

**OFFICIAL**



---

## **Review of the Security Legislation Amendment (Critical Infrastructure) Bill 2020**

---

**Submission to the  
Parliamentary Joint Committee on Intelligence and Security**

The Hon Dr Christopher Jessup QC  
Inspector-General of Intelligence and Security

23 March 2021

**OFFICIAL**

## 1. INTRODUCTION

1. The Inspector-General of Intelligence and Security (IGIS) welcomes the opportunity to make this submission to the Parliamentary Joint Committee on Intelligence and Security's (the Committee) review of the *Security Legislation Amendment (Critical Infrastructure) Bill 2020* (the Bill).
2. The Inspector-General is an independent statutory officer who reviews the activities of the Australian Security Intelligence Organisation (ASIO), the Australian Secret Intelligence Service (ASIS), the Australian Signals Directorate (ASD), the Australian Geospatial-Intelligence Organisation (AGO), the Defence Intelligence Organisation (DIO) and the Office of National Intelligence (ONI). The overarching purpose of IGIS's activities is to provide assurance that each intelligence agency acts legally and with propriety, complies with ministerial guidelines and directives, and respects human rights. The Hon Dr Christopher Jessup QC commenced as the Inspector-General on 8 February 2021 (having been acting Inspector-General since 18 January 2021).
3. As is its usual practice, IGIS does not express a view on the policy aspects of the Bill, except to the extent that IGIS oversight is affected. Accordingly, this submission focuses on the implications of the Bill for oversight of the agencies in the IGIS jurisdiction, specifically, ASD.
4. The Department of Home Affairs consulted with IGIS during the development of the Bill. Key features of the Bill relevant to IGIS oversight include:
  - authority for ASD to assist and cooperate with the Department of Home Affairs in respect of any of the Department's functions (i.e. not just in respect of the critical infrastructure framework proposed in the Bill);
  - possible legal and practical impediments to persons making complaints arising from the scheme to relevant oversight bodies, including IGIS;
  - authority for ASD to use information domestically obtained in the course of exercising powers or functions under the Act for any of its other functions; and
  - the applicability of broad criminal and civil immunity for staff of ASD in respect of acts performed in accordance with the framework.

## 2. OVERSIGHT OF THE FRAMEWORK

5. IGIS's existing jurisdiction under the *Inspector-General of Intelligence & Security Act 1986* (the IGIS Act) would enable IGIS to oversee ASD's conduct under the framework proposed by the Bill. As is the case under the IGIS Act at present, IGIS would not have authority to oversee Ministerial action taken or not taken in accordance with the framework set out in the Bill. Similarly, IGIS would not oversee the activities of the Secretary of the Department of Home Affairs or his or her Department in its exercise of functions under the framework, as these do not fall within IGIS's jurisdiction. It is proposed that the Commonwealth Ombudsman would oversight certain other aspects of the framework within its current mandate.<sup>1</sup>
6. The proposed framework envisages a shared oversight regime between the Ombudsman and IGIS. Attachment B to the Explanatory Memorandum states that 'the Commonwealth Ombudsman, within its current mandate, would have the ability to receive, consider and take action in relation to complaints made by an entity in relation to a direction issued by the Secretary of Home Affairs under this power or the Australian Federal Police's actions in supporting the Australian Signals Directorate.'<sup>2</sup>

---

<sup>1</sup> *Explanatory Memorandum*, Attachment A, paragraphs 21, 1047 and 1058 and Attachment B, *Regulatory Impact Statement*, p. 20.

<sup>2</sup> *Explanatory Memorandum*, Attachment B, *Regulatory Impact Statement*, p. 20.

**OFFICIAL**

**IGIS EVIDENTIARY CERTIFICATES**

7. The Bill also proposes to provide IGIS with the authority to ‘issue a written certificate setting out any facts relevant to the question of whether anything done, or omitted to be done, by the authorised agency, or an approved staff member of the authorised agency, was done, or omitted to be done, in the exercise of any power or authority conferred by this Division’.<sup>3</sup>
8. Such a certificate would be prima facie evidence of the matters stated in the certificate and would found a claim by ASD to immunity from proceedings arising in connection with the execution of an intervention request under proposed section 35AX.<sup>4</sup>

**BRIEF OVERVIEW OF ASD’S ROLE UNDER THE PROPOSED FRAMEWORK**

9. Broadly, under the Bill, ASD:
  - would be the default recipient of mandatory reports concerning cyber security incidents;
  - may be appointed as a mandatory observer of industry cyber security exercises;
  - may be designated as the recipient of regular reports on the operation of systems of national significance; and
  - would be empowered to intervene domestically, including by coercive means, in response to a cyber security incident.
10. These roles would be accompanied by auxiliary functions, powers or immunities, including civil and criminal immunity for conduct in the course of exercising intervention powers. ASD would be able to use any information gathered in the course of exercising these functions for the purposes of any of ASD’s other legislative functions set out under the *Intelligence Services Act 2001* (the IS Act).

**3. ASPECTS OF THE BILL IMPACTING OVERSIGHT**

**INTELLIGENCE SERVICES ACT REGULATIONS**

11. Proposed section 35AZ provides:
  - (1) The authorised agency is authorised to do an act or thing in compliance with a request under section 35AX.<sup>5</sup>
  - (2) An act or thing done by the authorised agency in compliance with a request under section 35AX is taken to be done in the performance of the function conferred on the authorised agency by paragraph 7(1)(f) of the *Intelligence Services Act 2001*.<sup>6</sup>
12. The Explanatory Memorandum indicates that this section is intended to operate as a deeming provision, such that any act done by ASD in accordance with a request under section 35AX is taken to be done in accordance with ASD’s functions under paragraph 7(1)(f) of the IS Act. Paragraph 7(1)(f) of the IS Act provides a general function for ASD to cooperate with other government agencies listed in the regulations issued under section 13A of the IS Act.
13. Separate to this Bill, draft regulations were released by the Department of Home Affairs as part of a public consultation process in November 2020. A draft explanatory statement to the draft regulations was issued at the same time. This draft statement, in stating the policy intention of the Regulations, said that the Regulations ‘are intended to enable ASD under paragraph 7(1)(f) of the Act to cooperate with and assist the Home Affairs Department in the exercise of powers and

---

<sup>3</sup> Item 45 of Schedule 1.

<sup>4</sup> Item 45 of Schedule 1.

<sup>5</sup> Intervention requests, as proposed in Item 45 of Schedule 1, proposed section 35AX.

<sup>6</sup> Item 45 of Schedule 1.

**OFFICIAL**

performance of functions under the SOCI Act.<sup>7</sup> IGIS acknowledges this intention, but notes that the draft Regulations, in their current form, would be of general application and would provide scope for ASD to co-operate with the Department of Home Affairs more broadly. Such cooperation would be subject to any arrangements or directions given by the responsible Minister (in this case, the Minister for Defence).<sup>8</sup>

**INFORMATION SHARING AND DISCLOSURE OF ‘PROTECTED INFORMATION’**

14. The Bill would introduce a range of new circumstances to which the prohibited use and disclosure provisions in section 45 of the SOCI Act would not apply. Those exceptions relate to disclosures by the Secretary of Home Affairs to IGIS officials,<sup>9</sup> disclosures as between Ombudsman officials and IGIS officials,<sup>10</sup> and disclosures within ASD for the purposes of the performance of its functions under section 7 of the IS Act.<sup>11</sup>
15. Those exceptions would not apply to disclosures to IGIS by others not mentioned, such as staff employed in ASD or Home Affairs, regulated entities<sup>12</sup> or third parties. However, such disclosures would be protected by existing provisions of the IGIS Act, whether the disclosures were under compulsion<sup>13</sup> or were voluntary.<sup>14</sup>
16. One category of disclosure which is not the subject of an exception from the operation of section 45 of the SOCI Act, either in the existing legislation or in the Bill, is a disclosure between IGIS officials made for the purpose of exercising functions under the IGIS Act. A precedent for an exception of this kind is to be found in section 41B of the IS Act. A similar, albeit not identically-worded, exception has been made for ASD staff in the Bill itself,<sup>15</sup> but disclosures as between IGIS officials have not been dealt with in the same way.
17. IGIS suggests that, to ensure that there are no barriers (perceived or otherwise) to its oversight, an amendment to the Bill be considered to permit IGIS staff to communicate prohibited information to each other.<sup>16</sup>

---

<sup>7</sup> Draft Explanatory Statement accompanying the exposure draft of the proposed *Intelligence Services Regulations 2020*, page 1.

<sup>8</sup> IS Act, paragraph 13(2)(a).

<sup>9</sup> Item 50 of Schedule 1, proposed section 43A.

<sup>10</sup> Item 50 of Schedule 1, proposed sections 43B and 43C.

<sup>11</sup> Item 50 of Schedule 1, proposed section 43D.

<sup>12</sup> We note that paragraph 45(4)(b) of the existing SOCI Act exempts entities from the prohibition against disclosing protected information where the information relates to the entity.

<sup>13</sup> IGIS Act, subsection 18(9).

<sup>14</sup> IGIS Act, section 34B.

<sup>15</sup> Item 50 of Schedule 1, proposed section 43D.

<sup>16</sup> See proposed sections 43A and 43C of the Bill.