Review of the National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017

Submission to the Parliamentary Joint Committee on Intelligence and Security

The Hon Margaret Stone
Inspector-General of Intelligence and Security

22 January 2018

Introduction

The Inspector-General of Intelligence and Security (IGIS) is an independent statutory officer who reviews the activities of the Australian intelligence agencies. Information about the role and functions of the IGIS is provided at **Attachment A**. This submission addresses the potential effect on the IGIS office of the proposed secrecy offences in Schedule 2 to the National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017 (the Bill). Similar issues may arise for other oversight agencies including the Commonwealth Ombudsman, but this submission is limited to effects on IGIS.

Key issues

The Explanatory Memorandum states that the new offences 'should in no way impinge on the ability of the Inspector-General … or their staff to exercise their powers, or to perform their functions and duties'.[1] However, several issues in the design of the new offences may produce the opposite result:

1. The creation of barriers to people making complaints or disclosures to the IGIS, particularly:
   (a) an absence of protection for persons who deal with records for the purpose of making a communication to the Inspector-General or IGIS staff (IGIS officials), but have not yet done so or are prevented from doing so
   (b) ambiguity about the relationship between the new offences and other legislation containing 'secrecy override' provisions. There is a risk that the new offences may be construed or perceived as overriding important immunities available under the *Inspector-General of Intelligence and Security Act 1986* (*IGIS Act*) and *Public Interest Disclosure Act 2013* (*PID Act*) for persons who communicate information to IGIS officials
2. The potential exposure of IGIS officials to investigation and prosecution for a serious offence, merely for communicating or dealing with information to undertake their normal duties, and the need for them to rely on a defence to avoid criminal sanction
3. The proposed defences do not seem to recognise the legal barrier in s 34 of the *IGIS* Act to IGIS officials to providing evidence of the kind that would normally be required to discharge an evidential burden in defending an alleged offence.

These issues could be addressed with some targeted amendments to the proposed offences and offence-specific defences, including removal of the evidential burden on IGIS officials.

Other issues

This submission identifies three other issues arising from Schedule 2 to the Bill:

4. The absence of a direct link between concepts of sabotage, espionage and foreign interference in the proposed offences and the same concepts in the definition of security in the *Australian Security Intelligence Organisation Act 1979* (*ASIO Act*)
5. Potential for real or perceived misuse of the proposed offence and related procedural provisions concerning the classification of information
6. Potential practical consequences of the proposed offence of failure to comply with lawful directions for the retention, use or disposal of certain information

---

[1] Explanatory Memorandum, p. 278, paragraph 1625.

1. Barriers to making complaints or disclosures to the IGIS

General observations

It is essential to the effectiveness of the IGIS office that individuals with knowledge of, or concerns about, illegal or improper activity by Australian intelligence agencies are able to disclose that information to IGIS officials. It is also essential that staff in intelligence agencies cooperate fully with IGIS inspections and investigations as well as with formal IGIS inquiries. Any real or perceived barriers to such disclosures or cooperation would seriously impede the operations of the IGIS office.

Almost all the information that IGIS officials routinely review will fall within the proposed definition of 'inherently harmful information'[2]. The Bill, if enacted, would make it a serious offence to communicate, deal with, remove or hold 'inherently harmful information'.[3] The offences are aggravated if the information bears a certain classification or the person holds an Australian Government security clearance,[4] as most of the people who provide information to the IGIS do. It is a defence to the proposed offences if the person communicated the information to the IGIS, or their staff, for the purpose of those officers exercising their powers or performing their functions or duties. It is also a defence if the person communicated the information in accordance with the *PID Act*.[5] The defendant bears the evidential burden of proving that the communication was made to the Inspector-General for a relevant purpose or in accordance with the procedures in the *PID Act*.[6]

As a general observation, it is possible that the prospect of exposure to criminal investigation and prosecution, and the need to satisfy a court of the evidential burden in relation to a defence, may deter some individuals from speaking up about real or perceived wrongdoing by an intelligence agency. Exposure to criminal sanction, and the need to rely on a defence, may also cause staff within the agencies to hesitate when responding to requests for information by the IGIS.[7] The design of the proposed defences, and the relationship of the new offences with existing 'secrecy override' provisions in other Acts may also create legal barriers to disclosures or complaints.

The defences to the new 'dealing' and 'removal' offences require proof of communication

The defences in proposed ss 122.5(3) and (4) seem to only be enlivened if the person has *communicated* the information. The defences do not appear to cover preparatory actions such as printing or copying a document for the purpose of giving it to the IGIS or making a PID *unless* the person also communicated the information to the IGIS or authorised recipient of a PID. Accordingly, a person who prints, copies or makes notes from a document for one of these purposes, but has not yet or is prevented from, communicating the information to the IGIS would be exposed to criminal liability[8]. This would be the case even if the person who stopped the defendant from making the

---

2 Schedule 2, item 6, proposed s 121.1 on page 51 of the Bill.

3 Schedule 2, item 6, proposed s 122.1 on page 53-54 of the Bill.

4 Schedule 2, item 6, proposed s 122.3 on page 56-57 of the Bill.

5 Schedule 2, item 6, proposed s 122.5 on page 58-59 of the Bill contains these defences in subsections (3) and (4), for ease of reference these are extracted at **Attachment B.** .

6 *Criminal Code,* s 13.3(3).

7 This should not be read as implying that intelligence officials do not currently willingly cooperate with IGIS inspections and investigations: exactly the opposite is true. In my experience, staff in all six of the intelligence agencies currently cooperate fully and freely with IGIS inspections and investigations.

8 Under the offences for dealing with inherently harmful information in proposed ss 122.1(2) and 122.3

ultimate communication was the subject of the intended complaint or PID. In this circumstance, it would appear that a prospective defendant would be reliant on the discretion of the intelligence agency not to refer the matter to police or the discretion of law enforcement agencies not to investigate or prosecute the offence.

In contrast, the current offences in the *ASIO Act* and *Intelligence Services Act 2001* (*ISA*) for 'entrusted persons' who engage in an unauthorised dealing with a record of an intelligence agency, or the unauthorised recording of information of or about an intelligence agency, are subject to exceptions for dealings or recordings made for the purpose of the IGIS exercising a power or performing a function (extracts at **Attachment C**). These exceptions do not require proof that any information was ultimately communicated to the IGIS. Rather, they require proof of the person's intention to do so at the material time of dealing with or making the record.[9] These provisions of the *ASIO Act* and *ISA* would, in my view, provide a better model for the exceptions in proposed ss 122.5(3) and (4).

New offences may override existing immunity provisions in the IGIS Act and PID Act

Proposed Division 122 of the *Criminal Code* does not expressly deal with the interaction of the proposed provisions and existing 'secrecy override' clauses in other legislation, including s 24 of the *PID Act* and s 18(9) of the *IGIS Act*.[10] There is a risk that the proposed secrecy offences could be interpreted as overriding such provisions. This would mean that people making PIDs to the IGIS and those cooperating with IGIS inquiries could potentially be exposed to criminal liability or at the very least may have doubt about their legal position and concern about the need to rely on the proposed defences with their obligation to discharge the evidential burden.[11] The proposed scheme provide a lesser degree of protection than the immunity from liability that is currently available under s 18(9) of the *IGIS Act* or s 24 of the *PID Act* . The reduction of clear legal protections may reduce the willingness of people to provide information to the IGIS. Accordingly, I encourage the Committee to consider the inclusion of a 'relationship of laws provision' in new Division 122 to provide that the offences in that Division are not intended to override the immunity from liability provisions in the *IGIS Act* and *PID Act*.

2. The need for IGIS officials to rely on a defence to a serious offence to undertake their normal duties

As noted above, almost all of the information that IGIS officials routinely deal with would fall within the proposed definition of 'inherently harmful information'.[12] The Bill, if enacted, would make it a serious offence if a person communicates, deals with, removes or holds inherently harmful

---

9 *ASIO Act,* ss 18A(2A) and 18B(2A); *ISA,* subsection (2A) of each of ss 40C-40M.

10 These provisions confer immunity from legal liability on persons who make PIDs, and persons who provide information or documents to an IGIS inquiry in response to a statutory notice. These provisions purport to override other laws (including secrecy offences) that would otherwise expose the person to penalty for communicating the information or providing the documents to the IGIS.

11 A person who provides information or produces a document in compliance with a notice issued by the IGIS under section 18 of the *IGIS Act* could also rely on the general defence of lawful authority in section 10.5 of the *Criminal Code*. However, as with the offence-specific defences proposed in the Bill, the defendant would be required to discharge an evidential burden in relation to this defence, making it a lesser degree of protection than the immunity in subsection 18(9) of the *IGIS Act.*

12 Schedule 2, item 6, proposed s 121.1 on page 51 of the Bill.

information.[13] The offence is aggravated if the information bears a certain classification or the person holds an Australian Government security clearance,[14] as all IGIS officials do.

Clearly, in order to perform their ordinary and proper work, IGIS officials need constantly to deal with and communicate (including to each other) inherently harmful information. This will be an offence under proposed s 122.1, and in most instances, will constitute an aggravated offence under proposed s 122.3. IGIS officials will need to rely on the defence in proposed s 122.5(1)(a) that 'the person was exercising a power, or performing a function or duty, in the person's capacity as a Commonwealth officer' and, in relation to communication of information, the defence in proposed s 122.5(3). This will mean that the evidentiary onus lies with individual IGIS officials to adduce or point to evidence suggesting, in effect, a reasonable possibility that they have not committed an offence by doing their normal job. This raises a general question of whether it is appropriate for the criminal law to place individual officials in this position. In addition, as explained below, the secrecy provisions of the *IGIS Act* may be incompatible with IGIS officials discharging an evidential burden.

3. Inability of IGIS officials to discharge an evidential burden as part of the defence to an offence under Division 122

Secrecy provisions in s 34 of the IGIS Act

The *IGIS Act* contains comprehensive secrecy provisions that restrict the disclosure of information, including to courts. This is appropriate: intelligence agencies must have confidence that the sensitive national security information they provide to the IGIS will not be disclosed publically. The role of the IGIS is to assist Ministers and Government in assuring the Parliament and the public that intelligence and security matters are open to scrutiny.[15] It is not the role of the IGIS to play a role in the criminal justice system or private litigation.[16]

Subsection 34(1) of the *IGIS Act* makes it an offence for the Inspector-General or her staff to disclose information obtained in the course of their duties to any person, *or to a court,* other than for the purpose of the performance by the IGIS of his or her duties under the *IGIS Act*, *PID Act* and certain other legislation not relevant for present purposes. Subsection 34(5) also prevents the IGIS and staff from being compelled to provide such information to a court. (These provisions are extracted at **Attachment D.**)

Impact of s 34 on IGIS officials in relation to the proposed offences

IGIS officials as prospective defendants and witnesses

In the event that a current or former IGIS official was investigated for, or charged with, one of the proposed offences in Division 122 of the *Criminal Code*, it would, for all practical purposes, be impossible for them to discharge the evidential burden of proving that the alleged dealing with or communication of information contrary to the proposed offences was undertaken in the course of

---

13 Schedule 2, item 6, proposed s 122.1 on page 53-54 of the Bill.

14 Schedule 2, item 6, proposed s 122.3 on page 56-57 of the Bill.

15 *IGIS Act*, s 4.

16 With a very limited exception where the IGIS has a specific role in providing evidence in certain matters in the AAT under the *Freedom of Information Act 1982* and *Archives Act 1983*.

their duties. Indeed, they would potentially commit an offence under s 34(1) of the *IGIS Act* by disclosing that information in their defence at trial, or providing it to law enforcement officials investigating the potential commission of an offence under Division 122. Similar difficulties may arise in the investigation or prosecution of a person who made a complaint or disclosure to the IGIS that included 'inherently harmful information'.

Potential oversight of the impacts of s 34 of the IGIS Act in designing new Division 122

The interaction of s 34 of the *IGIS Act* and the proposed offences and defences in the Bill may have been overlooked. For example, the Explanatory Memorandum merely states, in relation to the defence in proposed s 122.5(1), that 'the imposition of the evidential burden on the defendant is appropriate because the defendant should be readily able to point to evidence that their conduct was … done in their official capacity as a Commonwealth official'.[17] The Explanatory Memorandum does not appear to acknowledge the possibility that a Commonwealth official may be subject to secrecy obligations under other laws, such as s 34 of the *IGIS Act*, which could prevent them from adducing the evidence that is necessary to discharge the evidential burden.

Possible legislative solution

The 'information offence provisions' of the *ASIO Act* and *ISA* do not apply to IGIS officials who engage in the conduct constituting those offences for the purpose of exercising powers, or performing functions or duties, as IGIS officials. The official does not bear the evidential burden to establish that he or she was an IGIS official and communicated the information, or dealt with or made a record, in that capacity.[18] (Extracts of these provisions are provided at **Attachment E.**) The Explanatory Memorandum to the amending legislation that enacted these provisions in 2014 commented specifically on the appropriateness of the prosecution, rather than the IGIS official as defendant, bearing the evidential burden.[19]

In my view, it would be preferable if the elements of the proposed offences in new Division 122 of the *Criminal Code* contained a similar exclusion of IGIS officials to those in the *ASIO Act* and *ISA*. This approach would overcome the difficulties in IGIS officials discharging an evidential burden in relation to a defence, while also preserving the secrecy obligations imposed by s 34 of the *IGIS Act*. Further, it would ensure that IGIS officials are treated consistently under key Commonwealth secrecy offences to which they are subject.

4. No direct link between the proposed concepts of 'sabotage', 'espionage' and 'foreign interference' in the Criminal Code and existing concepts in the definition of 'security' in the ASIO Act

The definition of the term 'security' in the *ASIO Act* is pivotal to the exercise of all of ASIOs powers including a range of warrants. The definition is contained in s 4 of the *ASIO Act* (extracted at

---

17 Explanatory Memorandum, p. 276 at paragraph 1617.

18 *ASIO Act*, s 18D and *ISA*, s 41B.

19 Explanatory Memorandum, National Security Legislation Amendment Bill (No. 1) 2014, p. 159 at paragraph 801. ('It is appropriate that the prosecution bears the evidential burden … A person's status as an IGIS official creates a strong inference that his or her conduct was for the purposes of exercising powers or performing functions or duties as an IGIS official'.)

Attachment F). The definition includes 'espionage' and 'sabotage'. These component terms are not defined in the *ASIO Act* and, as such, have their ordinary English meaning. This introduces a level of uncertainty into the definition of security, and therefore to the scope of the matters to which ASIO's powers and functions may be directed. As a matter of transparency and certainty, it would be preferable for the terms to have a clear statutory definition.

The Bill would, if enacted, introduce comprehensive offences relating to espionage and sabotage as well as definitions relevant to these terms. Linking, and limiting, the terms 'espionage' and 'sabotage' in the *ASIO Act* to conduct covered by the relevant offences in the Bill could provide greater certainty and transparency about ASIO's role and the boundaries of its powers. Other parts of the definition of security in s 4 of the *ASIO Act* are defined by reference to other parts of the *Criminal Code*, for example, acts that are offences under Division 119 of the *Criminal Code* (foreign incursions and recruitment).[20] A similar point can be made about the term 'foreign interference'. That definition (extracted at **Attachment F**) is similar to, but not identical with, the circumstances constituting 'foreign interference' for the purpose of the elements of the proposed offences in new Division 92 of the *Criminal Code*.[21] Inconsistencies may lead to uncertainty about the scope of ASIO's remit and powers. Such uncertainty is undesirable from a transparency and accountability perspective. If the Parliament's intention is that ASIO's powers in relation to espionage, sabotage and foreign interference should cover matters beyond those criminalised by the proposed provisions, then it would be beneficial for this to be made explicit.

5. Provisions concerning the security classification of information

Assigning a security classification to information or a document is not a precise science. As Inspector-General, I frequently see documents that appear to be over-classified or documents that may have been correctly classified when created but would now warrant a lower classification because of the passage of time or authorised public disclosure of related information. A tendency to over-classify documents 'to be safe' is understandable. In practical terms, the main things that presently hinge on this are the procedures that need to be applied to store, transport, destroy and disseminate the document. [23]

However, the Bill now proposes to give direct and profound legal consequences to the security classification assigned to a document or information. For example, any information that is 'security classified information' will, by definition, be 'inherently harmful information' for the purpose of the offences in the proposed Part 5.6 of the *Criminal Code* and a person will commit an aggravated offence

---

20 Offences under certain other legislation are also incorporated in the definition of 'politically motivated violence' as are terrorism offences.

21 Schedule 1, item 17 on page 32-38 of the Bill, inserting new Division 92 of the *Criminal Code*

23 In relation to intelligence agency documents, the main form of legislatively mandated review would seem to be where documents are in the open period for the *Archives Act* and are the subject of a request for access. In contrast, I have seen documents from other countries that bear markings that indicate they are to be de-classified on a set date if not reviewed earlier.

if the information bears certain classifications.[24] Some offences make the existence of a security classification a matter of strict liability.[25]

The basis upon which security classifications are to be assigned for the purpose of the proposed new offences is not transparent: proposed s 90.5 of the *Criminal Code*[26] leaves it to the regulations to define the term 'security classification' and allows those regulations to prescribe a matter by applying, adopting or incorporating any matter contained in an instrument or other writing as in force or existing from time to time. While the Explanatory Memorandum identifies a policy intention to incorporate by reference documents forming part of the Commonwealth Protective Security Policy Framework 'that are all publicly available on the internet'[27] there is no legal requirement that a document that is incorporated by reference must be publicly available. This means there is no guarantee that there will be ongoing public visibility of what 'security classification' ultimately means, or the criteria by which classification decisions are made. There is also no requirement in the proposed legislation that security classifications only be given for a specific purpose, such as the protection of national security.

Proposed s 121.3 of the *Criminal Code* would allow the Attorney-General to give a certificate in relation to information or a thing stating that it has, or had at a specified time, a particular security classification. There is no requirement that the Attorney-General consider whether the classification had been properly assigned or remained appropriate. The certificate would be prima facie evidence of the matters certified in it. As a practical matter, it is very difficult to see how a person could mount an effective challenge to such a certificate, given that they may not have access to the information or thing that is the subject of the certificate, or to the documents incorporated into the definition of a 'security classification' by the regulations.

The lack of transparency about the basis for classifications and the absence of any requirement as to the purpose of classification leaves open the risk, or at least the perception, that documents may be classified or over-classified for purposes such as avoiding public disclosure of politically inconvenient information or information about illegal or improper activities of intelligence agencies. Consideration might be given to including in primary legislation parameters for the term 'security classification' and requirements for the issuing of evidentiary certificates by the Attorney-General to manage these risks.

---

24 See proposed s 122.3 of the *Criminal Code*, inserted by Schedule 2, item 6 at pp. 56-57 of the Bill.

25 See, for example, the circumstance of aggravation in proposed s 122.3(3) of the *Criminal Code*, inserted by Schedule 2, item 6 at p. 57 of the Bill. See also, s 122.1(5) of the *Criminal Code,* inserted by Schedule 2, item 6 at p. 54 of the Bill.

26 Schedule 1, Item 8 on page 22 of the Bill. (The reference in proposed s 121.1 to the definition being in s 90.4 appears to be a typographical error: Schedule 2, item 5 on page 52 of the Bill.)

27 However, this assurance to incorporate by reference documents are publicly available is caveated: 'if this is considered an efficient and appropriate means of ensuring the definition of 'security classification is consistent with the Australian Government's policies relating to protective security'. (Explanatory Memorandum, p. 105 at paragraph 592)

Similar transparency issues also arise in relation to the definition of 'security clearance'[28] and 'proper place of custody'[29].

6. Offence of failing to comply with a lawful direction regarding 'inherently harmful information'

Proposed s 122.1(4) of the *Criminal Code* makes it an offence to fail to comply with a lawful direction regarding the retention, use or disposal of 'inherently harmful information' (which includes all classified information). The offence is aggravated in certain circumstances including if the person has a security clearance, making it punishable by up to 10 years' imprisonment.[30]

The term 'lawful direction' is not defined in the Bill. Nor is there any specific limitation on who may make these directions or the content of directions beyond the broad subject matter to which they must relate (being the retention, use or disposal of the relevant information, which could conceivably cover most dealings with it). This means a broad class of people (including presumably most or all supervisors) will have the ability to give directions which will effectively criminalise behaviour. Such directions may well be lawful but, in my view, it does not necessarily follow from the mere fact that a direction is lawful that there is an appropriate basis for applying criminal liability to contraventions of all such directions. The proposed offence could attach significant criminal sanctions to the breach of directions that are of a relatively trivial nature and do not, in fact, raise any realistic prospect of the relevant information being placed at risk of compromise.

There is also a risk that the application of criminal sanctions to any and all such directions may engender a punitive and defensive approach towards security compliance. This may create reluctance on the part of some officers to proactively disclose and report breaches, and may lead to the concealment of compliance issues out of fear of exposure to criminal penalty. Consideration might be given to whether further statutory parameters could be applied to the concept of a 'lawful direction' for the purpose of the new offence in proposed s 122.1(4). This could help to ensure that the proposed criminal law response is proportionate to the wrongdoing sought to be targeted, is not unduly reliant on administrative discretion to achieve this objective, and minimises the risk of unintended consequences of the kind outlined above.

---

28 *Australian Government security clearance* is not defined and would therefore have its ordinary English meaning. The Explanatory Memorandum states the policy intention is that the phrase would capture security clearances granted by the Australian Government Security Vetting Agency or another government agency conducting and issuing security clearances. It would capture, for example, security clearances from Baseline to Top Secret Positive Vetting level. (EM at p. 132 at para 759)

29 Proposed 121.2 of the *Criminal Code*, inserted by Schedule 2, item 6 at p. 52 of the Bill

30 Proposed s 122.3(1)(b)(v) of the *Criminal Code*, inserted by Schedule 2, item 6 at p. 57 of the Bill.

ATTACHMENT A

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 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 is not part of the Department of the Prime Minister and Cabinet and has separate appropriation and staffing.

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. 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.

ATTACHMENT B

Extracts of proposed s 122.5 of the Criminal Code: Offence-specific defences to the secrecy offences in proposed Division 122

122.5 Defences

Powers, functions and duties in a person's capacity as a Commonwealth officer etc. or under arrangement

(1) It is a defence to a prosecution for an offence by a person against this Division that:

(a) the person was exercising a power, or performing a function or duty, in the person's capacity as a Commonwealth officer or a person who is otherwise engaged to perform work for a Commonwealth entity; or

(b) the person dealt with, removed or held the information in accordance with an arrangement or agreement to which the Commonwealth or a Commonwealth entity is party and which allows for the exchange of information.

Note: A defendant bears an evidential burden in relation to the matters in this subsection (see subsection 13.3(3)).

***

Information communicated to the Inspector-General of Intelligence and Security, the Commonwealth Ombudsman or the Law Enforcement Integrity Commissioner

(3) It is a defence to a prosecution for an offence by a person against this Division relating to the communication of information that the person communicated the information:

(a) to any of the following:

(i) the Inspector-General of Intelligence and Security, or a person engaged or employed to assist the Inspector-General as described in subsection 32(1) of the *Inspector-General of Intelligence and Security Act 1986*;

(ii) the Commonwealth Ombudsman, or another officer within the meaning of subsection 35(1) of the *Ombudsman Act 1976*;

(iii) the Law Enforcement Integrity Commissioner, a staff member of ACLEI, or a consultant to, or a person made available to, the Integrity Commissioner under the *Law Enforcement Integrity Commissioner Act 2006*; and

(b) for the purpose of the Inspector-General, the Ombudsman or the Law Enforcement Integrity Commissioner (as the case requires) exercising a power, or performing a function or duty.

Note: A defendant bears an evidential burden in relation to the matters in this subsection (see subsection 13.3(3)).

Information communicated in accordance with the Public Interest Disclosure Act 2013

(4) It is a defence to a prosecution for an offence by a person against this Division relating to the communication of information that the person communicated the information in accordance with the *Public Interest Disclosure Act 2013*.

Note: A defendant bears an evidential burden in relation to the matters in this subsection (see subsection 13.3(3)).

ATTACHMENT C(1)

Extracts of ASIO Act and ISA secrecy offences: Exceptions to 'unauthorised dealing' and 'unauthorised recording' offences

ASIO Act

18A Unauthorised dealing with records

(See also s 18B(2A)—equivalent exception for offence of unauthorised recording of information)

Offence for unauthorised dealing with records

(1) A person commits an offence if:

(a) the person is, or has been, an entrusted person; and

(b) the person has obtained a record in the person's capacity as an entrusted person; and

(c) the record:

(i) was acquired or prepared by or on behalf of the Organisation in connection with its functions; or

(ii) relates to the performance by the Organisation of its functions; and

(d) the person engages in any of the following conduct (the ***relevant conduct***):

(i) copying the record;

(ii) transcribing the record;

(iii) retaining the record;

(iv) removing the record;

(v) dealing with the record in any other manner; and

(e) the relevant conduct was not engaged in by the person:

(i) as an ASIO employee in the course of the person's duties as an ASIO employee; or

(ii) as an ASIO affiliate in accordance with the contract, agreement or other arrangement under which the person is performing functions or services for the Organisation; or

(iii) in accordance with a contract, agreement or arrangement the person has entered into with ASIO (other than as an ASIO affiliate); or

(iv) acting within the limits of authority conferred on the person by the Director-General; or

(v) with the approval of the Director-General, or of a person having the authority of the Director-General to give such an approval.

Penalty: Imprisonment for 3 years.

***

Exception—Inspector-General of Intelligence and Security

(2A) Subsection (1) does not apply if the person deals with the record for the purpose of the Inspector-General of Intelligence and Security exercising a power, or performing a function or duty, under the *Inspector-General of Intelligence and Security Act 1986*.

Note: A defendant bears an evidential burden in relation to the matter in subsection (2A) (see subsection 13.3(3) of the *Criminal Code*).

ATTACHMENT C(2)

Extracts of ASIO Act and ISA secrecy offences: Exceptions to 'unauthorised dealing' and 'unauthorised recording' offences

ISA

40C Unauthorised dealing with records—ASIS

(See also, subsection (2A) of each of 40D-40M—equivalent exceptions to unauthorised dealing and recording offences for all ISA agencies and ONA)

(1) A person commits an offence if:

(a) the person engages in any of the following conduct (the ***relevant conduct***):

(i) copying a record;

(ii) transcribing a record;

(iii) retaining a record;

(iv) removing a record;

(v) dealing with a record in any other manner; and

(b) the record was obtained by the person by reason of:

(i) his or her being, or having been, a staff member or agent of ASIS; or

(ii) his or her having entered into any contract, agreement or arrangement with ASIS; or

(iii) his or her having been an employee or agent of a person who has entered into a contract, agreement or arrangement with ASIS; and

(c) the record:

(i) was acquired or prepared by or on behalf of ASIS in connection with its functions; or

(ii) relates to the performance by ASIS of its functions; and

(d) the relevant conduct was not engaged in:

(i) in the course of the person's duties as a staff member or agent; or

(ii) in accordance with a contract, agreement or arrangement with ASIS; or

(iii) by the person acting within the limits of authority conferred on the person by the Director-General; or

(iv) with the approval of the Director-General or of a staff member having the authority of the Director-General to give such an approval.

Penalty: Imprisonment for 3 years.

***

Exception—Inspector-General of Intelligence and Security

(2A) Subsection (1) does not apply if the person deals with the record for the purpose of the Inspector-General of Intelligence and Security exercising a power, or performing a function or duty, under the *Inspector-General of Intelligence and Security Act 1986*.

Note: A defendant bears an evidential burden in relation to the matter in subsection (2A): see subsection 13.3(3) of the *Criminal Code*.

ATTACHMENT D

Extracts of IGIS Act, s 34

34 Secrecy

(1) Subject to subsection (1A), a person who is, or has at any time been, the Inspector-General or a member of the staff of the Inspector-General or who is acting, or has at any time acted, as the Inspector-General or as a member of the staff of the Inspector-General shall not, either directly or indirectly, except in the performance of his or her functions or duties or in the exercise of his or her powers under this Act or the *Public Interest Disclosure Act 2013*:

(a) make a record of, or divulge or communicate to any person or to a court, any information acquired under this Act by reason of the person holding, or acting in, that office; or

(b) make use of any such information.

Penalty: Imprisonment for 2 years or 50 penalty units, or both.

***

(5) If a person is prohibited by this section from disclosing information, the person must not be required to:

(a) produce in a court any document of which the person has custody, or to which the person has access, because the person is performing functions or duties or exercising powers under this Act, Division 9 of Part VII or section 60A of the *Freedom of Information Act 1982* or section 50A of the *Archives Act 1983*; or

(b) divulge or communicate to a court any information obtained by the person because the person is performing those functions or duties or exercising those powers;

except where it is necessary to do so:

(ba) if the person has custody of, or access to, the document because the person is performing functions or duties or exercising powers under this Act—for the purposes of this Act; and

***

(6) In this section:

court includes any tribunal, authority or person having power to require the production of documents or the answering of questions.

produce includes permit access to.

ATTACHMENT E

Extracts of secrecy provisions of the ASIO Act (s 18D) and ISA (s 41B): Exceptions for IGIS officials

ASIO Act

18D Offences against section 18, 18A or 18B—IGIS officials

(1) A person does not commit an offence against subsection 18(2), 18A(1) or 18B(1) if:

(a) the person is an IGIS official; and

(b) the relevant conduct is engaged in by the person for the purposes of exercising powers, or performing functions or duties, as an IGIS official.

(2) In a prosecution for an offence against subsection 18(2), 18A(1) or 18B(1), the defendant does not bear an evidential burden in relation to the matter in subsection (1) of this section, despite subsection 13.3(3) of the *Criminal Code*.

ISA

41B Offences against this Division—IGIS officials

(1) A person does not commit an offence against an information offence provision if:

(a) the person is an IGIS official; and

(b) the relevant conduct is engaged in by the person for the purpose of exercising powers, or performing functions or duties, as an IGIS official.

(2) In a prosecution for an offence against an information offence provision, the defendant does not bear an evidential burden in relation to the matter in subsection (1), despite subsection 13.3(3) of the *Criminal Code*.

(3) In this section:

information offence provision means subsection 39(1), 39A(1), 40(1), 40A(1), 40B(1), 40C(1), 40D(1), 40E(1), 40F(1), 40G(1), 40H(1), 40J(1), 40K(1), 40L(1) or 40M(1).

ATTACHMENT F

Extracts from ASIO Act, s 4: definition of 'security'

security means:

(a) the protection of, and of the people of, the Commonwealth and the several States and Territories from:

(i) espionage;

(ii) sabotage;

(iii) politically motivated violence;

(iv) promotion of communal violence;

(v) attacks on Australia's defence system; or

(vi) acts of foreign interference;

whether directed from, or committed within, Australia or not; and

(aa) the protection of Australia's territorial and border integrity from serious threats; and

(b) the carrying out of Australia's responsibilities to any foreign country in relation to a matter mentioned in any of the subparagraphs of paragraph (a) or the matter mentioned in paragraph (aa).

***

acts of foreign interference means activities relating to Australia that are carried on by or on behalf of, are directed or subsidised by or are undertaken in active collaboration with, a foreign power, being activities that:

(a) are clandestine or deceptive and:

(i) are carried on for intelligence purposes;

(ii) are carried on for the purpose of affecting political or governmental processes; or

(iii) are otherwise detrimental to the interests of Australia; or

(b) involve a threat to any person.