Australian Government

Office of the Australian Information Commissioner

Security Legislation Amendment (Critical Infrastructure) Bill 2020 - Submission to the Department of Home Affairs

Angelene Falk

Australian Information Commissioner and Privacy Commissioner

1 December 2020

OAIC

Our reference: D2020/022334

Critical Infrastructure Centre
Department of Home Affairs
[redacted]

By email: ci.reforms@homeaffairs.gov.au

Security Legislation Amendment (Critical Infrastructure) Bill 2020

The Office of the Australian Information Commissioner (OAIC) welcomes the opportunity to comment on the Exposure Draft of the Security Legislation Amendment (Critical Infrastructure) Bill 2020 (the Bill). 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).

The OAIC's submission draws attention to the following:

As the regulator of the *Privacy Act 1988* (Cth) (Privacy Act), which includes the Notifiable Data Breaches Scheme (NDB scheme) and Australian Privacy Principles (APPs) on governance and security of personal information, the OAIC's functions intersect with those proposed by the Bill. This occurs principally in two ways. First the Privacy Act applies to entities that will be regulated by the Bill. It is important then that the OAIC's jurisdiction continues to operate unimpeded and that sharing of information can occur to ensure a coordinated and efficient regulatory system.

The Bill amends section 5 of the SCI Act to significantly expand the definition of 'protected information' and effectively captures information obtained under the SCI Act. This will capture information provided as part of the proposed new mechanisms such as a risk management program or mandatory cyber incident reporting to the Department of Home Affairs (Home Affairs). The OAIC considers that restrictions on an entity making a record of, using or disclosing protected information in Division 3 of Part 4 of the SCI Act have the potential to prevent entities voluntarily disclosing some information required for the administration of the Privacy Act. The OAIC is also concerned that section 47 of the SCI Act provides that an entity cannot be compelled to produce protected information to a court, tribunal or any other person who has the power to require the production of information or documents, which would include the OAIC.

Second, the OAIC also regulates the handling of personal information by the Minister and Home Affairs. It is important to ensure that the proposed expansion of 'protected information' in the Bill does not impact the OAIC's ability to regulate the handling of personal information by Home Affairs. The OAIC emphasises the importance of ensuring that the functions and powers conferred by the Bill are exercised to minimise the impact on privacy and safeguard the handling of personal information that may occur as a result of the exercise of powers, with appropriate oversight.

The OAIC seeks clarification on these issues. We would not want the definition of 'protected information' to adversely impact entities (and Home Affairs') ability to lawfully comply with the Information Commissioner's requests for information or the Privacy Act's NDB requirements.

The OAIC seeks to participate in the proposed partnership-based approach to developing rules and guidance that will allow 'relevant entities'[1] to meet their obligations imposed by the Bill. This will assist to ensure that rules and guidance take account of Privacy Act obligations. The OAIC recognises the benefits of an effective and consistent approach to uplifting resilience in all of Australia's critical infrastructure sectors.

We also note that initiatives which impact privacy must be reasonable, necessary, and proportionate to achieving legitimate policy aims. Given that there are inherent privacy risks associated with some of the measures proposed by the Bill, these measures must be subject to appropriate safeguards, oversight, and accountability. For example, the expansion of powers, particularly those involving access and control of data, should be accompanied by protections that will ensure personal information, if required to be accessed, is only accessed by authorised persons.

As the OAIC has not had the opportunity to comprehensively consider all aspects of the Bill, we provide the comments below focused on a limited number of matters.

Enhanced cyber security obligations and the Positive Security Obligation

The Bill would introduce 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, 'business critical data' that includes personal data that relates to at least 20,000 individuals or sensitive information (as defined in the Privacy Act) may attract the positive security obligation to report.

Under the Australian NDB scheme any organisation or agency the Privacy Act covers 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 extends to cyber-security incidents involving personal information.

There is a potential overlap of the reporting obligations proposed in the draft Bill and those already applicable to entities covered by existing privacy legislation.

Similar issues were raised by the Office of the Victorian Information Commissioner's submission of 16 September 2020 to Home Affairs' 'Protecting Critical Infrastructure and Systems of National Significance' Consultation Paper.[2]

The OAIC envisages that a coordinated Commonwealth assessment of the risks and responses to these reporting measures will require effective information sharing between regulators. Assessment and response coordination across receiving agencies efficiently leverages the combined capability of the Commonwealth and ensures proportionate, targeted and efficient responses. It also mitigates against a risk of a fractured, overlapping or inconsistent response where there are multiple reporting obligations in relation to particular incidents.

[1] Security Legislation Amendment (Critical Infrastructure) Bill 2020, s 5.

[2] The submission can be downloaded at www.homeaffairs.gov.au/reports-and-publications/submissions-and-discussion-papers/protecting-critical-infrastructure-systems.

While the Bill envisages information-sharing between regulatory agencies will be set out in the rules, consideration should be given to ensure this will be permissible under secrecy provisions. A consequential amendment should also be made to section 29 of the *Australian Information Commissioner Act 2010* to ensure that information sharing of the kind required to support efficient regulation is permitted.

The OAIC will also need to support the implementation of the Bill through, for example, contributions to sector-specific guidance about 'business critical data' to help ensure all reporting obligations are well understood by regulated entities, and the development of rules.

Accordingly, for the above reasons the Bill will also have resourcing implications for the OAIC.

Government Assistance to entities

The Bill introduces a 'Government Assistance' regime, which would provide the Government with powers to protect assets during or following a significant cyber-attack. This includes the powers to authorise:

- information gathering directions (s 35AK)
- action directions (s 35AQ)
- intervention requests (s 35AX).

As an overarching observation the OAIC notes that the Bill provides a wide discretionary power to issue and make directions under Ministerial authorisations. Given the breadth of these powers, and in order to build trust and confidence in the framework, we suggest that consideration be given to an independent authorisation process where exercise of powers applies to 'business critical data'.

Under the Bill, we understand that the Secretary 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'.[3] As noted above, this broad power must be balanced with appropriate safeguards, oversight, and accountability.

The OAIC recommends that the Secretary be required to consider privacy impacts in so far as the exercise of powers applies to 'business critical data'.

The OAIC also recommends that there be a requirement to have regard to guidance developed in consultation with the OAIC about the personal information-handling obligations that would apply to their use. This guidance should consider the requirements of the Privacy Act, particularly those regarding the security of personal information APP 11. APP 11 requires all entities covered by the Privacy Act to take reasonable steps to protect personal information that they hold from misuse, interference and loss, and from unauthorised access, modification or disclosure.

We refer to our *Guide to securing personal information*, which discusses the range of reasonable steps entities can take to assist them to comply with APP 11, many of which would be relevant to the

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

practices envisaged by the Bill. For example, the guidance should consider information and communications technology and physical security of the transfer of personal information from entities to the Secretary.

The OAIC also recommends that ss 35AB(8) and (11) of the Bill be expanded to clarify that the Minister for Home Affairs must have regard to the potential impacts on the privacy of individuals, where these directions or requests will likely involve the handling of personal information.

The OAIC also recommends the Government consider amendments to the SCI Act secrecy provisions to ensure there is no ousting of the independent compliance oversight by the OAIC in relation to the obligations of the Department under the Privacy Act.

Privacy Impact Assessments

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 a PIA assists APP entities to build privacy considerations into the design of a project and achieve the project's goals while minimising the negative and enhancing the positive privacy impacts. A PIA can 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.

The *Privacy (Australian Government Agencies – Governance) APP Code 2017* (Privacy Code) requires Australian Government agencies subject to the Privacy Act to conduct a privacy impact assessment (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.

Given that the Bill suggests new personal information management practices, the OAIC expects that Home Affairs will conduct a PIA, if it has not done so already.

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.

Thank you for the opportunity to provide a submission on the Exposure Draft of the Bill. The OAIC is available to provide further information or assistance as required.