Australian Government
Office of the Australian Information Commissioner

Review of the Security Legislation Amendment (Critical Infrastructure) Bill 2020 – Submission to the Parliamentary Joint Committee on Intelligence and Security

Angelene Falk
Australian Information Commissioner and Privacy Commissioner
22 February 2020

OAIC

Contents

1. Introduction

1. The Office of the Australian Information Commissioner (OAIC) welcomes the opportunity to provide this submission to the Parliamentary Joint Committee on Intelligence and Security (Committee) on the Security Legislation Amendment (Critical Infrastructure) Bill 2020 (Bill).[1] The draft Bill seeks to introduce "an enhanced regulatory framework, building on existing requirements under the *Security of Critical Infrastructure Act 2018* (Cth) (SCI Act)."[2]

2. The Bill seeks to:

   - introduce a positive security obligation for a range of critical infrastructure assets across critical sectors
   - increase the cyber obligations on systems of national significance
   - ensure that Government has the necessary powers to provide direct assistance to industry in the event of a serious cyber security incident.

3. The OAIC has regulatory oversight of the *Privacy Act 1988* Cth (Privacy Act), which sets out how Australian Privacy Principle (APP) entities (including most Australian Government agencies, and all private sector and not-for-profit organisations with an annual turnover of more than $3 million) must collect, use and disclose individuals' personal information.[3]

4. The obligations under the Privacy Act apply to entities that will be regulated by the Bill. Further, the Notifiable Data Breaches Scheme (NDB scheme) and binding principles for governance and security of personal information contained in the Privacy Act will intersect with functions proposed by the Bill. It is important that the Bill does not override or curtail those existing obligations and that sharing of information can occur to ensure a coordinated and efficient regulatory system.

5. The OAIC supports measures that would strengthen the security or resilience of systems, assets, or data that are critical to Australia's national interests or defence. However, we note that initiatives which impact personal information handling and privacy must be reasonable, necessary, and proportionate to achieving legitimate policy aims.

6. The OAIC makes four recommendations as follows:

   Recommendation 1 – The Bill ensure that the disclosure of protected information is permitted for the purposes of giving effect to the exercise of the Information Commissioner's privacy functions.[4]

   Recommendation 2 – The Bill permit information sharing between regulatory agencies and that a consequential amendment is made to s 29 of the *Australian Information Commissioner Act*

[1] https://parlinfo.aph.gov.au/parlInfo/download/legislation/bills/r6657_first-reps/toc_pdf/20182b01.pdf;fileType=application%2Fpdf.
[2] Explanatory Memorandum, Security Legislation Amendment (Critical Infrastructure) Bill 2020 (Cth) 3, [6].
[3] Personal information is defined in section 6(1) as any 'information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether the information or opinion is true or not, and whether the information is recorded in a material form or not'.
[4] *Australian Information Commissioner Act 2010* (Cth) s 9.

2010, to ensure that information sharing of the kind required to support efficient regulation is permitted.

Recommendation 3 – The Bill be amended to require the Minister to have regard to any potential impact on the privacy of individuals when determining whether an authorisation under s 35AB is a proportionate response to a cyber security incident.

Recommendation 4 – The Explanatory Memorandum make reference to the Commissioner's guidance function in s 28 of the Privacy Act and indicate that it is intended that the OAIC is consulted in relation to any guidance about the personal information-handling obligations that would apply to the scheme. Where substantive guidance about personal information is required, this should be developed by the OAIC as the privacy regulator.

2. Protected information

7. The Bill amends s 5 of the SCI Act to significantly expand the definition of 'protected information'. The OAIC wishes to ensure that the restrictions on an entity making a record of, using or disclosing protected information under Division 3 of Part 4 of the SCI Act do not limit the ability of the OAIC to exercise its privacy functions, or prevent entities from disclosing information required for compliance with and the administration of the Privacy Act.

8. Section 46 of the SCI Act provides that the offence for unauthorised use or disclosure of protected information in s 45 does not apply if the making of the record, or the disclosure or use of the information, is required or authorised by or under a law of the Commonwealth. However, s 47 of the SCI Act provides that, except where it is necessary to do so for the purposes of giving effect to that Act, an entity is not to be required to disclose protected information, or produce a document containing protected information to "a tribunal, authority or person that has the power to require the answering of questions or the production of documents."

9. The OAIC has the power to require the answering of questions or production of documents under the Privacy Act. The OAIC may make inquiries, handle complaints, or conduct investigations into matters which relate to protected information. By way of example, an eligible data breach, notifiable to the OAIC under the relevant provisions of the Privacy Act may include protected information as defined by the SCI Act and expanded by the Bill.

10. Clause 54B of the Bill would expand s 47 of the SCI Act, allowing entities to disclose protected information in certain circumstances, including for the purposes of giving effect to any Act that confers functions, powers, or duties on the Inspector-General of Intelligence and Security (IGIS). The Explanatory Memorandum (EM) states that the effect of cl 54B of the Bill is to:

> *extend the exception to also apply when it is necessary to disclose or produce protected information for the purposes of the IGIS Act, or any other Act conferring functions, powers or duties on the IGIS…The extension of this exception is intended to ensure that the IGIS is able to compel access to information that may be relevant to an inquiry despite the protection against disclosure provided by section 47*.[5]

11. We recommend that the Committee consider a similar amendment to s 47 to ensure that the

[5] Explanatory Memorandum, Security Legislation Amendment (Critical Infrastructure) Bill 2020 (Cth) 210, [1100-1101].

disclosure of protected information is permitted for the purposes of giving effect to the exercise of the Information Commissioner's privacy functions.

12. We also refer to ss 43A to 43D of the Bill, which authorise the use and disclosure of protected information to and between IGIS officials, Ombudsman officials, or by the Director-General of the Australian Signals Directorate (ASD) or a staff member of ASD for the purpose of the exercise of their powers or performance of their functions or duties. The EM to the Bill[6] states that these sections provide an authorisation for the purposes of excluding the application of the offence provision in s 45 of the SCI Act relating to the unauthorised use or disclosure of protected information.

13. We recommend the Committee consider these provisions as mechanisms through which to clearly authorise the use and disclosure of protected information to the Information Commissioner or delegate. In relation to information sharing between regulators and agencies, we also refer to Recommendation 2 below.

Recommendation 1 – That the Bill ensure that the disclosure of protected information is permitted for the purposes of giving effect to the exercise of the Information Commissioner's privacy functions.

3. Enhanced cyber security obligations and the Positive Security Obligation

14. The Bill introduces a 'Positive Security Obligation' for critical infrastructure, including a risk management program, to be delivered through sector-specific requirements and mandatory cyber incident reporting. In particular, if a cyber incident has occurred or is occurring in relation to a critical infrastructure asset, the entity will be obliged to report the incident to the relevant Commonwealth body (s 30BC).

15. Under the NDB scheme, entities across the economy must notify affected individuals and the OAIC when a data breach is likely to result in serious harm to an individual whose personal information is involved. This includes cyber-security incidents involving personal information.

16. We consider that there is a potential overlap of the reporting obligations proposed in the Bill and those already applicable to entities covered by existing privacy legislation. The OAIC envisages the need for efficient assessment and response coordination between the receiving agencies to leverage the combined capability of the Commonwealth and ensure proportionate and targeted responses. It also mitigates against a risk of fractured, overlapping or inconsistent responses where there are multiple reporting obligations in relation to particular incidents.

17. While the Bill envisages information-sharing between regulatory agencies will be set out in the rules, the OAIC recommends this be considered in light of the secrecy provisions of the SCI Act. A consequential amendment to s 29 of the *Australian Information Commissioner Act 2010* will also be needed, to ensure that information sharing of the kind required to support efficient

[6] Available for download at: https://parlinfo.aph.gov.au/parlInfo/download/legislation/ems/r6657_ems_928e0092-fabb-4c31-a67b-b47ac1123e17/upload_pdf/JC000738.pdf;fileType=application%2Fpdf.

regulation is permitted.

Recommendation 2 – The Bill permit information sharing between regulatory agencies and that a consequential amendment is made to s 29 of the *Australian Information Commissioner Act 2010*, to ensure that information sharing of the kind required to support efficient regulation is permitted.

4. Government Assistance to entities

18. The Bill introduces a 'Government Assistance' regime, which would provide the Government powers to protect assets during or following a significant cyber-attack. This includes the power to authorise information gathering directions (s 35AK), action directions (s 35AQ), and intervention requests (s 35AX).

19. The Bill proposes that where an appropriate Ministerial authorisation is in force, the Secretary to the Department of Home Affairs can compel relevant entities to produce any information that may assist with determining whether a power should be exercised in relation to the incident and asset in question. The Secretary may also direct an entity 'to do, or refrain from doing, a specified act or thing'.[7] This broad power should be balanced with appropriate safeguards, oversight, and accountability to ensure it is proportionate.

20. The OAIC recommends that, in deciding whether or not to give the necessary authorisation, the Minister should be required to consider the privacy impacts of the exercise of these powers insofar as they apply to 'business critical data' or other data that may include personal information. In our view, this would help to build both industry and community trust and confidence in the proposed framework.

21. This requirement to consider privacy could be included in the matters that the Minister must have regard to when determining whether a direction or request is a proportionate response to a cyber security incident, as under ss 35AB (8) and (11). There is precedent for this approach in s 180F ('Authorised officers to consider privacy') of the *Telecommunications (Interception and Access) Act 1979* (Cth).

Recommendation 3 – The Bill be amended to require the Minister to have regard to any potential impact on the privacy of individuals when determining whether an authorisation s 35AB is a proportionate response to a cyber security incident.

5. Consultation with the OAIC

22. The OAIC welcomes the co-design process proposed in the Explanatory Memorandum, whereby the Department of Home Affairs, Government agencies, key industry stakeholders and sector regulators will work together to develop the sector-specific requirements that underpin the risk management program.

[7] Security Legislation Amendment (Critical Infrastructure) Bill 2020 (Cth) s 35AQ(1).

23. Noting one of the key initiatives of this partnership is to ensure that the new industry requirements build on and do not duplicate existing regulatory or non-regulatory approaches across sectors, the OAIC should be consulted on matters relating to privacy, in particular those regarding the security of personal information (Australian Privacy Principle 11) and the NDB scheme.[8]

24. To the extent that substantive guidance on personal information handling is required, the Commissioner's statutory function to make guidelines for the avoidance of acts or practices that may impact privacy would be operable.[9] The OAIC recommends that the EM indicate that the OAIC would be consulted in relation to the privacy aspects of the scheme.

Recommendation 4 – The Explanatory Memorandum make reference to the Commissioner's guidance function in section 28 of the Privacy Act and indicate that it is intended that the OAIC is consulted in relation to any guidance on the personal information-handling obligations that would apply to the scheme. Where substantive guidance on personal information handling is required, this should be developed by the OAIC as the privacy regulator.

6. Privacy Impact Assessments

25. A privacy impact assessment (PIA) is a systematic written assessment of an activity or function that identifies the impact that the activity or function might have on the privacy of individuals and sets out recommendations for managing, minimising or eliminating that impact. Undertaking PIAs are a key component of a 'privacy by design' approach. They also help to build the community's trust that privacy risks have been identified, and protections embedded, at the design stage of a new project involving personal information handling.

26. The *Privacy (Australian Government Agencies – Governance) APP Code 2017* (Privacy Code) requires Australian Government agencies subject to the Privacy Act to conduct a PIA for all 'high privacy risk projects'. A project may be a high privacy risk project if the agency reasonably considers that the project involves new or changed ways of handling personal information that are likely to have a significant impact on the privacy of individuals.

27. Given that the Bill contemplates new personal information handling practices, the OAIC expects that the Department of Home Affairs will have regard to these PIA obligations. We also note that PIAs should be revisited and updated when changes to a project are considered, and, in some instances, it may be necessary to undertake another PIA. The OAIC has published a *Guide to undertaking privacy impact assessments* and *When do agencies need to conduct a privacy impact assessment?* to assist agencies in meeting their Privacy Code obligations.

28. Thank you for the opportunity to provide a submission to the Committee. The OAIC is available to provide further information or assistance as required.

[8] *Privacy Act 1988* (Cth) pt IIIC.
[9] *Privacy Act 1988* (Cth) s 28.