First Security of Critical Infrastructure Bill

December 2021

Authors

Thomas Crowe; Amanda Khoo; Susan Kantor; Leah Mooney; Paul Kallenbach

T +61 3 8608 2622
paul.kallenbach@minterellison.com

MinterEllison.

First Security of Critical Infrastructure Bill is now live

1. BACKGROUND

The security of critical infrastructure (**SOCI**) laws are a key measure under the Australian Cyber Security Strategy 2020. They are in response to evidence that well-resourced and persistent state-sponsored actors are maliciously targeting critical infrastructure and stealing intellectual property developed in Australia. While Australia has not suffered a catastrophic attack on critical infrastructure, there have been several high profile cyber attacks in the public and private sectors that have had a significant impact.

You can read more about the history of the SOCI laws in our previous article, Changes to critical infrastructure laws in 2021: is your sector impacted? as well as specifically how these changes are affecting Foreign Investment Review Board processes.

During SOCI laws' passage through Commonwealth Parliament, the Bill was amended, and then separated into two parts. Only the first part of the Bill is now law.

The *Security Legislation Amendment (Critical Infrastructure) Bill 2021* (Cth) (**First Bill**) amends the scope of the *Security of Critical Infrastructure Act 2018* (Cth) (**Act**), which underpins a framework for managing cyber risks relating to critical infrastructure. The First Bill:

1. Extends the obligations in the Act to a broader range of sectors – now eleven in total as compared with the previous four. The sectors that are defined as 'critical infrastructure sectors' are now as follows:
    a. communications;
    b. data and storage or processing;
    c. financial services and markets;
    d. water and sewerage;
    e. energy;
    f. healthcare and medical;
    g. higher education and research;
    h. food and grocery;
    i. transport;
    j. space technology;
    k. defence industry; and

2. Introduces new obligations:
    a. empowering the Government to issue information gathering and other directions, as well as request specified agencies to provide support, in certain circumstances, in respect of a cyber security incident (the **Government Assistance Measures**); and
    b. if 'switched on' for a particular sector:
        i. mandating cyber security incident reporting (the **Mandatory Reporting Obligation**); and
        ii. requiring certain entities to maintain a register of critical infrastructure assets containing specified information (the **Asset Register Obligation**).

Under the First Bill, the Government Assistance Measures apply to all sectors from the date of royal assent (2 December 2021).

An exposure draft for a second *Security Legislation Amendment (Critical Infrastructure*) Bill (**Second Bill**) is expected to be released in the coming weeks for consultation with impacted sectors. The Department has been engaging with several sectors in relation to the Second Bill, which will introduce comprehensive risk management program obligations (the **Risk Management Program Obligation**), as well as enhanced cyber security obligations.

2. OVERVIEW OF OBLIGATIONS

The First Bill specifies, with reference to each of the new sectors, the critical infrastructure assets covered by the enhanced framework and the entities with responsibility for compliance (**responsible entities**).

While the First Bill broadly affects the eleven critical sectors, not all assets owned by organisations operating in the those sectors will fall under the definition of a 'critical infrastructure asset'. The First Bill provides a set of criteria for each sector and class of assets, as described in section 12 of the Bill. On 13 December 2021, the *Security of Critical Infrastructure (Definitions) Rules 2021 (***Rules**) were registered, which provide additional clarification on which assets may fall within definitions under the Act of 'critical infrastructure assets' in relation to the communications, energy, transport, financial services and markets, and food and grocery sectors.

At the Town Hall held by the Cyber and Infrastructure Security Centre (**CISC**) on 25 November 2021 (**Town Hall**), on behalf of the Department of Home Affairs (**the Department**), CISC indicated that the Minister's intention is to exercise their power to 'switch on' the Mandatory Reporting Obligation for specific critical assets in almost all of the eleven impacted sectors. Impacted entities that own or operate critical assets within those sectors will be contacted by the Department by email in relation to this intention.

However, the CISC has advised that, at this stage, the Minister does not necessarily intend to 'switch on' the Asset Registration Obligation for all sectors.

It is important for all organisations that are responsible entities to ensure that they carefully consider the new regime and its potential impact, particularly as there will be continuing engagement opportunities throughout the development of Bill Two.

Government Assistance Measures

The First Bill empowers the Minister for Home Affairs to authorise the Secretary to do any or all of the following things in relation to the critical infrastructure sector if a cyber security incident has had, is having, or is likely to have, a relevant impact on a critical infrastructure asset:

1	***give information-gathering directions***	>	to determine if another power under the Act should be exercised;
2	***give an action direction***	>	directing a responsible entity to do, or refrain from doing, a specified act or thing; or
3	***give an intervention request***	>	request an authorised agency (ie, the Australian Signals Directorate) to provide support (with agreement from the Prime Minister and the Minister for Defence).

The Government Assistance Measures may be provided immediately prior, during or following a relevant cyber security incident.

A **cyber security incident** is defined as "one or more acts, events or circumstances involving unauthorised:

2. modification of computer data or a computer program;
3. impairment of electronic communication to or from a computer; or
4. impairment of the availability, reliability, security or operation of a computer, computer data or a computer program."

For the Government Assistance Measures to be authorised, the Minister must be satisfied that:

2. the incident has had, is having, or is likely to have, a relevant impact on a critical infrastructure asset; and
3. there is a material risk that the incident has seriously prejudiced, is seriously prejudicing, or is likely to seriously prejudice:
   a) the social or economic stability of Australia or its people; or
   b) the defence of Australia; or

   and no existing regulatory system of the Commonwealth, a State or a Territory could be used to provide a practical and effective response to the incident.

Accordingly, there is a threshold that must be met before the Government Assistance Measures may be invoked. There are also additional protections built into the First Bill for each of the Government Assistance Measures to further protect against misuse. These are summarised in the table below:

Minister's available response to a reported cyber security incident	Response requirements
Issue an information-gathering direction	The Minister must be satisfied that the directions that could be authorised are likely to facilitate a practical and effective response to the incident.
Issue an action direction	The Minister must be satisfied that: 1. the relevant entity is unwilling or unable to take all reasonable steps to respond to the incident; 2. the direction is reasonably necessary for the purposes of responding to the incident; 3. the direction is proportionate response to the incident (having regard to the impact of the direction on the activities carried on by the entity and the functioning of the asset concerned, the consequences of compliance with the direction and such other matters the Minister considers relevant); and 4. compliance with the direction is technically feasible. Further, the Minister must not give an action direction that constitutes an intervention action or forces the entity to take offensive cyber action against a person who is directly or indirectly responsible for the incident.
Issue an intervention request	The Minister must be satisfied that: 1. issuing an action direction would not amount to a practical and effective response to the incident; 2. the relevant entity (or entities) is (or are) unwilling or unable to take all reasonable steps to respond to the incident; 3. it meets the necessity, proportionality and technical requirements outlined in relation to action directions above; 4. compliance with the request is technically feasible; 5. it does not force the responsible entity to take offensive cyber action against a person who is directly or indirectly responsible for the incident; and 6. each of the acts or things specified in the request falls within the acts or things listed in section 35AC. The Minister must also have obtained the agreement of the Prime Minister and the Defence Minister regarding the specified request.

It is apparent that the Government Assistance Measures (in particular, the intervention request) are only intended to be used in very serious circumstances. This conclusion is supported by guidance material produced by CISC, which provides that the Government Assistance Measures (particularly the intervention request) are measures of 'last resort' and directions will not be made without consultation with the responsible entity. The guidance materials also confirm that directions provided under the Government Assistance Measures will specify the timeframe during which the directions apply (which may not exceed 20 days).

Measures Mandatory Reporting Obligation

The Mandatory Reporting Obligation does not presently apply, but may be 'switched on'. At the Town Hall, CISC indicated that the Minister's intention was to exercise their power to 'switch on' this obligation for each of the sectors (other than defence).

The Minister may commence a consultation period for a minimum of 28 days on draft rules to 'switch on' the Mandatory Reporting Obligation. Affected entities will be emailed to advise them of the consultation process, and the opportunity to make submissions will be provided.

Further detail of the Mandatory Reporting Obligation will be contained in the (yet to be released) rules. However, the First Bill provides a framework for a mandatory obligation to notify 'critical cyber incidents' and other cyber Incidents. The timeframes and circumstances for these notifications are summarised in the table below:

Class of cyber incident	Description of the incident	Matters to include in the notice	Initial notice period	Notice period if initial notice given orally
SECTION 30BC: **Critical cyber incident**	Where the responsible entity becomes aware of a cyber security incident that has occurred or is occurring and that incident has had, or is having, a 'significant impact' (directly or indirectly) on the availability of a critical asset.	The entity must give the relevant Commonwealth body (to be specified in the rules) a report that: 1. is about the incident; and 2. includes such information (if any) as is prescribed by the rules.	Within 12 hours of the entity becoming aware of the incident.	Within 84 hours of the time the initial oral report was given, in an approved form.
SECTION 30BD: **All other cyber security incidents**	Where the responsible entity becomes aware of a cyber security incident that has occurred or is occurring or is imminent, and that incident has had, is having or is likely to have a 'relevant impact' (directly or indirectly) on a critical asset.	The entity must give the relevant Commonwealth body (to be specified in the rules) a report that: 1. is about the incident; and 2. includes such information (if any) as is prescribed by the rules.	Within 72 hours of the entity becoming aware of the incident.	Within 48 hours of the time the initial oral report was given, in an approved form.

Critical cyber incidents

A cyber security incident will have a ***significant impact*** if the critical infrastructure asset is used in connection with the provision of essential goods or services, and the incident has materially disrupted the availability of those essential goods or services. The rules may also prescribe circumstances giving rise to a 'significant impact'.

Other cyber incidents

A *relevant impact* includes an impact on the availability, integrity, reliability or confidentiality of the critical infrastructure asset.

Asset Register Obligation

The Minister may also 'switch on' the Asset Register Obligation. This requires reporting entities, who are either direct interest holders or the responsible entity for critical infrastructure assets, to maintain a register of interest and control and operational information. At the Town Hall, CISC indicated that the Minister does not currently intend to 'switch on' this obligation for all of the sectors.

3. ENFORCEMENT

The First Bill provides enforcement powers including civil penalty orders, injunctions and infringement notices. For example, in relation to both types of cyber security incidents, contravention of provisions relating to the timing and form of the report carry a civil penalty of 50 penalty units (approximately $11,100). An entity that provides notice under sections 30BC and 30BD will not be held liable for damages in relation to an act done or omitted in good faith in compliance with these sections.

4. TIMEFRAME

The Government Assistance Obligations became law on 2 December 2021. The CISC is currently drafting rules expected to 'switch on' the Mandatory Reporting Obligation, likely in 2022.

The Department has also consulting with a number of sectors in relation to the Second Bill, which will introduce comprehensive risk management program obligations. The Department indicated at the Town Hall that, at this time, it does not intend to recommend that the Minister 'switch on' the risk management program obligation for all of the sectors.

5. NEXT STEPS

If your organisation is in one of the affected sectors, and receives a direction under the Government Assistance Measures that meets the thresholds in the Act, it must comply with that direction. Organisations should also be alert to a possible email communication from the Department to 'switch on' the Mandatory Reporting Obligation and Asset Register Obligation for their sector.

In preparation for these changes, organisations should consider what uplifts are required to their existing policies, procedures and processes, as well as with entities in their supply chain, in order to comply with these new obligations.

MinterEllison provides full service IT legal and consultancy services with extensive experience in cyber security, privacy, data protection and software and IT service procurement. Please contact us if you would like assistance in understanding and implementing your obligations under the new security of critical infrastructure laws.