Client Alert

October 2024

Australia: Cyber Security Legislative Package 2024

The Australian Government takes its next step towards becoming a world cyber security leader by 2030

In brief

In 2023, the Australian Government released the 2023-2030 Australian Cyber Security Strategy.

9 October 2024 marked the latest in a series of legislative reforms in pursuit of that strategy, as the Cyber Security Legislative Package 2024 (**Package**) was introduced to Parliament. The Package has been referred to the Parliamentary Joint Committee on Intelligence and Security for inquiry and report.

The Package contains the following:

1. *Cyber Security Bill 2024* (**Cyber Security Bill**);
2. *Intelligence Services and Other Legislation Amendment (Cyber Security) Bill 2024* (**Intelligence Services Amendment Bill**); and
3. *Security of Critical Infrastructure and Other Legislation Amendment (Enhanced Response and Prevention) Bill 2024* (**SOCI Amendment Bill**).

The Package is targeted at addressing legislative gaps to bring Australia in line with global best practice and fostering collaboration and information-sharing between industry and government. This includes establishing a mandatory reporting requirement for ransomware and cyber extortion payments. Businesses should closely watch the progress of the Package.

Contents

Key takeaways

Key areas of focus for businesses will likely be:

- Understanding the complexity of the Package and how the provisions inter-relate with existing regulatory schemes.
- Identifying what additional processes may be needed, in particular for managing and reporting cyber security incidents as well as increased engagement with government bodies on such incidents.
- The potential extra-territorial impact of the Package.

In more detail

Cyber Security Bill

The Australian Government seeks to increase proactive industry reporting and engagement following cyber incidents. The Government has perceived that businesses may be hesitant to voluntarily report information due to concerns that such information may be shared between Government agencies and used against them in future proceedings. The Cyber Security Bill sets out a framework for the Government to gather information about emerging cyber threats and Australia's overall risk position, which in turn will inform future protections and policy.

Security standards for IOT devices

IOT devices include home and personal technology such as smart TVs, smart watches, home assistances and baby monitors. These devices collect and process increasing volumes of personal and other sensitive information, often without the knowledge of the user.

The Bill introduces a broad power for the Government to prescribe mandatory security standards for IOT devices. The Government has indicated that the intention is for Australia to align itself with international best practice with a particular focus on the UK, reinforced by adoption of the UK definition of 'relevant connectable products'.

Manufacturers and suppliers will be required to provide a statement of compliance for any devices they manufacture or supply to the Australian market. The Bill also introduces an enforcement and compliance regime under which compliance notices, stop notices and recall notices may be issued in the event of non-compliance with applicable standards. Manufacturers and suppliers of relevant connectable products, including those located outside of Australia, could find themselves subject to the new reporting requirements.

Mandatory reporting of ransomware and cyber extortion payments

The Government continues to consider ransomware among the most significant cyber threats. The Bill introduces a framework for mandatory reporting of ransomware and cyber extortion payments. Ransomware is malware designed to encrypt devices and data, rendering them inaccessible without a decryption key which is only provided if a ransom is paid. Cyber extortion involves the theft of confidential information (such as personal information) and the threat of disclosure if a ransom is not paid.

An entity is a 'reporting entity', subject to the new reporting obligation, if it:

- carries on business in Australia, with an annual turnover above a yet-to-be specified threshold (which may align with the AUD $3 million small business threshold in the *Privacy Act 1988* (Cth)); or
- is a responsible entity for a critical infrastructure asset covered by the *Security of Critical Infrastructure Act 2018* (Cth) (**SOCI Act**).

If a reporting entity experiences or reasonably suspects a cyber security incident, has received a demand, and provides a payment to the extorting party (or is aware that a third party has done so), it will be required to make a report to the Australian Cyber Security Centre (**ACSC**) through the Online Portal. The report must be made within 72 hours of the payment or awareness of the payment.

The definition of cyber security incident adopted by the Bill is based on section 12M of the SOCI Act and broadened slightly to include where a communication has been intercepted by an unauthorised party.

Limited Use Obligation on government

The Bill will impose a "Limited Use Obligation" on government bodies receiving cyber security incident information. For example, cyber incident information disclosed voluntarily to the National Cyber Security Coordinator (**NCSC**), and information disclosed to the ACSC or Australian Security Directorate (**ASD**) in a ransomware payment report, can only be used to assist the entity to mitigate and respond to the incident, and for limited further cyber security purposes.

The following protections will generally apply to information disclosed (subject to limited exceptions):

- it cannot be recorded, used or disclosed to investigate or enforce a breach of law by the reporting entity (other than a criminal offence or, in relation to a breach of the ransom payment reporting obligation);
- it will not affect any existing right or claim to legal professional privilege; and
- it is not admissible in evidence against the reporting entity for civil or criminal proceedings, tribunal proceedings, or any other proceedings for a breach of law (including the common law).

Additionally, neither an entity nor its representatives who made or omitted an act in good faith, in making a ransom payment report, will be liable in relation to that act or omission.

Importantly, the Limited Use Obligation provisions will not serve as a 'safe harbour' to shield businesses from liability. Reported information can still be used against the reporting entity if collected through other means.

Cyber Incident Review Board

The Bill establishes the Cyber Incident Review Board (**Board**) to review certain cyber security incidents and make recommendations to government and industry based on its findings, acknowledging that there are further lessons to be learned by both Government and industry when it comes to high-profile and high-impact cyber security incidents.

The aim of investigations conducted by the Board will not be to assign liability, but to reflect on common elements or themes, and what can be done to avoid them in the future.

The Board will have limited information-gathering powers – to be used only where voluntary requests for information from entities involved in a cyber security incident have been unsuccessful.

Intelligence Services Amendment Bill

The provisions proposed by the Intelligence Services Amendment Bill are designed to create a safe environment for businesses to voluntarily report on cyber security incidents, without compromising the efficacy of the regulatory function. The Bill incorporates the Limited Use Obligation set out above with respect to the NCSC into the *Intelligence Services Act 2001* (Cth), to apply to the ASD (including the ACSC).

SOCI Amendment Bill

The SOCI Amendment Bill proposes a series of amendments to the SOCI Act in pursuit of Shield 4 of the 2023-2030 Australian Cyber Security Strategy: Protected Critical Infrastructure. The Bill seeks to remedy gaps in the current regulatory framework for protecting critical infrastructure and broaden the asset classes that fall within the scope of the framework.

Expansion of critical infrastructure asset definition

The Bill expands the definition of critical infrastructure assets to include data storage systems holding business critical data, as opposed to solely applying to operational assets. A responsible entity for a critical infrastructure asset may need to revisit its SOCI Act obligations to ensure this new category of critical infrastructure asset is sufficiently protected including adequate cyber security incident response processes.

Government powers relating to critical infrastructure incidents

Currently, the Government is empowered to do the following in response to a serious cyber security incident affecting a critical infrastructure asset:

- issue information-gathering directions to relevant entities, requiring entities to provide information;
- issue actions directions to relevant entities, requiring entities to do or omit a certain act; and
- give intervention requests to the authorised Government agency, allowing them to step in.

These powers are intended to serve as a last resort.

The Government has assessed that the current powers do not allow it to adequately respond to incidents affecting critical infrastructure assets more generally (i.e. non-cyber incidents), where the availability, integrity and reliability of the asset may still be at risk. As a result, the Bill proposes that the information-gathering and action direction powers (but not the intervention power) be broadened to be enlivened following any incident affecting a critical infrastructure asset.

Simplification of information-sharing across industry and government

"Protected Information" under the SOCI Act, broadly-speaking, is information obtained in the course of exercising powers or performing duties or functions under the SOCI Act including information prepared or exchanged in specified circumstances (e.g., to report certain matters required under the SOCI Act). It also includes key documents such as a critical infrastructure risk management program. Unauthorised disclosure of Protected Information can constitute an offence.

It may not always be clear whether information falls under this definition. Given the potential for criminal proceedings, dealing with this information appropriately has caused some concern for entities responsible for critical infrastructure assets. This has impeded information-sharing by industry with government.

In response, the Bill would restrict the definition of Protected Information to an assessment of whether it could cause harm, or pose risk to the Australian public, the security of the asset, commercial interests, the socioeconomic stability, national security or defence of Australia. Additionally, disclosure of Protected Information will be permitted for an entity to operate the critical infrastructure asset or manage its own affairs.

Addressing serious cyber risk management deficiencies

Entities that are responsible for cyber security assets must establish, maintain and comply with a Critical Infrastructure Risk Management Program (**CIRMP**). This is to ensure responsible entities are proactively and holistically identifying, preventing and mitigating risks to critical infrastructure assets.

At present, the Government is not empowered to require an entity to vary a deficient CIRMP. The Bill will enable the Government to issue directions to address any serious deficiencies that are identified in a CIRMP, addressing perceived gaps in the current powers available.

Security of critical telecommunications assets

The Bill proposes bringing the regulation of the telecommunications sector further under the SOCI Act. Currently there is a hybrid scheme with some SOCI Act requirements for the telecommunications sector being addressed under instruments issued under the *Telecommunications Act 1997* (Cth). The intention is to clarify security and other obligations for responsible entities of critical telecommunications assets and unify regulation of critical infrastructure assets under the SOCI Act.

Responsible entities for critical infrastructure telecommunications assets must:

- protect the asset to ensure security, confidentiality of communications, and the availability and integrity of the asset; and
- notify the Government of changes that may affect the entity's ability to protect the asset.

Where the Government considers there may be a risk to security, they may issue a direction to the responsible entity not to use or supply the asset.

Thank you to Hannah Stacey for her assistance in preparing this alert.

Contact Us

Anne Petterd
Partner
anne.petterd@bakermckenzie.com

Adrian Lawrence
Partner
adrian.lawrence@bakermckenzie.com

Ryan Grant
Partner
ryan.grant@bakermckenzie.com

Paul Forbes
Partner
paul.forbes@bakermckenzie.com

Simone Blackadder
Special Counsel
simone.blackadder.@bakermckenzie.com

Jarrod Bayliss-McCulloch
Special Counsel
Jarrod.Bayliss-McCulloch@bakermckenzie.com