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

Further submission to the Parliamentary Joint Committee on Intelligence and Security

The Hon Margaret Stone
Inspector-General of Intelligence and Security

13 March 2018

Introduction

The Parliamentary Joint Committee on Intelligence and Security (PJCIS or Committee) is inquiring into the National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017 (the Bill). The Inspector-General of Intelligence and Security (IGIS) made a submission to the inquiry on 22 January 2018, addressing the potential effect on IGIS of the proposed secrecy offences in Schedule 2 to the Bill (submission 13). IGIS officials appeared at a public hearing on 31 January 2018.

On 5 March 2018, the Attorney-General, the Hon Christian Porter MP, circulated and sought the views of the PJCIS on proposed Government amendments to certain provisions of Schedule 2. The Attorney-General also stated his intention to move further amendments to address several legal and practical issues identified by the IGIS, subject to the views of the PJCIS on those proposals.[1]

The Committee has invited the Inspector-General to make a further submission on the proposed amendments. This submission covers the following matters:

(1) some initial remarks on the proposals to develop additional, IGIS-related amendments, recognising that much will depend on the details of the legislative design and drafting; and

(2) issues raised in the original IGIS submission that are touched on in the proposed amendments in the Attorney-General's submission 40.1 but are not addressed by them, namely:

   (a) the definition of 'security classification' for the purpose of the new offences in relation to 'inherently harmful information';[2]

   (b) the requirements of proof in relation to the security classification assigned to information for the purpose of the above offences;[3] and

   (c) the elements of the offence of failing to comply with a lawful direction about 'inherently harmful information'.[4]

Proposals for further amendments—IGIS-related measures

I welcome the Attorney-General's statement of intention to amend Schedule 2 to the Bill to address several of the matters that I have raised with the PJCIS. I have also had the benefit of a preliminary discussion with the Attorney-General on these matters.

I support, in principle, the three proposals for further amendments to the Bill set out in the Attorney-General's letter of 5 March (submission 40 at pp. 4-5). These measures concern:

(1) the removal of the evidential burden from IGIS officials in relation to the defences in proposed section 122.5 of the *Criminal Code Act 1995* (*Code*). This would take account of the burden that the Bill, as introduced, would have placed upon IGIS officials, due to the secrecy provisions of the *Inspector-General of Intelligence and Security Act 1986* (*IGIS Act*) making it

---

1 Attorney-General, Submission to the PJCIS, *Submission 40*, pp. 4-5.

2 IGIS, Submission to the PJCIS, *Submission 13*, p. 2 and pp. 7-8 (key issue 5); and J Blight (Deputy IGIS) *Committee Hansard*, Canberra, 31 January 2018, pp. 5-6 and 12.

3 Above n. 2.

4 IGIS, Submission to the PJCIS, *Submission 13*, p. 2 and p. 9 (key issue 6); and J Blight (Deputy IGIS) *Committee Hansard*, Canberra, 31 January 2018, pp. 12-13.

impossible, for all practical purposes, for them to discharge the evidential burden without committing an offence under the *IGIS Act*;

(2) the extension of the offence-specific defences in proposed subsections 122.5(3) and (4) to cover persons who deal with 'inherently harmful information' for the purpose of making a communication or a public interest disclosure (PID) to the IGIS, without also requiring proof of the ultimate communication. This amendment would provide an explicit legal protection for actions done at all stages in the process of communicating information to the IGIS; and

(3) the inclusion of a provision to the effect that the defences to the proposed secrecy offences in new Division 122 of the *Code* do not affect any immunities that exist in other legislation, such as the immunities from liability to penalty under the *IGIS Act* and the *Public Interest Disclosure Act 2013* (*PID Act*).

I am optimistic that, subject to my consideration of specific provisions, these proposals have the potential to resolve the key legal and practical issues for the IGIS that I have raised with the PJCIS.[5]

The need to scrutinise draft provisions

Much will turn upon matters of detail in the design and drafting of the proposed amendments. A more definitive opinion on the effectiveness of the proposals would require an opportunity to consider and comment on specific provisions. If draft provisions were referred to this Committee for a similar process of scrutiny to that presently being given to the provisions in submission 40.1, then I would be grateful for the opportunity to contribute my views to that process.

To assist the Committee in its initial consideration of the three proposals, I provide the following preliminary comments on each measure, based on the information presently available.

Removal of the evidential burden on IGIS officials in new section 122.5

I support, in principle, the proposal to amend new section 122.5 to provide that IGIS officials do not bear the evidential burden in relation to the offence-specific defences for communicating or dealing with 'inherently harmful information'.[6] Specifically, I support the removal of the evidential burden on IGIS officials to establish that they were IGIS officials, and that they communicated or dealt with the information in that capacity. This is consistent with my submission of 22 January 2018.[7]

These amendments will ensure that IGIS officials are not placed in the untenable situation of being exposed to criminal liability for doing no more than performing their duties, and are then unable to discharge the evidential burden in relation to a defence without contravening the secrecy provisions in section 34 of the *IGIS Act*.

Amendments of this kind will resolve my concerns in a way that maintains the important secrecy obligations applying to IGIS officials under section 34 of the *IGIS Act*. These obligations are essential to maintaining the security and integrity of the highly classified and other sensitive information that is obtained and used by my Office to perform its functions, and in giving agencies and others an assurance that their information is secure and cannot be used for any other purpose.

---

5 These issues are set out in: IGIS, Submission to the PJCIS, *Submission 13*, pp. 2 and 3-5 (key issues 1-3); and J Blight (Deputy IGIS) *Committee Hansard*, Canberra, 31 January 2018, pp. 9-11.

6 Attorney-General, Submission to the PJCIS, *Submission 40*, p. 5.

7 IGIS, Submission to the PJCIS, *Submission 13*, pp. 5-6.

While it is not possible to give unqualified support to the proposals without considering draft provisions, my general observation is that the equivalent 'information offence provisions' enacted in 2014 in section 18D of the *Australian Security Intelligence Organisation Act 1979* (*ASIO Act*) and section 41B of the *Intelligence Services Act 2001* (*ISA*) would provide a sound precedent.[8] I am supportive of amendments that reflect the *ASIO Act* and *ISA* provisions as closely as possible.

Extension of the matters covered by subsections 122.5(3) and (4)

The Attorney-General has indicated an intention to move amendments that will broaden the matters in the offence-specific defences in proposed subsections 122.5(3) and (4) 'to cover all dealings with information'.[9]

I understand this to mean there will be defences to cover both communications made to the IGIS, and dealings with information for the purpose of communicating it to the IGIS without also requiring proof of the ultimate communication.

I am supportive, in principle, of amendments to this effect. They would ensure that people who deal with information for the purpose of communicating it to the IGIS, but have not yet done so or are prevented from doing so, are not deprived of a defence to a serious offence.[10]

The drafting of the relevant provisions would warrant careful scrutiny. This comment applies to an assessment of the technical effect of the relevant provisions, and their likely practical effectiveness in providing an assurance to people who would be required to rely on a defence that all stages of their dealing with information for the purpose of communicating it to my Office are covered. My submission of 22 January identified certain provisions of the *ASIO Act* and *ISA* that would provide an effective model. These provisions cover dealings with information for the purpose of the IGIS performing functions or duties or exercising powers.[11]

Relationship of the proposed secrecy offences with other immunities

Consistent with my submission of 22 January,[12] I consider that there would be benefit in the insertion of a provision that contains an explicit statement of the Parliament's intention that the offences in proposed Division 122 'do not affect any immunities that exist in other legislation'.[13]

In the case of the IGIS, such 'other legislation' would include the statutory immunity from liability to penalty under subsection 18(9) of the *IGIS Act* for persons who provide information to my inquiries in compliance with a statutory notice issued under subsection 18(1) or (3) of my Act. It would also include the immunities from liability under sections 10 and 78 of the *PID Act* for persons who make and investigate PIDs.

---

8 *National Security Legislation Amendment Act (No 1) 2014*. These provisions implemented a recommendation of the PJCIS that the offence provisions should not apply to communications or other disclosures to or by IGIS officials: PJCIS, *Advisory Report on the National Security Legislation Amendment Bill (No 1) 2014*, September 2014 (recommendation 14 and reasoning at pp. 66-67).

9 Attorney-General, Submission to the PJCIS, *Submission 40*, p. 4.

10 IGIS, Submission to the PJCIS, *Submission 13*, pp. 4-5.

11 IGIS, Submission to the PJCIS, *Submission 13*, p. 5.

12 IGIS, Submission to the PJCIS, *Submission 13*, p. 4.

13 Attorney-General, Submission to the PJCIS, *Submission 40*, p. 5.

A provision of this kind would substantially resolve the concerns raised in my submission, subject to the two matters outlined below. The first concerns the framing of the matters in proposed subsections 122.5(3) and (4) as defences or exceptions to the offences in Division 122. The second matter is ensuring that legal protection for people who provide information to my Office on a voluntary basis is equal to the protection of those who do so under compulsion in an inquiry.

Defences v exceptions

On the first issue, the Attorney-General has remarked that it is not considered necessary for the matters in proposed subsections 122.5(3) and (4) to be framed as exceptions, as is the case for similar provisions in the *ASIO Act* and *ISA* that were inserted on the recommendation of this Committee in 2014. This position appears to be premised on the view that rules on the allocation of evidential burden under subsection 13.3(3) of the *Code* are relevant to the interaction between defences and immunities that cover the same ground.[14]

Rules regarding the allocation of evidential burden are not relevant to concerns about the framing of the offences and defences raised in my submission. My concern is to eliminate the potential for uncertainty or argument as to whether the offences impliedly abrogate existing immunities and *replace them* with offence-specific defences.[15] I am also concerned about the non-legal risk that people may be less willing to come forward to IGIS if they must rely upon a defence to a serious criminal offence to do so.

It should be possible for these concerns to be managed through a provision of the kind detailed above that explicitly records the Parliament's intention for the *IGIS Act* and *PID Act* immunities to prevail, such that the new offences do not apply to conduct covered by those immunities. As explained below, additional protections would be necessary for persons who provide information voluntarily to my Office and are not covered by existing statutory immunities.

Protection of persons who voluntarily provide information to the IGIS

The effectiveness of a 'relationship with other laws' provision would be dependent on the scope of immunities in other legislation (such as the *IGIS Act* or *PID Act*).

In contrast with the *Ombudsman Act*, the *IGIS Act* presently contains no immunity from liability for persons who provide information to my Office on a voluntary basis.[16] For example, there is no statutory immunity for complainants and agency officials who may variously communicate information to my Office in compliance with my requests for information in inspections, preliminary inquiries into complaints, and inquiries in which I elect not to issue a notice to produce.

---

14 Attorney-General, Submission to the PJCIS, *Submission 40*, p. 5.

15 For example, section 10 of the *PID Act* confers an immunity from legal liability on persons who make public interest disclosures (PIDs), and section 24 provides that section 10 applies despite any other Commonwealth law. However proposed subsection 122.5(4) of the *Code* contains a *defence* to the offences in Division 122 that the person communicated information for the purpose of making a PID (the same conduct that is covered by the immunity in the *PID Act*).

16 The immunity from liability in subsection 18(9) of the *IGIS Act* currently extends to persons who provide information to the IGIS in compliance with a notice to produce issued under section 18 as part of an inquiry conducted under Part II of the *IGIS Act*. The *Ombudsman Act* confers immunity on persons who voluntarily provide information in preliminary inquiries into complaints and investigations: subsections 7A(1C) and 8(2C).

There is also no immunity under the *IGIS Act* for complainants or agency officials who provide information to my Office on a proactive or otherwise unsolicited basis, such as disclosures of identified breaches or complaints made under the *IGIS Act* about the legality or propriety of an agency's actions.

While there are circumstances in which a person who provides information to my Office will be subject to the immunity in section 10 of the *PID Act* because their communication is a PID, not all persons who disclose information to my Office do so by way of making a PID. This may be because the person is not a 'public official', or because their disclosure does not relate to 'disclosable conduct' by the relevant agency within the meaning of the *PID Act*, or because the disclosure is not made to an 'authorised officer' under the *PID Act*.

These persons are currently protected by an absence of applicable criminal offences to their conduct in communicating information to my Office, rather than a positive statutory immunity. The offences in proposed section 122.1 of the Bill will, if enacted in their present form, change this position. In the absence of an immunity, people who provide information to my Office on a voluntary basis would satisfy the elements of the proposed offences' and would be wholly reliant on the defence to an offence under proposed section 122.1 (or an aggravated offence under section 122.3). They would have less legal protection than those who provide information under compulsion. This significant difference would arise only by reason of the technical legal basis upon which the person provided the information, rather than the substance of the information itself.

The need for equal legal protections

People who provide information to my Office voluntarily should, in my view, be accorded legal protection equal to that available to to those who do so compulsorily in an inquiry. Equality of protection will be particularly important if the Parliament passes legislation to implement the Government's decision to extend my oversight to cover the intelligence functions of an additional four agencies, being the Australian Criminal Intelligence Commission, the Australian Federal Police, the Australian Transaction Reports and Analysis Centre and the Department of Home Affairs.[17]

These agencies, and persons who may wish to complain about their activities, are accustomed to oversight by the Ombudsman, and the attendant immunities under the *Ombudsman Act* for the voluntary provision of information. Accordingly, the nature and strength of their protection from liability under proposed Division 122 of the *Code* (that is, whether they have immunity as of right, or whether they would be exposed to prosecution and required to rely on a defence) would be determined by reference to whether they complain to the IGIS or the Ombudsman.

Possible legislative solutions

If there is no intention to cast the matters in proposed subsections 122.5(3) and (4) as exceptions, or to limit the elements of the offences in proposed section 122.1, then I ask that consideration is given to extending the statutory immunities under the *IGIS Act* to persons who provide information voluntarily. If such a provision were included in the *IGIS Act* it would also need to make clear, preferably by its express terms, an intention for the immunity to prevail over laws that would

17 This decision is recorded in: Senator the Hon James McGrath, *Portfolio Additional Estimates Statements 2017-2018, Prime Minister and Cabinet Portfolio*, 1 February 2018, p. 33.

otherwise expose the person to a penalty for providing the information or documents to my Office, such as proposed Division 122 of the *Code.*[18]

Other issues not addressed in the proposed amendments

The draft Government amendments circulated to the PJCIS in Submission 40.1 touch on some of the 'other issues' raised in my submission of 22 January but do not address them fully. These issues concern:

(1) the definition of 'security classification' for the purpose of the new offences in relation to 'inherently harmful information';[19]

(2) the requirements of proof in relation to the security classification of information for the purpose of those offences;[20]

(3) the breadth of the offence of failing to comply with a lawful direction about 'inherently harmful information'.[21]

The definition of 'security classification'

The draft Government amendments to the Bill place some limitations on the definition of 'security classification' in new subsection 90.5(1) of the *Criminal Code Act 1995* (*Code*). The term, as amended, would cover information classified as SECRET or TOP SECRET or any other 'equivalent' classification that is prescribed by the regulations.[22] The regulations must not be inconsistent with Commonwealth protective security policy, and may incorporate by reference any instrument or other writing as in force or existing from time-to-time.[23]

The terms SECRET and TOP SECRET are not defined legislatively, and would presumably be intended to take their meaning, for the purpose of the offences in the *Code*, from the *Protective Security Policy Framework* (*PSPF*) or other relevant administrative materials as in force from time-to-time. The current definitions of these terms in the *PSPF* are assigned on the basis of the degree of damage to the national interest, organisations or individuals that could arise from unauthorised release.[24] Accordingly, the definition, as amended, would not prescribe any minimum legal requirements or parameters for the content of the definition of the terms SECRET or TOP SECRET, as incorporated in the *Code* for the purpose of the new offences. These terms would take their meaning *exclusively* from policy as in force from time-to-time. (For example, there is no legislative requirement that the

---

18 An example of such a provision is found in the *PID Act*, section 24. (Alignment of the immunity provision with that in the *PID Act* would also be important to achieve equality of protection under the *IGIS Act* with that accorded to PIDs under the *PID Act*.)

19 IGIS, Submission to the PJCIS, *Submission 13*, p. 2 and pp. 7-8 (issue 5); and J Blight (Deputy IGIS) *Committee Hansard*, Canberra, 31 January 2018, pp. 5-6 and 12.

20 See also the above references to the IGIS submission and evidence.

21 See also: IGIS, Submission to the PJCIS, *Submission 13*, p. 2 and p. 9 (issue 6); and J Blight (Deputy IGIS) *Committee Hansard*, Canberra, 31 January 2018, pp. 12-13.

22 Attorney-General, Submission to the PJCIS, *Submission 40.1*, amending item 1.

23 Proposed subsections 90.5(2) and (3).

24 Australian Government, *Information security management guidelines: security classification system*, version 2.2, amended April 2015, pp. 8-9 (protective markings) and pp. 6-7 (how to identify national interest information).

security classifications to which the new offences apply must be, or must only be, based on the degree of damage to the national interest that unauthorised release of the information could cause.)

There is also no legislative requirement that any administrative documents defining the security classifications named in the amendments to new subsection 90.5(1) must be available publicly. This includes material that is incorporated by reference in the regulations prescribing 'equivalent' classifications under proposed subsection 90.5(2). I note that the supplementary submission of the Attorney-General's Department to the PJCIS commented that new section 90.5 could specifically include a requirement that any documents incorporated into the definition of 'security classified information' must be publicly available.[25]

Comment

In my submission of 22 January, I supported consideration of further statutory parameters for the regulation-making power in new section 90.5. I supported the inclusion of a legislative requirement that any material incorporated by reference into regulations must be publicly available. I also supported a legislative requirement that a 'security classification' within the meaning of section 90.5 must be a classification that is assigned for the purpose of protecting national security.[26] These remain my views in relation to the provision in its amended form.

Requirements of proof—security classified information

The offences in new Division 122 of the *Criminal Code* applying to 'inherently harmful information' that is 'security classified information' do not include a requirement to establish that the 'security classification' assigned to the information was accurate at the time of the conduct constituting the alleged offence.

Comment

I remain of the view that such a requirement would be desirable, for the reasons set out in my submission of 22 January.[27] I support the inclusion of such a requirement as a condition precedent to the initiation of a prosecution. Such a condition could be given effect by an equivalent (non-evidentiary) certification requirement to that in section 50A of the *Australian Border Force Act 2015* (*ABF Act*) in relation to the secrecy offences in that Act.[28]

I note the views expressed on section 50A of the *ABF Act* in the supplementary submission of the Attorney-General's Department. It was suggested that the accuracy or appropriateness of a classification at the time of the conduct constituting the offence is a matter of opinion that would be

25 Attorney-General's Department, Submission to the PJCIS, *Submission 6.1*, p. 39.

26 IGIS, Submission to the PJCIS, *Submission 13*, pp. 7-8; and J Blight (Deputy IGIS) *Committee Hansard*, Canberra, 31 January 2018, pp. 5-6 and 12.

27 IGIS, Submission to the PJCIS, *Submission 13*, pp. 7-8. See also: J Blight (Deputy IGIS) *Committee Hansard*, Canberra, 31 January 2018, pp. 5-6 and 12.

28 *ABF Act,* section 50A provides: 'If an offence against section 42 relates to information that has a security classification, proceedings for the offence must not be initiated unless the Secretary has certified that it is appropriate that the information had a security classification at the time of the conduct that is alleged to constitute the offence'.

unsuitable for inclusion in an *evidentiary certificate* issued by the Attorney-General.[29] A certificate of the kind specified in section 50A of the *ABF Act* is not an evidentiary certificate (in the sense of being prima facie evidence of a matter in a prosecution or any other proceedings). Rather, it is a condition precedent to the commencement of a prosecution.[30] The reasons that a matter of opinion could not properly form the basis for such a condition are not readily apparent.

The existence of such a condition in the *ABF Act*, and the absence of such a condition in new Division 122 of the *Code*, may also produce an anomalous result. If the Bill is passed, an unauthorised disclosure of 'security classified information' could potentially constitute an offence under both Acts. A prosecution for a disclosure offence under section 42 of the *ABF Act* would be subject to the certification condition in section 50A. That offence applies a maximum penalty of two years' imprisonment. A prosecution for an offence against proposed subsection 122.1(1) of the *Code* would apply a maximum penalty of 15 years' imprisonment (or 20 years' imprisonment if the offence is aggravated under proposed section 122.3). The more serious offences in the *Code* would not contain an equivalent condition to the commencement of a prosecution to that applying to the less serious offence in the *ABF Act*.

Offence of failing to comply with a lawful direction about the handling of 'inherently harmful information'

The offence of failing to comply with a lawful direction about the retention, use or disposal of 'inherently harmful information' in proposed subsection 122.1(4) does not require proof that the contravention of the direction, in fact, placed at risk the security of that information to unauthorised access or disclosure. There is also no requirement that the direction must be issued for the purpose of protecting the security of the information to which it relates.[31]

The underlying policy appears to be that the risk of harm to the security of information is considered to be implicit in the fact of the assignment of a security classification (or the establishment of another limb of the definition of 'inherently harmful information'). In response to the IGIS submission of 22 January, the Attorney-General's Department commented:

> The department's view is that when a person is dealing with the type of harmful information that is covered by the offences in Schedule 2, it is important that lawful directions about the retention, use or disposal of the information are complied with. The department does not agree with the assertion that breach of such directions are necessarily 'relatively trivial', when taking into account the nature of the information covered by the offences.[32]

29 Attorney-General's Department, Submission to the PJCIS, *Submission 6.1*, pp. 4-5.

30 See also: Explanatory Memorandum, Australian Border Force Amendment (Protected Information) Bill 2017, p. 18 at [67]: 'It is not proposed that the Secretary's certificate is an evidentiary certificate'.

31 See further: IGIS, Submission to the PJCIS, *Submission 13*, p. 9.

32 Attorney-General's Department, Submission to the PJCIS, *Submission 6.1*, p. 39.

Comment

I continue to support the application of further statutory parameters to the concept of a 'lawful direction' for the purpose of the offence in proposed subsection 122.1(4) for the reasons provided in my submission of 22 January.[33] I am supportive of the insertion of an additional element into the offence, which requires the direction to have been issued for the purpose of protecting the security of the information against unauthorised access or disclosure.

I remain of the view that the risk of compromise or other harm to security is not inherent in the combination of the nature of the information and the mere fact of its use, retention or disposal in contravention of *any* lawful direction about those matters. It is conceivable that a direction about use, retention or disposal of information may have no bearing upon the protection of the security of that information.

For example, the following directions about the retention or use of classified information would appear to be lawful, in the sense of not contravening applicable laws and being reasonably open to the issuer to make. Their contravention could, nonetheless, constitute an offence under new subsection 122.1(4):

- A direction to store a document of a particular classification (such as SECRET) in one safe and not another, purely for reasons of convenience of access by authorised persons within an agency. Each safe could possess the same security specifications (for example, 'Class B') and could be subject to identical access controls that restrict access to the same persons, all of whom are authorised to access the relevant information.
- A direction to contact another person at, or by, a particular time and disseminate a piece of security classified information that is relevant to the sending and receiving agencies' functions, although the appointed deadline is not critical to the performance of those functions. (Noting that the 'use' of information could conceivably cover its dissemination.)

33 IGIS, Submission to the PJCIS, *Submission 13*, p. 9.