Review of the Security of Critical Infrastructure Bill 2017

Submission to the Parliamentary Joint Committee on Intelligence and Security

The Hon Margaret Stone
Inspector-General of Intelligence and Security

16 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 is limited to the identification of a technical issue in the Security of Critical Infrastructure (Consequential and Transitional Provisions) Bill 2017 (CTP Bill). It concerns a consequential amendment to the *Australian Security Intelligence Organisation Act 1979* (ASIO Act).

I make no comment on the substantive regulatory regime proposed in the Security of Critical Infrastructure Bill 2017 (the Bill) beyond observing that that it is unlikely to raise substantial oversight implications for my Office. The majority of the new functions and powers are conferred on the Minister administering the new Act and the Secretary of the relevant portfolio Department. Other than in the case of certain inquiries directed by the Prime Minister, the *Inspector-General of Intelligence and Security Act 1986* (IGIS Act) limits my oversight to the legality and propriety of the actions of intelligence agencies, and generally excludes from inquiry the actions of Ministers.[1] Further, the main role of ASIO under the new scheme appears to be the issuing of security assessments under Part IV of the *ASIO Act* in relation to critical infrastructure operators and service providers (termed 'responsible entities' in clause 5 of the Bill). The issuing of an adverse security assessment (ASA) is a condition precedent to the Minister exercising the power to issue a direction that requires a responsible entity to do, or refrain from doing, a specified act or thing on security related grounds.[2] ASAs issued in connection with the proposed scheme would be subject to merits review by the Security Division of the Administrative Appeals Tribunal (AAT).[3] Paragraph 9AA(c) of the *IGIS Act* provides that my functions do not include inquiring into matters that are, or could be, the subject of review by the Security Division of the AAT.

Ability to withhold notice of the issuing of an ASA under s 38 of the ASIO Act

Adverse security assessments issued in relation to 'responsible entities' under the Bill would be subject to the requirements of section 38 of the *ASIO Act*. In accordance with that section the entity must be given written notice of the making of the assessment, including a copy of the assessment and notice of its right to apply to the Security Division of the AAT for merits review of the assessment.[4] This notification requirement is subject to the Attorney-General issuing a certificate declaring, among other matters, that withholding a notice from the entity is essential to the security of the nation.[5] If the Attorney-General issues such a certificate, the notice requirements in section 38 do not apply to the security assessment.[6] Accordingly, the application of the certification scheme

---

1 *IGIS Act,* section 8 (intelligence agency inquiry functions), subsection 9(3) (inquiries into intelligence or security matters relating to Commonwealth agencies on the direction of the Prime Minister) and paragraph 9AA(b) (prohibition on inquiring into action taken by a Minister).

2 Security of Critical Infrastructure Bill, subclause 32(3)(c). See also: Security of Critical Infrastructure (Consequential and Transitional Provisions) Bill 2017, Schedule 1, item 1 (amendment to the definition of 'prescribed administrative action' in section 35 of the *ASIO Act,* which will enable ASAs to be issued in connection with the Ministerial directions power in clause 32 of the Bill).

3 *ASIO Act,* Part IV, Division 4.

4 *ASIO Act*, subsection 38(1).

5 *ASIO Act*, paragraph 38(2)(a). (Paragraph 38(2)(b) also allows the statement of grounds contained in a security assessment to be withheld from the person, if disclosure would be prejudicial to security.)

6 *ASIO Act*, subsection 38(4).

in section 38 of the ASIO Act creates the possibility that a 'responsible entity' could be the subject of a Ministerial direction under the scheme proposed in the Bill, but may not receive notice of the making of the ASA or the entity's right to seek review of the ASA in the AAT, if the Attorney-General issues a certificate under paragraph 38(2)(a). In this event, it would fall to the responsible entity to infer from the issuing of the Ministerial direction that it was the subject of an ASA, and to independently inform itself of its right to seek merits review of the ASA. This outcome could effectively deprive some responsible entities of an opportunity to exercise their review rights. It would yield no apparent benefit to security, as the making of the Ministerial direction would necessarily reveal the existence of the ASA. In my view, it would be preferable if there was no power to withhold notice of the issuing of an ASA in connection with the exercise of the Ministerial directions power in clause 32 of the Bill. Rather, it should only be possible to withhold so much of the contents of the ASA attached to the notice as is necessary to avoid causing prejudice to security. A simple legislative solution would appear to be available (summarised below).

Possible solution: consequential amendments to s 38A of the ASIO Act

Adverse security assessments issued in connection with the Ministerial directions power in clause 32 of the Bill could be made subject to the separate notification requirements in section 38A of the *ASIO Act*, rather than the general notification requirements (and Ministerial certification-based exceptions) in section 38. The separate requirements in section 38A currently apply to ASAs that are issued in connection with certain Ministerial directions given under the *Telecommunications Act 1997.*[7] Subsection 38A(3) of the *ASIO Act* does not allow a notice of the issuing of such an ASA to be withheld from the assessed entity. It permits only the exclusion of certain information from the copy of the assessment that is attached to the notice. This is provided that the relevant Minister is satisfied that the disclosure of that information would be prejudicial to the interests of security. Importantly, all of the types of prescribed administrative action to which section 38A applies are Ministerial directions under the *Telecommunications Act* that can only be made on security related grounds. The Explanatory Memorandum to the legislation enacting section 38A indicates that, for this reason, a power to withhold notice of the making of an ASA, and attendant review rights, was considered unnecessary.[8]

The modified notification requirements in section 38A apply to ASAs issued in connection with Ministerial directions given to telecommunications carriers and service providers under sections 315A and 315B of the *Telecommunications Act.* These provisions were enacted as part of the telecommunications sector security reforms (TSSR).[9] The critical infrastructure scheme is modelled on the TSSR measures.[10] Aligning the notification requirements for ASAs issued in connection with each scheme would ensure the equal treatment of regulated entities in this regard.

---

7 *ASIO Act*, subsection 38A(1). These are directions issued under the *Telecommunications Act* on security related grounds to the following entities: telecommunications carriers and carriage service providers, requiring them to cease providing a service or to do, or cease doing, certain things in connection with the provision of a service (ss 315A and 315B); and the ACMA, requiring it to refuse to issue a carrier licence (s 58A), and to refuse to grant installation permits in relation to submarine cables (Sch 3A, cls 57A, 72A).

8 Supplementary EM, Communications Legislation Amendment Bill (No 1) 2004, pp. 3-4.

9 *Telecommunications and Other Legislation Amendment Act 2017*, Schedule 1, item 34 (inserting a new paragraph 38A(1)(b) in the *ASIO Act*). These amendments will commence on 18 September 2018.

10 This policy intention is stated explicitly in the extrinsic materials to the Bill. See: the Hon M Cormann, Second Reading Speech, Senate, *Debates*, 7 December 2017, p. 10096.

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.