Australian Government

Office of the Australian Information Commissioner

Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022 – Submission to the Parliamentary Joint Committee on Intelligence and Security

Angelene Falk

Australian Information Commissioner and Privacy Commissioner

1 March 2022

OAIC

March 2022

Contents

March 2022

The Office of the Australian Information Commissioner (OAIC) welcomes the opportunity to provide a submission to the Parliamentary Joint Committee on Intelligence and Security's (the Committee's) review of the Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022 (the Bill).

The OAIC has previously provided submissions to the Department of Home Affairs and the Committee to ensure that the *Privacy Act 1988* (Privacy Act) continues to operate alongside the Critical Infrastructure framework, and that the framework facilitates regulatory collaboration with the OAIC.[1] The matters raised by the OAIC have not been addressed in the *Security Legislation Amendment (Critical Infrastructure) Act 2021* or in the Bill before the Committee.

The OAIC and the Privacy Act has an important role to play in Australia's cyber security ring of defence, through requiring the security of personal information and the reporting of notifiable data breaches. The OAIC is supportive of measures that strengthen the security and resilience of systems, assets and data that are critical to Australia's national interests. A strong cybersecurity posture across the breadth of Australian entities can have positive effects on the protection of personal information. However, as we understand it, the proposed Critical Infrastructure framework risks impacting the effective operation of the security and breach reporting requirements under the Privacy Act.

The OAIC reiterates two key recommendations to the Committee to address this concern. Our recommendations suggest minor amendments that will support the key objectives of the *Security of Critical Infrastructure Act 2018* – facilitating collaboration between regulators and providing a regime for the Commonwealth to respond to serious cyber security incidents.[2]

In making these recommendations, the OAIC seeks to ensure that the Critical Infrastructure framework (both the *Security of Critical Infrastructure Act 2018* and the Bill):

- is able to co-exist with the current security and breach reporting requirements under the Privacy Act (and does not impede the operation of the Privacy Act)
- facilitates greater regulatory efficiencies for regulators and regulated entities alike by permitting information sharing.

Recommendation 1 – ensure that Privacy Act functions are not impeded

The *Security of Critical Infrastructure Act 2018* prevents the disclosure of protected information unless an exception applies, or the disclosure is otherwise authorised.[3] There is no exception or authorisation for an entity to disclose protected information to the OAIC.[4] Further, an entity can rely on the Act to refuse to disclose this information if the OAIC uses its powers to require the production of documents.[5]

---

[1] See the OAIC's previous submission to Home Affairs and submission to the PJCIS on the original Bill which contained the same recommendations included in this submission.

[2] See s 3(b) and (e) of the *Security of Critical Infrastructure Act 2018.*

[3] See s 45 of the *Security of Critical Infrastructure Act 2018*.

[4] See s 46 of the *Security of Critical Infrastructure Act 2018*.

[5] See s 47 of the *Security of Critical Infrastructure Act 2018*. This provision states that entities cannot be required to disclose protected information, or produce a document containing protected information, to a person that has the power to require the answering of questions or the production of documents. This could impact the operation of s 44 of the *Privacy Act 1988*.

A consequence of this is that where circumstances constitute both a cyber security incident under the *Security of Critical Infrastructure Act 2018* [6] and a notifiable data breach under the Privacy Act,[7] entities will be restricted from reporting that breach to the OAIC under the Privacy Act. This is because cyber security incidents reported under the *Security of Critical Infrastructure Act 2018,* are considered protected information under that Act.[8] The impact of these provisions is further heightened by the expanded definition of critical infrastructure sectors and asset classes,[9] and has real consequences for regulating the protection of Australian's personal information in accordance with the Privacy Act.

The OAIC recommends that this issue be addressed through the following:

- An amendment to Part 4, Division 3, subdivision A of the *Security of Critical Infrastructure Act 2018* to provide for the authorised use and disclosure of protected information to the Australian Information Commissioner, for the purpose of notifying an eligible data breach under the Privacy Act.
- An amendment to Section 47(2) of the *Security of Critical Infrastructure Act 2018* to include the OAIC and allow entities to produce documents and answer questions where they relate to a notifiable data breach and other regulatory functions of the OAIC under the Privacy Act.

These amendments will ensure that entities regulated under the Privacy Act are not prohibited from reporting notifiable data breaches to the OAIC, and the OAIC can investigate any relevant breaches or compliance issues.[10] The OAIC is not aware of any adverse impacts on the operation of the Critical Infrastructure framework that would result from our proposed amendments, which will ensure the continued effective operation of the Privacy Act.

The identification of data breaches is imperative to ensuring that any impact on individuals' privacy can be mitigated as quickly as possible.[11] It is important for the Critical Infrastructure framework to work alongside the notifiable data breach framework and not prevent notifications to the OAIC, or otherwise constrain the operation of the Privacy Act.

OAIC recommendation: That the Bill include amendments to the following parts of the *Security of Critical Infrastructure Act 2018*:

- Part 4, Division 3, subdivision A to provide for the authorised use and disclosure of protected information to the Australian Information Commissioner for the purposes of notifying an eligible data breach under the *Privacy Act 1988*

[6] See ss 30BC and 30BD of the *Security of Critical Infrastructure Act 2018*.

[7] See Part IIIC of the *Privacy Act 1988*.

[8] See definition of protected information in s 5 of the *Security of Critical Infrastructure Act 2018*.

[9] See ss 8D and 8E of the *Security of Critical Infrastructure Act 2018*.

[10] For example, compliance with Australian Privacy Principle (APP 11) which requires an APP entity to take active measures to ensure the security of personal information it holds, and to actively consider whether it is permitted to retain personal information.

[11] The OAIC's Notifiable Data Breaches Report for the period July–December 2021 found that since the introduction of Australia's mandatory notifiable data breach regime in 2018, over 3,500 notifications have been received by the OAIC. That is a more than an eight-fold increase on notifications made under the previous voluntary notification scheme.

- Section 47(2) to include the OAIC and allow it to require entities to produce documents and answer questions where they relate to a notifiable data breach or other regulatory functions of the OAIC under the *Privacy Act 1988*

Recommendation 2 – include information sharing provisions for regulatory efficiencies

The OAIC has previously noted that the Bill presents an opportunity to facilitate information sharing to promote regulatory efficiency and co-operation. This is particularly relevant where reporting obligations are enlivened under both the Privacy Act's notifiable data breach framework and the Critical Infrastructure framework. Where this occurs, it is important that the OAIC is able to share information with other regulatory agencies to ensure any regulatory overlap is minimised and the OAIC has access to information relevant to its decision making.

The *Security of Critical Infrastructure Act 2018* includes provisions for information sharing between the IGIS, the Commonwealth Ombudsman and ASD. We recommend this be expanded to include the OAIC in the current Bill.

In order to ensure the OAIC is not precluded from information sharing in this regard, the Bill should include a consequential amendment to section 29 of the *Australian Information Commissioner Act 2010* to enable this to occur.[12]

OAIC recommendation: That the Bill include an amendment to Part 4, Division 3, subdivision A of the *Security of Critical Infrastructure Act 2018* to provide authority for the OAIC to share information with the ASD and IGIS and vice versa

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

[12] Section 29 of the *Australian Information Commissioner Act 2010* sets out the circumstances in which the Commissioner may share information. By way of example, under s 29(2)(aa) of the Act, the Commissioner is expressly authorised to share information acquired in the course of performing a function conferred by Part IVD (about the consumer data right) of the *Competition and Consumer Act 2010* with, amongst other entities, the Australian Competition and Consumer Commission.