to make ASD into a statutory authority will, of itself, not have any impact on IGIS oversight of ASD. Having ASD staff employed under the *Intelligence Services Act 2001* rather than the *Public Service Act 1999* will have some consequential effects on IGIS jurisdiction including in relation to complaints and the addition of new functions for ASD will have an impact on the IGIS inspection program and scope for inquiries. All of these changes can be accommodated within the current IGIS oversight framework and the additional resources required will be drawn from the recent increase in IGIS resources in response to a recommendation of the 2017 Independent Intelligence Review.

Employment arrangements

ASD staff are currently employed under the *Public Service Act*. This means that Directions given under that Act as well as Australian Public Service wide policies currently apply to ASD. ASD staff currently have recourse to the Merit Protection Commissioner in relation to a broad range of employment matters.[4] In contrast, staff employed in ASIS and ASIO have never been employed under the *Public Service Act* or its predecessor.

This difference in employment arrangements and the ability of *Public Service Act* staff to readily seek review through the Merit Protection Commissioner is reflected in the *IGIS Act*. Broadly speaking, the IGIS can currently review employment related matters for ASIS and ASIO staff but not for staff in agencies that employ under the *Public Service Act*.[5] The Bill would, if enacted, change this so that ASD staff are in the same position as ASIS and ASIO staff when it comes to IGIS jurisdiction in relation to employment matters.[6] The current limits on IGIS jurisdiction in relation to employment matters are set out in Attachment B. In essence, the IGIS can look at ASIS and ASIO employment matters once appropriate internal review mechanisms have been exhausted and in circumstances where the

4 Staff from the Defence Intelligence Organisation, Australian Geospatial-Intelligence Organisation and Office of National Assessments are also employed under the *Public Service Act.* (Although the latter may also engage staff under subsection 17(6) of the *Office of National Assessments Act 1977.*)

5 *IGIS Act* ss 8(5), 8(6), 8(7) and 11(5). In relation to 'ASIO affiliates' (persons who perform services for ASIO under contract, agreement or other arrangement) also see *IGIS Act* ss 8(8), 8(8A), 8(9) and 11(6).

6 Bill, Schedule 1, items 73-77. Proposed Parts 3A and 5A of the *Intelligence Services Act* (to be inserted by item 27 and 29 of the Bill) also largely mirror the existing arrangements for ASIS.

Inspector-General is satisfied that it is reasonable for the complainant not to have pursued an available action in a tribunal or court.

The IGIS receives a small number of ASIS and ASIO employment related complaints each year. In 2016-17 five such complaints were received and in the first half of the current financial year three were received. ASIS and ASIO staff face unique barriers when it comes to seeking redress through other mechanisms such as the Fair Work Commission. In particular, it is an offence to disclose the fact that a person is employed by one of these agencies.[7] Most of the work undertaken by ASIS and ASIO is highly classified. Various offences may apply to the external disclosure of matters relevant to employment such as security procedures, training opportunities and, in many cases, even location of work.[8] Other sensitivities may arise in relation to the admission of such information in evidence in judicial or administrative proceedings. For these reasons the Inspector-General usually exercises her discretion to investigate ASIS and ASIO employment related complaints once the individual has exhausted appropriate internal review mechanisms.[9]

If the Bill is enacted the question of whether any particular future employment related complaint by an ASD staff member should be inquired into by the IGIS will be considered on its merits. It is likely that one of the factors the IGIS will take into account in considering whether a complainant should have pursued a right to review by a tribunal or a court will be whether there are security related reasons why it would not be practicable for them to do so. The absence of relatively easy and inexpensive review via the Merit Protection Commissioner will also be relevant.

It is also worth noting that the unique security considerations that apply to ASIS and ASIO staff have also contributed to different industrial relations arrangements being in place in those agencies compared to other government bodies. Both ASIS and ASIO have a 'staff association' which has been in existence for many decades. These organisations:

- promote the interests of staff in employment related matters;
- protect the welfare of staff;
- foster and maintain a spirit of cooperation and common interest within the agency; and
- provide a direct avenue for communication on employment matters with the Director-General.

---

7 The relevant offences apply to the publication of the identities of current or former staff members, including any information from which the identity of those persons can reasonably be inferred. They are punishable by a maximum penalty of 10 years' imprisonment: *ASIO Act* s 92 and *Intelligence Services Act* s 41.

8 See, for example: *ASIO Act* s 18(2) and *Intelligence Services Act* s 39 (offences for the unauthorised communication of information or matter acquired or prepared by ASIO and ASIS in connection with, or relevant to, the performance of their functions). These offences apply to 'entrusted persons' who include staff members and are punishable by a maximum penalty of 10 years' imprisonment.

9 In accordance with s 11(4) of the *IGIS Act* the Inspector General can decline to inquire into a complaint where the Inspector-General is of the opinion that it would be reasonable for the complainant to exercise a right to review before a tribunal or court.

Pay and conditions in ASIO and ASIS are set under determinations made by the relevant Director-General.[10] These determinations are not certified agreements but are negotiated with staff and the staff association in a similar way to agreements in other government agencies.

Although ASIO and ASIS do not employ staff under the *Public Service Act* they are obliged to adopt the principles of that Act to the extent which the Director-General considers they are consistent with the effective performance of the functions of the agency.[11] The same approach is proposed for ASD.[12] In my experience ASIS and ASIO adhere to this requirement and the employment related policies in the agencies are similar to those in the APS.

New ASD function – cybercrime undertaken by people or organisations outside Australia

Item 9 of Schedule 1 to the Bill proposes a new function for ASD in new s 7(1)(c):

> (c) to prevent and disrupt, by electronic or similar means, cybercrime undertaken by people or organisations outside Australia.

This function is broadly consistent with the existing functions of ASD and, like ASD's intelligence functions, is focused on people and organisations outside Australia.

The proposed new function will not, of itself, allow ASD to undertake any activity which would constitute a crime in Australia. For example, it would not allow ASD to engage in conduct constituting a computer offence in Part 10.7 of the *Criminal Code*. In general terms, these offences apply to persons who cause unauthorised access to, or modification of, data held in a computer; or unauthorised impairment of electronic communication to or from a computer.

The only circumstances in which ASD staff have immunity from civil and civil liability are those set out in section 14 of the *Intelligence Services Act*.[13] Section 14 is extracted in Attachment C. Subsection 14(1) provides a broad immunity for actions done *outside Australia* in the proper performance of a function – this would include any new functions of ASD.[14] A much narrower immunity is available under s 14(2) for preparatory acts that occur inside Australia but only where that preparatory act together with an act, event or circumstance or result outside Australia could amount to an offence.[15] The immunity in s 14(2) can cover cyber-related actions where some steps are taken inside Australia but the action or result which would amount to a crime happens outside Australia. The immunity does not apply to actions which ASIO could not do in Australia without a warrant. So, for example, nothing in the *Intelligence Services Act* would allow ASD to access restricted data on a computer physically located inside Australia – even where doing so would assist

10 For ASIS see s 33(3) of the *Intelligence Services Act,* and for ASIO see s 84(2) of the *ASIO Act*.

11 *Intelligence Services Act* s 35, and *ASIO Act* s 88.

12 Bill, Schedule 1, item 27 (proposed s 38F of the *Intelligence Services Act*).

13 See also a corresponding provision in s 476.5 of the *Criminal Code*, which applies to 'computer-related acts' done in the proper performance of the functions of ASD (and ASIS and AGO). A 'computer-related act' is, in summary, an act, event, circumstance or result concerning the operation of a computer, data held in a computer, and electronic communications to or from a computer.

14 See also the corresponding provision in s 476.5(1) of the *Criminal Code.*

15 See also the similar provision in s 476.5(2) of the *Criminal Code.*

in gathering intelligence or disrupting crime. Accessing data located inside Australia is properly an action that requires an ASIO or police warrant.[16]

A change which extended the immunity or which changed ASD's focus for its covert or intrusive intelligence related activities to people and organisations *inside* Australia would be a profound one – the proposed additional function relating to cybercrime is not such a change. Rather, the proposed change is consistent with the existing focus and immunity arrangements.

ASD is focused on the activities of people and organisations outside Australia. This does not mean it can never undertake activities that are directed towards Australian persons. Sections 8 and 9 of the *Intelligence Services Act* sets out a regime for ministerial authorisation to be sought and granted before ASD undertakes an activity for the specific purpose, or purposes which include the specific purpose, of producing intelligence on an Australian person and in certain other circumstances.[17] The Bill proposes to extend the ministerial authorisation regime to require ASD to seek authorisation before undertaking an activity, or a series of activities, for the specific purpose, or purposes which include the specific purpose, of preventing or disrupting cybercrime undertaken by, or enabled by, an Australian person.[18] This is an important safeguard and is consistent with the current framework in the *Intelligence Services Act*. The IGIS inspection regime in ASD pays particular attention to activities that require ministerial authorisation.

The *2017 Independent Intelligence Review* recommended introducing a requirement for all *Intelligence Services Act* agencies to seek ministerial authorisation for activities likely to have a *direct effect* on an Australian person.[19] Currently such a requirement only applies to ASIS.[20] To our knowledge, the government has not yet released a response to this recommendation.

New ASD function – protection of specialised technologies

Item 11 of Schedule 1 to the Bill proposes a new function for ASD in new s 7(1)(da):

> (da) to protect specialised technologies acquired in connection with the performance of any of the proceeding functions;

As noted above, ASD is focused on the activities of people and organisations outside Australia and the only circumstances in which ASD staff have protection from civil and criminal liability are those set out in s 14 of the *Intelligence Services Act*.[21] Any actions ASD staff take in order to protect ASD's specialised technologies under the proposed new function will need to be consistent with Australian law, except insofar as the immunity applies. Protection of specialised technologies may be impliedly

16 ASD could, if permitted by the terms of the warrant and authorised by the relevant agency head, assist the agency executing the warrant. See, for example, *ASIO Act*, section 24.

17 Arrangements for seeking authorisation in an emergency situation are set out in ss 9A, 9B and 9C of the *Intelligence Services Act.*

18 Bill, Schedule 1, item 15, inserting new s 8(1)(a)(iii).

19 M L'Estrange and S Merchant, *2017 Independent Intelligence Review*, June 2017, Recommendation 16(c). See also p. 99 at [6.37]-[6.38].

20 Subparagraph 8(1)(a)(ii) of the *Intelligence Services Act*. (See also s 8(1)(a)(ib) in relation to ASIS's activities in the course of providing assistance to the ADF in military operations.)

21 Or under the equivalent provision of section 476.5 of the *Criminal Code* in respect of computer-related acts.

within ASD's current functions but the proposed amendment will put this beyond doubt. As noted above any potentially unlawful actions not covered by the immunity or which would require a warrant cannot be undertaken in reliance on the proposed new function. This is consistent with the existing framework of the *Intelligence Services Act*.

Expanded ASD function – advice and assistance on security and integrity of electronic information

In addition to its covert intelligence-related activities, ASD has a 'network protection' function. Originally, this involved providing assistance to Commonwealth and State authorities.[22] Proposed ss 7(1)(ca) and 7(2) will extend this to foreign persons or entities and other persons within certain constitutional limits.[23] The provision of advice and assistance is a cooperative activity. Any actions ASD may take on a computer or network operated by the person or body being assisted under this function is done with their knowledge and consent. From an oversight perspective, the expansion in ASD's 'network protection' functions is unlikely to require any significant adjustment in IGIS inspection arrangements. The requirement in proposed s 13(5)[24] that ASD report annually to the Minister and the IGIS on significant cooperation with authorities of other countries undertaken for the purpose of its 'network protection' function will assist the Inspector-General in maintaining oversight of these arrangements.

22 Existing paragraph 7(c) of the *Intelligence Services Act.*

23 Items 10 and 13 of Schedule 1 to the Bill. See also proposed section 13 (item 23) under which the Minister may approve foreign entities with which ASD may cooperate for the purpose of performing its function under new s 7(1)(ca).

24 Item 23 of Schedule 1 to the Bill.

Attachment A – extracts from 2016-17 IGIS annual report

This report is available at http://igis.gov.au/publications-reports/annual-reports

INQUIRY INTO AN AUSTRALIAN SIGNALS DIRECTORATE MATTER (p. 12)

In February 2017 this office initiated an inquiry into an Australian Signals Directorate (ASD) matter pursuant to s 8(2) of the IGIS Act. The final report was provided to ASD in July 2017.

The Inspector-General found that ASD relied on incorrect legal advice in determining the parameters governing its interception of certain telecommunications. The inquiry also found inadequacies in ASD's reporting of the problem to the IGIS and to Ministers. The details of the incorrect legal advice and relevant contextual information are classified. The report included five (classified) recommendations designed to ensure that the situation would not arise in the future and to streamline communications with Ministers and with the IGIS.

ASD has accepted all the recommendations and has agreed to report to the Inspector-General on its progress in implementing the recommendations within 6 months. The Inspector-General is satisfied with ASD's corrective measures to date and with the revised reporting arrangements between ASD and this office.

A full account of the inquiry is contained in the classified report which has been provided to the Director of ASD, the Minister for Defence and the Prime Minister and copied to appropriate Australian Government recipients for information. Given the highly classified nature and details of the inquiry, no further information will be released publicly.

INSPECTION OF ASD ACTIVITIES (pp. 27-28)

During 2016–17 the office inspected a number of ASD activities, including:

- ministerial authorisations to produce intelligence on Australian persons
- ASD's compliance with the privacy rules
- compliance incident reports
- cyber activities
- ASD's access to sensitive financial information (discussed later in the report).

These inspections are supplemented by briefings on various matters across the year either at the request of this office or at the instigation of ASD. These briefings and subsequent investigations allow the office to stay abreast of emerging issues, and to pursue trends observed during inspections.

In this reporting period a significant focus for the office was an inquiry into ASD's interception of certain telecommunications outside authorised parameters. The ASD inquiry was labour intensive and, with the inquiry into the analytic independence and integrity of DIO, completing these inquiries meant diverting some staff from ASD inspections. Consequently, the office reviewed fewer ministerial authorisations to produce intelligence on Australian persons than in the previous reporting period, and was not able to complete any in-depth inspections of these authorisations.

MINISTERIAL AUTHORISATIONS TO PRODUCE INTELLIGENCE ON AUSTRALIAN PERSONS (p. 28)

During 2016–17 the office inspected about two-thirds of ASD's ministerial authorisations, down slightly on the previous reporting period. The submissions were generally of a high standard. In some cases, however, the office was able to suggest possible improvements for future submissions to the Minister. These matters were not significant, and ASD's response to these suggestions was appropriate.

When ASD seeks to renew a ministerial authorisation there can be a period between the expiry of the previous authorisation and approval of the renewal during which ASD must not attempt to produce intelligence or engage in other activities relating to the subject of the ministerial authorisation. In such cases IGIS officers investigate whether ASD ceased relevant activities during the relevant period. The office identified only one case where ASD conducted an activity during a short period between the expiry and renewal of the authorisations. ASD accepted the finding and its investigation into the incident was ongoing at the end of the reporting period.

A change of circumstances may prompt the Minister to cancel a ministerial authorisation, or it may expire at the end of the authorisation period. In either case within three months ASD is required to provide the Minister a report on its activities that relied on the authorisation. We reviewed a number of these cancellation and non-renewal reports and did not identify any concerns.

EMERGENCY MINISTERIAL AUTHORISATIONS (pp. 28-29)

Situations may arise where, as a matter of urgency, ASD requires a ministerial authorisation to undertake certain activities. Emergency authorisations may be provided orally by the Defence Minister, other select ministers where the Defence Minister is unavailable, or the Director ASD can authorise such activities if the ministers are not readily available. Emergency authorisations are only valid for 48 hours after which any further activity will require a new authorisation if ASD is to continue the relevant activity.

One emergency ministerial authorisation was issued for ASD during the reporting period. This authorisation is associated with an ASD compliance incident report provided to this office on 30 June 2017. This office will report on this matter in the next reporting period.

PROTECTING THE PRIVACY OF AUSTRALIAN PERSONS (p. 29)

The Minister for Defence makes written rules, the Rules to Protect the Privacy of Australians, to regulate how ASD communicates and retains intelligence information concerning Australian persons. ASD is required to report to this office any breaches of the privacy rules and during inspections IGIS staff pay close attention to ASD's compliance with the privacy rules and to its distribution of intelligence about Australian persons. In accordance with its obligations under the privacy rules, ASD has continued to report cases where the presumption that an individual is not an Australian is subsequently rebutted and the person is shown to be Australian. These reports include details of the measures taken to protect the privacy of that person. In all such cases reported to this office by ASD, the presumption of nationality was reasonable based on the information ASD had at the time. The actions taken by ASD, including informing other intelligence agencies that the person is Australian, were appropriate and in accordance with the privacy rules. To ensure there are adequate safeguards

to protect the privacy of Australians ASD has also consulted with this office in relation to such matters as expanding information sharing with other countries.

There was one breach of the privacy rules, which occurred at the end of 2015–16 but was reported to this office in 2016–17. This breach resulted from human error where intelligence information on an Australian person was not removed from a wider dataset that was passed to a foreign intelligence agency. The office accepted ASD's account of this case, and was satisfied with the remedial actions ASD took to minimise the risk of this recurring.

Before being informed of this breach, the IGIS was briefed on ASD's procedures to redact information about Australians. The circumstances detailed in that briefing were similar to those of the breach, however the breach was not raised. The IGIS subsequently raised with Director ASD the need for ASD staff to be more candid in any future briefings. A lack of timely, detailed advice was also an issue in relation to the compliance incident report that prompted this office to undertake the inquiry into ASD. Subsequently, in the latter part of 2016–17, there has been a marked improvement in the openness of ASD's reporting and in its timeliness.

COMPLIANCE INCIDENT REPORTS (pp. 29-30)

Where ASD identifies matters involving breaches of legislation and significant or systemic matters of non-compliance with ASD policy, these are investigated by ASD and reported to the IGIS in compliance incident reports. This office reviews these reports and undertakes an investigation of the incident where necessary. ASD provided four such reports during 2016–17; one of these was provided on 30 June and, the results of our review will be reported in the next annual report.

In August 2016 ASD advised this office of its investigation into an incident that involved sharing certain types of data in support of operations in Afghanistan. The data intended to be shared included some data that ASD was not authorised to share. There was no resultant legislative breach as technological safeguards ultimately prevented non-compliant data from being shared. The ASD investigation made recommendations to improve the management of information sharing. This office was satisfied with ASD's investigation and remedial action proposed to prevent recurrence.

There was another incident in August 2016 after ASD collected intelligence about an individual in breach of the of the *Telecommunications (Interception and Access) Act 1979*. The Inspector-General formed the view that the cause of this breach was a failure to follow extant policies and procedures with the requisite care but was satisfied with the remedial actions proposed and implemented by ASD.

In December 2016, ASD reported on three breaches of the *Telecommunications (Interception and Access) Act 1979*. The configuration of an ASD collection system had led to it collecting certain telecommunications beyond the scope of the relevant warrant. In doing so ASD had relied on legal advice to the effect that communications beyond the scope of the warrant could be lawfully collected provided they were later destroyed. This led to the IGIS inquiry into the matter; the inquiry report was finalised and submitted to all relevant parties several weeks after the end of the current reporting period.

Among the concerns discussed in the report was the adequacy and timeliness of ASD's communications about the issues including to Ministers and to this office. An initial communication merely stated that there had been a breach but did not give any further details.

It was some months before additional details were provided. This was not consistent with the written guidance given to ASD about IGIS reporting expectations nor was it consistent with this office's reliance on agencies proactively reporting issues of legality and propriety. Since this issue was drawn to ASD's attention, which was well before the inquiry was completed, it has been gratifying to record that there have been noticeable improvements in the reporting on compliance matters to this office. The final report was submitted to all relevant parties some weeks after the end of the current reporting period. It contained classified recommendations designed to improve communications and prevent any future such issue.

As at 30 June ASD had also reported four additional breaches of the *ISA* and *Telecommunications (Interception and Access) Act 1979*. These matters were being investigated and will be reported on in the next annual report.

CYBER ACTIVITIES (p. 30)

In October 2016 this office concluded an inspection project in relation to ASD computer network operations, including sensitive cyber operations in support of ADF operations in Iraq and Syria. The project noted that ASD's offensive cyber capabilities are evolving rapidly and the governance frameworks underpinning some areas are still developing. This project found guidance in place at the time was appropriate and followed by staff, and no issues of legality or propriety were noted. This office continues to maintain an interest in the cyber activities of ASD.

Attachment B - Limits on IGIS jurisdiction in relation to employment matters

Section 8 of the *IGIS Act* provides the general jurisdiction for IGIS to oversee the legality and propriety of intelligence agency activities. That jurisdiction is limited in relation to employment matters as follows:

(5) The functions of the Inspector-General under subsections (1), (2) and (3) do not include inquiring into a matter to which a complaint to the Inspector-General made by an employee of AGO, ASD, DIO or ONA relates to the extent that the matter is directly related to:

(a) the promotion, termination of appointment, discipline or remuneration of the employee by the agency; or

(b) another matter relating to the agency's employment of the employee.

(6) The functions of the Inspector-General include inquiring into a matter to which a complaint to the Inspector-General made by an ASIO employee or an ASIS employee relates to the extent that the matter is directly related to:

(a) the promotion, termination of appointment, discipline or remuneration of the employee by ASIO or ASIS; or

(b) another matter relating to the employment of the employee by ASIO or ASIS.

(7) However, the Inspector-General must not inquire into a matter referred to in subsection (6) to the extent that the employee can have the matter reviewed by a body constituted by, or including, persons other than:

(a) for an ASIO employee—the Director-General of Security, ASIO employees or ASIO affiliates; and

(b) for an ASIS employee—the Director-General of ASIS or ASIS employees.

Note: See also subsection 11(5).

(8) The functions of the Inspector-General include inquiring into a matter to which a complaint to the Inspector-General made by an ASIO affiliate relates to the extent that the matter is related to:

(a) the contract, agreement or other arrangement under which the ASIO affiliate is performing functions or services for ASIO; or

(b) the performance of functions or services by the ASIO affiliate under the contract, agreement or other arrangement.

Section 11 of the *IGIS Act* provides the IGIS with jurisdiction to inquire into complaints about the activities of the intelligence agencies. That jurisdiction is limited in relation to employment matters as follows:

> (5) The Inspector-General shall not inquire into the matters to which a complaint of the kind referred to in subsection 8(6) relates in respect of action taken by an intelligence agency if the Inspector-General is satisfied that:
>
> (a) the procedures of that agency relating to redress of grievances of ASIO employees or ASIS employees (as the case may be) are adequate and effective; or
>
> (b) the complainant has not pursued those procedures as far as practicable; or
>
> (c) the matters to which the complaint relates are not of sufficient seriousness or sensitivity to justify an inquiry into those matters.
>
> (6) The Inspector-General may decide not to inquire into the matters to which a complaint of the kind referred to in subsection 8(8) relates in respect of action taken by ASIO if the Inspector-General is satisfied that:
>
> (a) the procedures of ASIO relating to redress of grievances of ASIO affiliates are adequate and effective; or
>
> (b) the complainant has not pursued those procedures as far as practicable; or
>
> (c) the matters to which the complaint relates are not of sufficient seriousness or sensitivity to justify an inquiry into those matters.

Attachment C – Immunity in s 14 of the Intelligence Services Act

Division 4—Other

14 Liability for certain acts

(1) A staff member or agent of an agency is not subject to any civil or criminal liability for any act done outside Australia if the act is done in the proper performance of a function of the agency.

(2) A person is not subject to any civil or criminal liability for any act (whether done inside or outside Australia) if:

(a) the act is preparatory to, in support of, or otherwise directly connected with, overseas activities of the agency concerned; and

(b) the act:

(i) taken together with an act, event, circumstance or result that took place, or was intended to take place, outside Australia, could amount to an offence; but

(ii) in the absence of that other act, event, circumstance or result, would not amount to an offence; and

(c) the act is done in the proper performance of a function of the agency.

(2A) Subsection (2) is not intended to permit any act in relation to premises, persons, computers, things, or telecommunications services in Australia, being:

(a) an act that ASIO could not do without a Minister authorising it by warrant issued under Division 2 of Part III of the *Australian Security Intelligence Organisation Act 1979* or under Part 2-2 of the *Telecommunications (Interception and Access) Act 1979*; or

(b) an act to obtain information that ASIO could not obtain other than in accordance with Division 3 of Part 4-1 of the *Telecommunications (Interception and Access) Act 1979*.

(2AA) Subsections (1) and (2) have effect despite anything in a law of the Commonwealth or of a State or Territory, whether passed or made

before or after the commencement of this subsection, unless the law expressly provides otherwise.

(2AB) Subsection (2AA) does not affect the operation of subsection (2A).

(2B) The Inspector-General of Intelligence and Security may give a certificate in writing certifying any fact relevant to the question of whether an act was done in the proper performance of a function of an agency.

(2C) In any proceedings, a certificate given under subsection (2B) is prima facie evidence of the facts certified.

(3) In this section:

act includes omission.

staff member includes the Director of AGO, the Director of ASD and the Director-General.