

# SOCI ACT EXPLAINED

*Cyber security and critical infrastructure law reforms*

Updated April 2023

LANDER  
& ROGERS

DISCLAIMER | This guide cannot be regarded as legal advice. Although all care has been taken in preparing this information, readers must not alter their position or refrain from doing so in reliance on this guide. Where necessary, advice must be sought from competent legal practitioners. The author does not accept or undertake any duty of care relating to any part of this document.

## INTRODUCTION

---

*More than 18 months after its original announcement, the full package of reforms to the Security of Critical Infrastructure Act 2018 (SOCI Act) has been implemented with important implications for critical infrastructure sectors in Australia.*

In this guide, we explore the importance of the reforms and the practical implications for Australian critical infrastructure providers. The guide also provides a snapshot of how the critical infrastructure reforms in Australia compare to other key jurisdictions in the US, UK, Canada, European Union, China and Singapore.

### Key obligations explained

Learn more about obligations and how they apply including:

- understanding and complying with positive security obligations (PSOs)
- other reforms and obligations including the enhanced cyber security obligations of Systems of National Significance (SoNS)

Importantly, whilst a business may be captured by the SOCI Act, not all of the obligations in the SOCI Act may be applicable to that business. However, it is important for businesses to identify if they are captured by the SOCI Act and understand whether additional responsibilities may apply in future.

For assistance assessing and managing the impacts of the reforms to the SOCI Act on your business, please contact the Lander & Rogers cyber team.

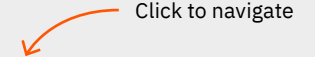
Homepage

Quick links



Click to navigate

Key terms

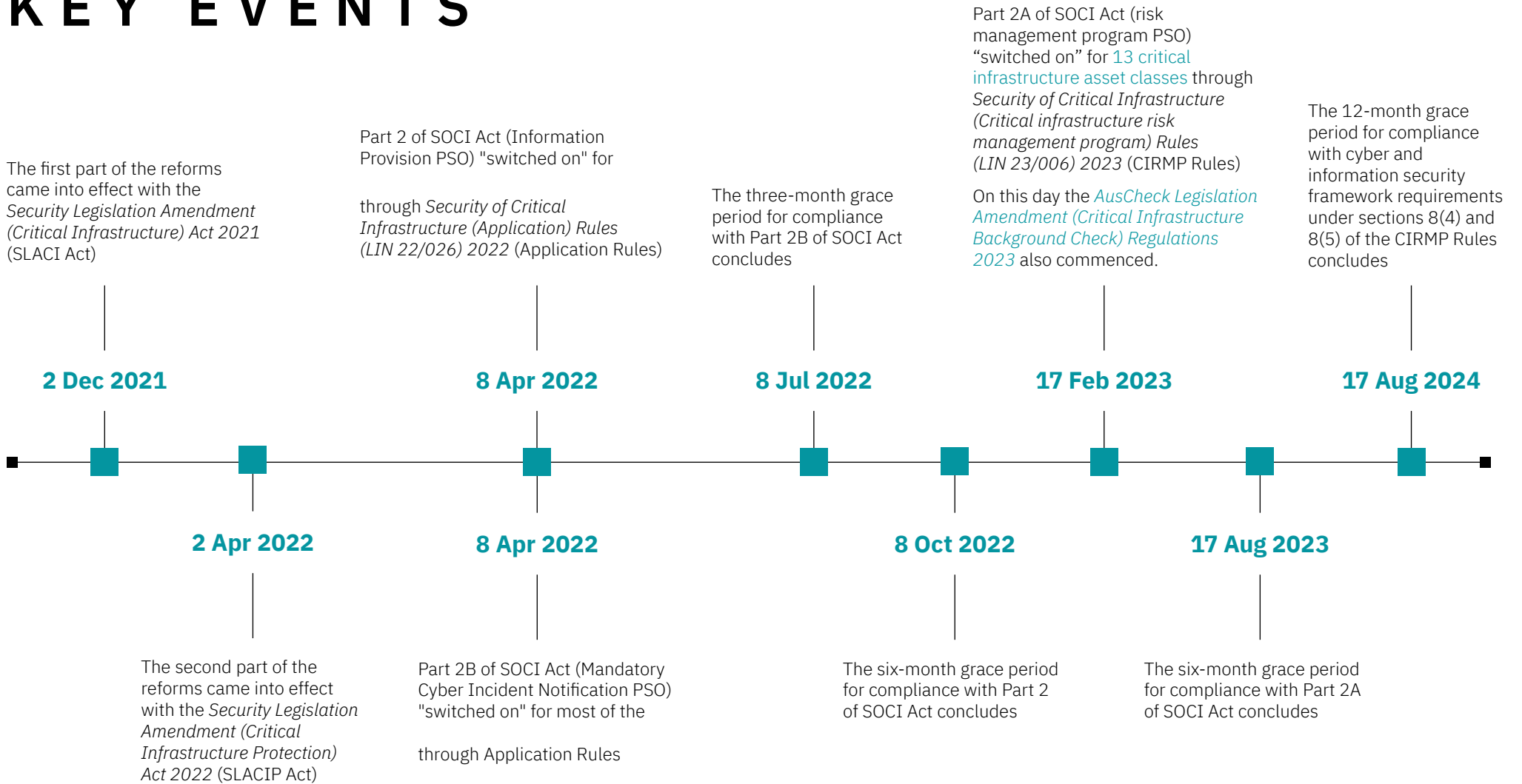


Click to navigate

# TIMELINE

 Hover over highlighted words for more information

# KEY EVENTS



## OVERVIEW

*The functioning of Australia's economy and society is underpinned by our critical infrastructure or essential services. However, geopolitical tensions and heightened cyber threats mean Australia's critical infrastructure is increasingly under threat.*

The statistics are sobering. According to the Australian Cyber Security Centre's (ACSC) Annual Cyber Threat Report, cybercrime reports are increasing, with approximately one quarter of the reported cyber incidents associated with Australia's critical infrastructure or essential services.<sup>1</sup> If successful, a significant cyber attack would be crippling and strike at the heart of Australia's national security.

The SOCI Act, which commenced on 11 July 2018, creates a framework for the regulation of critical infrastructure sectors. However, prior to the reforms, it only covered four sectors: electricity, gas, water and maritime ports.

As part of Australia's Cyber Security Strategy 2020, the Australian Government introduced critical infrastructure law reforms with the aim to protect and improve the resilience of Australia's critical infrastructure.

Most critical infrastructure in Australia is either privately owned and operated, or run on a commercial basis by government.<sup>2</sup> The cybersecurity and critical infrastructure law reforms reflect:

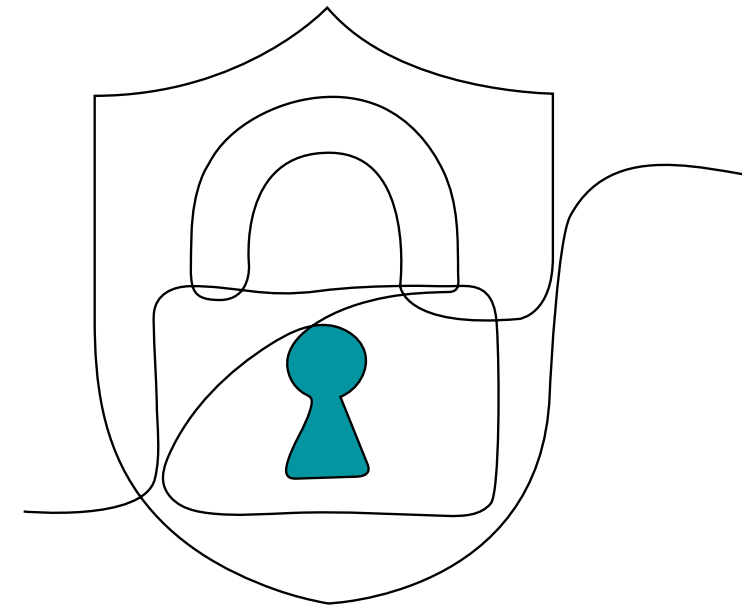
- the government's response to the increasing cyber security threats Australian organisations and essential services are facing; and
- a recognition that effectively addressing cyber security threats requires a joint effort and shared responsibility between the owners and operators of critical infrastructure and the Commonwealth and state/territory governments.

The reforms occurred over two stages:

1. The first part of the reforms came into effect on 2 December 2021 with the *Security Legislation Amendment (Critical Infrastructure) Act 2021* (SLACI Act).
2. The second part of the reforms came into effect on 2 April 2022 with the *Security Legislation Amendment (Critical Infrastructure Protection) Act 2022* (SLACIP Act).<sup>3</sup>

The split in implementation of the reforms was a result of the recommendations by the Parliamentary Joint Committee on Intelligence and Security (PJCIS) in its Advisory Report<sup>4</sup> published on 29 September 2021.

Learn more about the report and findings [here](#).



## DEFINITION

---

Australian federal, state and territory governments define critical infrastructure as:

*‘those physical facilities, supply chains, information technologies and communication networks which, if destroyed, degraded or rendered unavailable for an extended period, would significantly<sup>5</sup> impact the social or economic wellbeing of the nation or affect Australia’s ability to conduct national defence and ensure national security’.<sup>6</sup>*

# WHAT SECTORS AND ASSETS ARE COVERED?

*Under the reforms, the SOCI Act has expanded to cover eleven sectors and 22 asset classes.*

The expansion from four to eleven critical infrastructure sectors including health care and medical, food and grocery, and higher education and research, is a clear recognition by legislators that the social and economic wellbeing of Australia and the ability for Australia to ensure national security extends beyond just utilities and transport. It comes down to the key components for survival such as food and health, and potential avenues for foreign interference such as through Australian universities.

In comparison, the US has 16 critical infrastructure sectors,<sup>7</sup> which are largely consistent with the sectors in Australia, with a few additions. The additions include the chemical sector; dams sector; nuclear reactors, materials and waste sector; and commercial facilities sector, which includes a diverse range of sites that draw large crowds of people for shopping, business, entertainment, or lodging.

The Department of Homeland Security has stated that it considers the 16 critical infrastructure sectors “so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.”

The divergence in classifications lies largely in the differences between Australian and US economies, and what each nation considers its essential services that would significantly impact the social or economic wellbeing of their nation.

However, it is interesting to note that at the time of publication, space systems is absent from the list of US critical infrastructure sectors. However, the US government is taking steps to add space to its critical infrastructure list.<sup>8</sup>

### What is an asset?

The Act broadly defines an asset as a system, network, facility, computer, computer device, computer program, computer data, premises and “any other thing”.

The specific meaning of these assets can be found in section 5 and sections 10-12KA of the SOCI Act, and the *Security of Critical Infrastructure (Definitions) Rules (LIN 21/039) 2021* (Definition Rules). The Minister may also privately declare an asset to be a critical infrastructure asset,<sup>9</sup> or an asset may be declared as a critical infrastructure asset under the Rules (section 9(1)(f)<sup>10</sup>).

For example, critical food and grocery assets are critical supermarket retailers, critical food wholesalers and critical grocery wholesalers. The Definition Rules currently prescribes Aldi Pty Ltd, Coles Group Limited and Woolworths Group Ltd as critical supermarket retailers, and MetCash Trading Ltd as a critical grocery wholesaler.

# SOCI ACT EXPLAINED


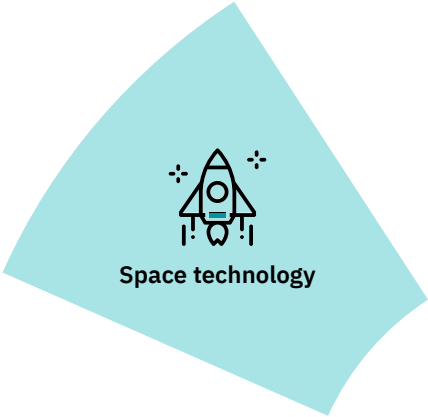
 Hover over the icons for more information

Diagram 1.0: SOCI Act sectors and asset classes



## Sectors





# WHAT ARE THE REFORMS AND NEW OBLIGATIONS?

*The reforms to the SOCI Act seek to strengthen the security and resilience of critical infrastructure assets by introducing Positive Security Obligations (PSOs) that require entities to manage the security and resilience of their critical infrastructure assets.*

### Positive Security Obligations (PSOs)

Following the reforms, there are now three PSOs for critical infrastructure assets in the SOCI Act.

- Extension of the obligation to report ownership and operational information relating to critical infrastructure assets to be included in the register of critical infrastructure assets (Part 2 of the SOCI Act, as amended by the SLACI Act) (*Information Provision PSO*).
- Mandatory cyber security incidents notification obligation (Part 2B of the SOCI Act, inserted by the SLACI Act) (*Mandatory Cyber Incident Notification PSO*).
- An obligation on the responsible entities of certain critical infrastructure assets to adopt and maintain a risk management program including regular review and updating of the program (Part 2A of the SOCI Act, inserted by the SLACIP Act) (*Risk Management Program PSO*).

Responsible entities exempt from the Risk Management Program PSO have separate annual reporting requirements (Part 2AA of the SOCI Act, inserted by the SLACIP Act).

Compliance with the PSOs will be required once ‘switched on’. The Rules will determine which elements of the PSOs are ‘switched on’ for particular types of critical infrastructure assets. The ‘switching on’ mechanism allows for tailored requirements that recognise (not duplicate) existing arrangements.

### Systems of National Significance (SoNS)

The reforms also introduced the concept of Systems of National Significance (SoNS):

- Declaration of Systems of National Significance (SoNS) (Part 6A of the SOCI Act, inserted by the SLACIP Act).
- Enhanced cyber security obligations applicable to SoNS (Part 2C of the SOCI Act, inserted by the SLACIP Act).

### Other reforms

The reforms also implemented the following key changes:

- The Government Assistance and Intervention Regime in relation to serious cyber security incidents (Part 3A of the SOCI Act, inserted by the SLACI Act).
- Enhancing the framework for the use and disclosure of protected information (amendments to Part 4 of the SOCI Act, as amended by the SLACI Act).

### Who has to comply?

The responsibility for complying with the new obligations lie principally with either the Responsible Entity or Direct Interest Holders.

#### Responsible Entity

A Responsible Entity<sup>41</sup> of a critical infrastructure asset is the entity with ultimate operational responsibility for the asset. This entity will have effective control or authority over the operations and functioning of the asset as a whole and able to engage the services of contractors and other operators. The Responsible Entity will also serve as the key contact point for consultation in relation to rules that may impact the asset.

#### Direct Interest Holders

Direct Interest Holders<sup>42</sup> are entities that hold a direct or joint interest of at least 10 per cent in a critical infrastructure asset, or who hold an interest and are able to directly or indirectly influence or control the asset.

However, as noted below, some of the obligations will impact a “relevant entity”, which is defined as the Responsible Entity or Direct Interest Holder or operator of the asset or a managed service provider<sup>43</sup> for the asset.

# HOW REFORMS WILL IMPACT AUSTRALIAN BUSINESSES

*There are numerous implications for Australian businesses flowing from the SOCI Act reforms.*

### Principle-based rules

The reforms largely rely on principle-based rules and regulation. This means the SOCI Act does not rely on prescriptive rules, but more on high-level, broadly stated rules or principles to set the standards by which regulated organisations must conduct business.

This is said to provide the necessary flexibility and clarity for industry and to enable Responsible Entities to manage security risks under principle-based outcomes.

Whilst principle-based rules can provide flexibility, they can also create uncertainty and unpredictability for both the regulator and the regulated community in relation to compliance, as they often come down to a question of judgment.

### Regulatory compliance costs

The regulatory compliance cost is not insignificant owing to the breadth of the reforms. The draft Regulatory Impact Statement (RIS) conducted in relation to Part 2A weighs the regulatory costs of the Risk Management Program rules against the damage to the economy if a business underinvests in security and allows breaches to occur.

The RIS has identified that, if the critical infrastructure risk management program obligation is introduced, the average expected costs for Responsible Entities to implement and maintain this obligation across all sectors is currently an average one-off cost of \$9 million per entity followed by an average ongoing cost of \$3.7 million per annum per entity to maintain compliance.

The cost of regulation will be borne by entities responsible for critical infrastructure assets who meet the relevant thresholds. Whilst community organisations and individuals will not be directly affected, there will likely be indirect costs passed onto consumers.

The RIS states that the likely benefits of the critical infrastructure risk management program obligation will be at least (and are expected to be more than) the costs of the regulation. Whilst that is true in the long run, some Responsible Entities may view the penalties as significantly lower in comparison to the ongoing costs of compliance. The highest monetary penalty appears to be 200 penalty units or \$44,400 for an individual and 1,000 penalty units or \$222,000 for a body corporate.<sup>49</sup>

### Mandatory notification timeframes

The short timeframe for notification of a cyber security incident requires businesses to ensure that they have a robust process in place to ensure compliance.

The SOCI Act now requires critical cyber security incidents to be reported within 12 hours of becoming aware of the incident and for other cyber security incidents to be reported within 72 hours of becoming aware of the incident.

These timeframes are relatively stringent when compared to the mandatory reporting regimes in other jurisdictions, notwithstanding the 6-hour requirement in India.

- In the US, the *Cyber Incident Reporting For Critical Infrastructure Act of 2022* requires notification to the Cybersecurity & Infrastructure Security Agency (CISA) within 72 hours after the entity “reasonably believes” that a covered cyber incident has occurred and requires notification of any ransom payments made within 24 hours.<sup>14</sup>
- In the UK, the Network and Information Security (NIS) Regulations applies to two groups of organisations:
  - ‘operators of essential services’ (OES) across critical infrastructure such as in health, energy and transport;
  - ‘relevant digital service providers’ (RDSPs).

In both instances, it requires a NIS incident to be notified to the Information Commissioner’s Office (ICO) without undue delay and not later than 72 hours of becoming aware of it.<sup>15</sup>

## SOCI ACT EXPLAINED

- In India, the Ministry of Electronics and Information Technology has mandated that service providers, intermediaries, data centres, body corporates and government organisations report any cyber breaches or leaks to CERT-In within six hours of noticing such incidents or being brought to notice about such incidents. The regulation comes into force 60 days from 28 April 2022 on 27 June 2022.<sup>16</sup>

In response, affected businesses must have a robust incident response plan in place that includes a clear understanding of the defined roles and reporting lines necessary to comply with the Mandatory Cyber Incident Notification PSO. This includes:

- an understanding of whose awareness would trigger the clock for notification,
- how the assessment of whether a cyber incident is “critical” or “other” would be undertaken, and
- who is in charge of ensuring the relevant notification is made within the 12-hour or 72-hour stipulation.

### Minister’s and Secretary’s powers

The Minister’s and Secretary’s powers under the SOCI Act have been enhanced with the reforms.

For example, section 30CB<sup>17</sup> and a number of other provisions in new Part 2C of the SOCI Act contain provisions that provide an administrative discretion by a decision maker, including the Secretary’s decision to provide written notices to SoNS regarding their enhanced cyber security obligations under subsections 30CM(1), 30CU(1), 30CR(2), 30DB(2), 30DC(2) and 30DJ(2).

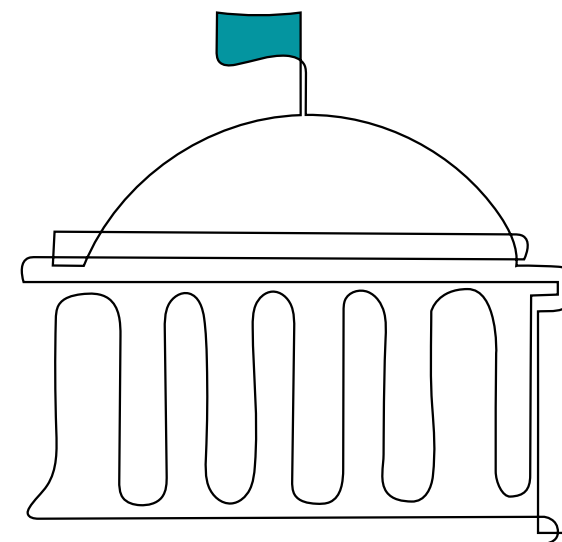
Recommendation 7 and paragraph 3.49 of the PJCIS report suggested that administrative decisions under these decisions, and decisions of the Minister to declare a SoNS (see section 52B) should be subject to merits review in the Security Division of the AAT.<sup>18</sup>

However, the government’s position is to exclude merits review for section 30CB, other Part 2C decisions and decisions to declare a SoNS because it is considered to be inappropriate in light of the sensitive nature of critical infrastructure assets, and to ensure that external or malicious actors would not be able to easily identify and target the assets of highest criticality.

Further, the Secretary’s decisions under Part 2C are likely to contain information that is even more sensitive, given that the various obligations may be applied to assist an entity to uplift and review its cyber security.

Ordinarily, merits review is excluded for decisions containing policy decisions of high political content because of their potential to impact the Australian economy, potential impact to Australia’s relations with other countries, and their relationship to national security.

In addition, the Minister’s decision for the declaration of an asset to be a critical infrastructure asset or to be a SoNS can only be made by the Minister personally, and there is no statutory power of delegation of the Minister’s powers under the SOCI Act. That said, judicial review, including review under the *Administrative Decisions (Judicial Review) Act 1997* (ADJR Act), is available in relation to such decisions.



## KEY OBLIGATIONS EXPLAINED

# UNDERSTANDING AND COMPLYING WITH PSO'S

### Information Provision PSO

Part 2 of the SOCI Act requires the Responsible Entity for a critical infrastructure asset to give operational information, and a Direct Interest Holder in relation to the asset must give interest and control information, to the Secretary of the Department of Home Affairs to be included in the Register of Critical Infrastructure Assets (Register).<sup>19</sup> This obligation to give information is ongoing.

If an event occurs that causes previously provided operational information or interest and control information to become incorrect or incomplete (a 'notifiable event'), then the Responsible Entity or Direct Interest Holder has an obligation to notify the Secretary of the notifiable event and correct or complete that information.<sup>20</sup>

Part 2 is not new. What is new is the extension of the PSO to the specified new sectors and asset classes that are 'switched on' in the rules.

The *Security of Critical Infrastructure (Application) Rules (LIN 22/026) 2022* (Application Rules) commenced on 8 April 2022 and have specifically 'switched on' Part 2 for 13 critical infrastructure asset classes.<sup>21</sup> The Application Rules however have not 'switched on' the Information Provision PSO for assets in the education, defence industry and space technology sectors, and specifically exclude four sugar mills in Queensland.<sup>22</sup>

Further, a six-month grace period is in place for compliance up until 8 October 2022. Non-compliance with the Information Provision PSO will result in civil penalties of 50 penalty units or \$11,100 for an individual and 250 penalty units or \$55,500 for a body corporate.

### Mandatory Cyber Incident Notification PSO

The new Part 2B of the SOCI Act requires Responsible Entities to report two types of cyber incidents:

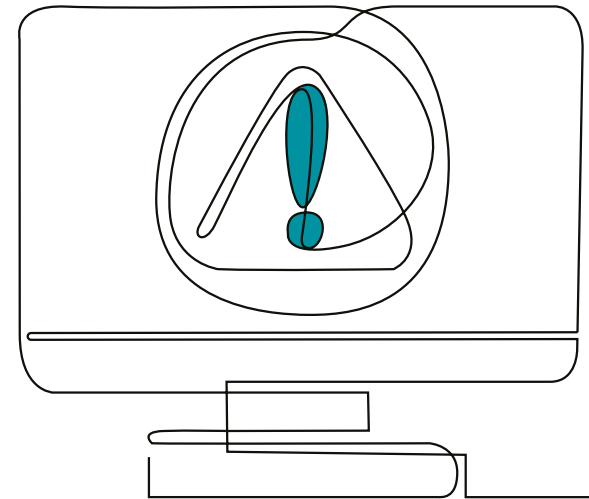
- Critical cyber security incidents, and
- Other cyber security incidents.

The SOCI Act defines "cyber security incident" as one or more acts, events or circumstances where there has been:

- unauthorised access or unauthorised modification to computer data or a computer program;
- unauthorised impairment of electronic communications to or from a computer; and
- unauthorised impairment of the availability, reliability, security or operation of a computer, computer data or a computer program.<sup>23</sup>

The purpose of the Mandatory Cyber Incident Notification PSO is to assist the government in developing an aggregated threat picture and comprehensive understanding of cyber security risks to critical infrastructure in a way that is mutually beneficial to government and industry.

This will better inform both proactive and reactive cyber incident response options, ranging from providing voluntary assistance to industry, to building a culture of cyber security.



# KEY OBLIGATIONS EXPLAINED

## Key considerations

In considering compliance with the Mandatory Cyber Incident Notification PSO, it is important to note the following.

- **Awareness:** awareness is a question of fact. It is important to consider and determine beforehand whose awareness within your organisation will trigger the countdown for notification, and who will have responsibility for making the notification within the timeframe.
- **Assessing significance:** the determination of whether an incident is having a “significant impact” on the availability of an asset will be a question of judgment. In assessing the criticality of a cyber incident, a Responsible Entity should consider the type of service provided, the impact of a disruption to essential services and the nature and extent of the cyber incident. A material disruption to the critical infrastructure’s essential services will satisfy the significant impact threshold.
- **Acting in good faith:** Section 30BE of the SOCI Act provides immunity by excluding Responsible Entities, a member of a related company group and contracted service provider (and their officers, employees or agents), from liability in an action or proceeding for damages if they acted in good faith in compliance with the Mandatory Cyber Incident Notification PSO. This provision is intended to protect entities from incurring liabilities, such as those resulting from contravening confidentiality requirements that may exist in contracts with customers, when complying with this PSO. However, the current immunities in the SOCI Act do not protect:
  - officers, employees and agents of separate but related entities who engage in conduct for the purpose of compliance with obligations of the primary entity (unless they come within the concept of an ‘agent’); and
  - persons (natural or legal) who are engaged to provide services or advice to the primary entity on a contractual basis.

**Table 1.1: The table below summarises the notification requirements.**

Type of cyber incident	Impact	Timing of notification	How to notify?
<b>Critical</b> If you become aware that a critical cyber security incident has occurred, or is occurring, and the incident has had, or is having, a ‘significant impact’ on the availability of your asset.	An incident will be considered to have a ‘significant impact’ if the critical infrastructure asset is used in connection with the provision of essential goods and services, and the incident has materially disrupted the availability of the essential goods or services delivered. (Section 30BEA)	Notify the Australian Cyber Security Centre (ACSC) within 12 hours after you become aware of the incident (section 30BC)	Verbally or in writing through the ACSC website. If report was made verbally, make a written record through the ACSC’s website within 84 hours of verbally notifying the ACSC.
<b>Other</b> If you become aware that a cyber security incident has occurred, or is occurring, and the incident has had, is having, or is likely to have, a ‘relevant impact’ on your asset	A ‘relevant impact’ means an impact on the availability, integrity, reliability or confidentiality of the asset. See Section 8G(2).	Notify the ACSC within 72 hours after you become aware of the incident (section 30BD)	Verbally or in writing through the ACSC website. If report was made verbally, make a written record through the ACSC’s website within 48 hours of verbally notifying the ACSC.

The Application Rules have specifically ‘switched on’ Part 2B for most of the critical infrastructure assets.<sup>24</sup> However, four sugar mills in Queensland<sup>25</sup> and certain critical aviation assets and critical maritime assets<sup>26</sup> are excluded. Further, a three-month grace period is in place for compliance up until 8 July 2022 to allow for transition.

### Non-compliance

Non-compliance with this Mandatory Cyber Incident Notification PSO will result in civil penalties of 50 penalty

units or \$11,100 for an individual and 250 penalty units or \$55,500 for a body corporate.

### Reporting

At this stage, the notification report will only be shared with the Department of Home Affairs, as the critical infrastructure security regulator, if the organisation consents. It will not be forwarded or shared with other regulators.



# KEY OBLIGATIONS EXPLAINED

## Risk management program PSO

The new Part 2A of the SOCI Act provides that the Responsible Entity of specified critical infrastructure assets must:

- adopt, maintain<sup>27</sup> and comply<sup>28</sup> with a written critical infrastructure risk management program;
- regularly review such a program<sup>29</sup> (noting a definitive timeframe within which the program must be reviewed is not specified);<sup>30</sup> and
- take all reasonable steps to ensure the program is up to date.<sup>31</sup>

Part 2A sets out the overarching obligations for the risk management programs, with the more detailed requirements to be contained in risk management program rules.

The *Security of Critical Infrastructure (Critical infrastructure risk management program) Rules (LIN 23/006) 2023* (CIRMP Rules) have been registered and commenced 17 February 2023. The *AusCheck Legislation Amendment (Critical Infrastructure Background Check) Regulations 2023* also commenced 17 February 2023.

Principle-based rules will be utilised to provide the necessary flexibility and clarity for industry. The SOCI Act and the proposed rules combined will ultimately require Responsible Entities to manage security risks under principle-based outcomes.



## Who does this PSO apply to?

This PSO only applies to critical infrastructure assets that are privately declared (pursuant to section 51), or specified in the CIRMP Rules, to be “switched on” and not subject to other regulatory schemes of a similar nature.

The CIRMP Rules have “switched on” this PSO for 13 asset classes where there are not already sufficient regulatory or administrative arrangements in place.

The 13 asset classes are:

- critical broadcasting assets;
- critical domain name systems;
- critical data storage or processing assets;
- critical electricity assets;
- critical energy market operator assets;
- critical gas assets;
- designated hospitals<sup>32</sup>;
- critical food and grocery assets;
- critical freight infrastructure assets;
- critical freight services assets;
- critical liquid fuel assets;
- critical financial market infrastructure assets mentioned in paragraph 12D(1)(i) of the Act (i.e. an asset that is used in connection with the operation of a payment system); and
- critical water assets.

Further, the Australian Government does not intend to ‘switch on’ any of the PSOs (including Part 2A) for critical education assets. This is because the assets are a class of critical infrastructure assets with appropriate regulatory requirements or arrangements in place.<sup>33</sup>

## Exempt entities and their obligations

The entities exempt from compliance with Part 2A are as follows where the:

- Responsible Entity is an entity that is certified strategic under the Commonwealth’s *Digital Certification Framework*;<sup>34</sup> or
- Responsible Entity is an entity covered by a federal, state or territory law specified by rules;<sup>35</sup> or
- critical infrastructure asset is covered by a provision of a federal, state or territory law specified by rules.<sup>36</sup>

For these critical infrastructure assets exempt from the Risk Management Program PSO, Part 2AA provides that the Responsible Entity must give an annual report, within 90 days after the end of a financial year, to the relevant Commonwealth regulator or Secretary.

The annual report prepared by exempt entities should be in the approved form and set out:

- why those assets are exempt,
- a description of any hazards having a relevant impact on assets, and
- the effectiveness of any actions the entity took to mitigate the hazard.

They must also be approved by the board, council or other governing body of the entity if they exist.<sup>37</sup> A failure to do so will result in civil penalties of 150 penalty units or \$33,300 for individuals and 750 penalty units or \$166,500 for a body corporate.

The information in such a report is not admissible in evidence and cannot be used by the regulator or Department of Home Affairs to take compliance action against the Responsible Entity under the SOCI Act.<sup>38</sup>



## KEY OBLIGATIONS EXPLAINED

### Risk management program requirements

Firstly, Responsible Entities must develop a written critical infrastructure Risk Management Program<sup>39</sup> with a purpose to:

- **Identify hazards and risk of occurrence.** Identify each hazard where there is a ‘material risk’ that the occurrence of the hazard could have a ‘relevant impact’<sup>40</sup> on the asset;
- **Minimise/eliminate risk of hazard occurring.** So far as it is ‘reasonably practicable to do so’, minimise or eliminate any material risk of such a hazard occurring;<sup>41</sup>
- **Mitigate relevant impact.** So far as it is reasonably practicable to do so, mitigate the relevant impact of such a hazard on the asset;<sup>42</sup>
- **Comply with any requirements specified in the rules.** The CIRMP Rules will be used to provide further requirements on how the principle-based obligations set out above are to be implemented.

Determinations of ‘material’ risk should consider the likelihood of the hazard occurring and the relevant impact of the hazard on the asset if the hazard were to occur.<sup>43</sup>

This obligation is not prescriptive. It is for the Responsible Entity to undertake this risk identification process, in line with existing processes inside the business, to determine how to understand and manage material risk.

### Meaning of “material risk”

Section 6(a) to (e) of the CIRMP Rules sets out what constitutes “material risk”. This includes the risk of impairment, stoppage, loss of access to or interference with the asset.

### Meaning of “relevant impact”

A “relevant impact” is a direct or indirect impact on the availability, integrity, reliability of the critical infrastructure asset or confidentiality of information about the asset, information stored in the asset if any, and, if the asset is computer data, the computer data. It must be more serious than a reduction in the quality of the service being provided.

### Meaning of “so far as it is reasonably practicable”

The requirement of ‘so far as it is reasonably practicable’ is to enable Responsible Entities to show what was, at a particular time, reasonably able to be done to address material risks. The expectation is not for Responsible Entities to eliminate risk entirely but to do so to the extent it is reasonably able to manage material risks. The board, or equivalent, is required to approve the risk management plan within this context, appropriately balancing operational costs with risk.

In preparing the written critical infrastructure Risk Management Program, Responsible Entities should consider all relevant factors, including:

- the likelihood of the risk;
- the degree of harm that might result from the risk;
- what the Responsible Entity concerned knows, or ought to reasonably know, about the hazard or risk;
- ways of eliminating or minimising the risk; and
- the availability and suitability of ways to eliminate or minimise the risk and the cost associated, including whether the cost is grossly disproportionate to the risk.

As part of its compliance activities, the Department of Home Affairs will consider the diversity of the entity, taking into consideration and assessing Responsible Entities against its compliance posture. It is not expected that all entities will be required to undertake the same measures. Rather, required measures will be determined based on the Responsible Entity’s operational context and operating costs.

### Annual reporting

The Responsible Entity must submit an annual report, in an approved form,<sup>44</sup> to the relevant Commonwealth regulator (if one has been prescribed in relation to the Part 2A asset under the rules)<sup>45</sup> or, in any other case, the Secretary within 90 days after the end of the financial year (Section 30AG).<sup>46</sup>

The annual report must be approved by the entity’s board, council or other governing body.

The default regulator is the Department of Home Affairs. It should also be noted that the relevant Commonwealth regulator for the critical financial market infrastructure asset mentioned in section 12D(1)(i) of the SOCI Act is the Reserve Bank of Australia (RBA).

This obligation does not require the Responsible Entity to provide the full critical infrastructure risk management program to the regulator / Secretary, but rather a statement that the program remains up to date, any variations to program, along with details about any hazards that have had a “significant” impact on the asset during the reporting period and details of how the program was effective in mitigating any relevant impacts.<sup>47</sup>

It is not intended that entities will be required to report day-to-day incidents - only those incidents that have had a significant relevant impact. The term ‘significant’ is not defined, and the regulator will work with Responsible Entities to provide guidance about this obligation. However, it is expected that a significant impact would include one that affects the functioning of the asset or its ability to deliver intended services, including:

- a genuine impact on the availability of the asset, or services delivered by the asset such as a significant ransomware attack;
- an impact that causes harm to customers or end-users; or
- a detrimental impact on information security that has undermined the integrity of, or led to the loss, theft or unauthorised access of, sensitive information or personal information, such as a significant data breach.

The information in such a report is not admissible in evidence and cannot be used by the regulator or Department to take compliance action against the Responsible Entity under the SOCI Act.<sup>48</sup>

### Non-compliance

A failure to adopt and maintain a risk management program, comply with the risk management program, regularly review the program, or take all reasonable steps



## KEY OBLIGATIONS EXPLAINED

to ensure the program is up to date will result in civil penalties of 200 penalty units or \$44,400 for individuals and 1,000 penalty units or \$222,000 for a corporate body.

A failure to submit an annual report in accordance with the requirements will result in civil penalties of 150 penalty units or \$33,300 for individuals and 750 penalty units or \$166,500 for a body corporate.<sup>50</sup>



### CIRMP Rules

In establishing their Risk Management Program, Responsible Entities are expected to take an “all-hazards” approach. As contemplated in the CIRMP Rules, the first rules to be made by the Minister under section 30AH(1)(c) will set out the approach taken in relation to four primary domains:

- cyber and information security hazards,
- personnel hazards,
- supply chain hazards, and
- physical and natural hazards.

#### Cyber and information security hazards

Cyber and information security hazards apply where a person, whether authorised or not, improperly accesses or misuses information or computer systems about or related to the asset, or where such person by use of a computer system obtains unauthorised control of or access to any function that may impair the proper functioning of the asset.

Section 8 of the CIRMP Rules provides that a Responsible Entity must establish and maintain a process or system in the risk management program, as far as it is reasonably practicable to do so, to minimise or eliminate a material risk that a cyber and information security hazard for which there is a material risk that the hazard could have a relevant impact on the asset, and to mitigate the relevant impact of a cyber and information security hazard on the asset.

In particular, the CIRMP Rules specify that within 12 months after the end of the six-month grace period, a Responsible Entity must comply with the frameworks contained in the following documents:

- Australian Standard *AS ISO/IEC 27001:2015*,
- At least Maturity Level 1 of the *Essential Eight Maturity Model* published by the Australian Signals Directorate (Essential Eight),

- *Framework for Improving Critical Infrastructure Cybersecurity* published by the US’s National Institute of Standards and Technology (NIST),
- At least Maturity Indicator Level 1 of the *Cybersecurity Capability Maturity Model* published by the US Department of Energy,
- At least Security Profile 1 of the *2020-21 AESCSF Framework Core* published by Australian Energy Market Operator Limited (ACN 072 010 327).

#### Personnel hazards

Personnel hazards apply where a critical worker<sup>51</sup> acts, through malice or negligence, to compromise the proper function of the asset or cause significant damage to the asset, as assessed by the entity, such as by causing a material risk to the asset.

Section 9 of the CIRMP Rules provides that a Responsible Entity must establish and maintain a process or system in the entity’s program:

- to identify the entity’s critical workers; and
- to assess, on an ongoing basis, the suitability of a critical worker to have access to the critical components<sup>52</sup> of the asset and only permit access where the critical worker has been assessed to be suitable to have such access; and;
  - as far as it is reasonably practicable to do so, minimise or eliminate material risks arising from malicious or negligent employees or contractors; and
  - arising from the off-boarding process for outgoing employees and contractors.

This is to address the hazard that trusted insiders (who have legitimate access to information, techniques, technology, assets or premises) pose to critical infrastructure assets.<sup>53</sup>



## KEY OBLIGATIONS EXPLAINED

The process and system for assessing the suitability of a critical worker to have access to the critical components of the asset may be a background check under the AusCheck scheme at regular intervals.<sup>54</sup> The background check is not a mandatory requirement.

The specific operation of the AusCheck scheme, including the criteria against which the background check will be conducted, and the associated amendments required for the *AusCheck Regulations 2017* to enable such background checks, are set out in the AusCheck Legislation Amendment (Critical Infrastructure Background Check) Regulations 2023. The purpose of the AusCheck Legislation Amendment (Critical Infrastructure Background Check) Regulations 2023 (Amendment Regulations) is to amend the AusCheck Regulations to provide for the establishment and operation of the AusCheck background checking scheme for an individual for whom a CIRMP permits a background check.

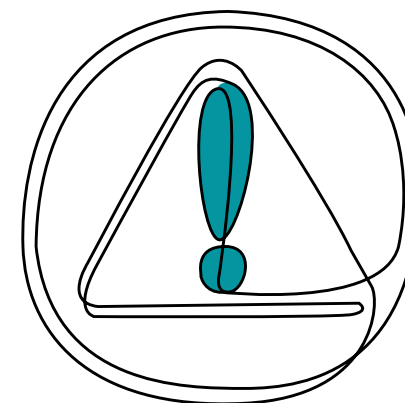
The measures inserted into the AusCheck Regulations by Schedule 1 include:

- introducing an ability for AusCheck to undertake a background check of an individual if such a check is permitted under a CIRMP (a critical infrastructure background check), and to conduct a further background check if the information provided for an initial background check was incomplete or the application requirements were not met;
- specifying the information required to be included in an application for a critical infrastructure background check;
- defining terms for the purposes of a critical infrastructure background check;
- providing advice about the outcome of a critical infrastructure background check to the individual and the responsible entity,
- requirements for conducting electronic and in-person identity verification;
- authorising the Secretary to grant an exemption from specified requirements of an electronic or in-person identity verification check if the individual is unable to meet those requirements;
- requiring the Secretary to give the individual written notice of, and reasons for, a preliminary assessment that an individual has an unfavourable criminal history and enable the individual to make representations;
- authorising the Secretary to request an individual or responsible entity to do a specified thing to ensure information is provided and application requirements are met, and to cancel a background check where that request is not complied with;
- requiring the Secretary to give further advice about a critical infrastructure background check if the Secretary becomes aware that the initial advice is inaccurate or incomplete;
- imposing an obligation on a responsible entity to inform the Secretary of certain decisions made in relation to granting access to the critical infrastructure asset or the revocation of access to the critical infrastructure asset, and create offences for failure to satisfy those obligations;
- authorising applications to be made to the Administrative Appeals Tribunal for review of decisions of the Secretary to refuse to grant an exemption in relation to identity verification requirements or to advise that an individual has an unfavourable criminal history,
- authorising the Secretary to charge a fee for an application for a critical infrastructure background check, and
- setting out offences that are CIRMP-security-relevant offences in Schedule 2.

### Supply chain hazards

To deal with supply chain hazards, section 10 of the CIRMP Rules provides that a Responsible Entity must establish and maintain in the entity's program a process or system that the entity uses to, as far as it is reasonably practicable to do so, minimise or eliminate the material risk of, or mitigate, the relevant impact of:

- unauthorised access, interference or exploitation of the asset's supply chain; and
- misuse of privileged access to the asset by any provider in the supply chain; and
- disruption and sanctions of the asset due to an issue in the supply chain; and
- threats to people, assets, equipment, products, services, distribution and intellectual property within supply chains; and
- high risk vendors / major suppliers; and
- any failure or lowered capacity of other assets and entities in the entity's supply chain; and
- a supply-chain hazard on the asset



## KEY OBLIGATIONS EXPLAINED

### Physical security hazards

Physical security hazards apply where the unauthorised access, interference, or control of critical assets, other than those covered by cyber and information security hazards, including where persons other than critical workers act, through malice or negligence, to compromise the proper function of the asset or cause significant damage to the asset, as assessed by the entity.

**Natural hazards** are defined to include a bushfire, flood, cyclone, storm, heatwave, earthquake, tsunami or health hazard (such as a pandemic).

Section 11 of the CIRMP Rules provides that a Responsible Entity must establish and maintain a process or system in the entity's program:

- to identify the parts of the asset that are critical to the functioning of the asset (the critical sites); and
- as far as it is reasonably practicable to do so, minimise or eliminate a material risk or mitigate a relevant impact of a physical security hazard on a physical critical component or a natural hazard on the CI asset; and
- to respond to incidents where unauthorised access to a critical site occurs; and
- to control access to physical critical components, including restricting access to only those individuals who are critical workers or accompanied visitors; and
- to test that security arrangements for the asset are effective and appropriate to detect, delay, deter, respond to and recover from a breach in the arrangements.

### When do the CIRMP obligations begin?

The CIRMP obligations will apply to the critical infrastructure assets mentioned above on the later of six months after the CIRMP Rules commence, or six months after the asset became a critical infrastructure asset. In other words:

- a. for an existing critical infrastructure asset as at 17 February 2023, the CIRMP obligations will apply from 17 August 2023;
- b. for an asset that becomes a critical infrastructure asset on 1 March 2023, the CIRMP obligations will apply six months from the date it became a critical infrastructure asset, that is, from 1 September 2023.

This is to ensure that the responsible entities are provided with a reasonable timeframe to establish and begin complying with their CIRMP before Part 2A applies to their critical infrastructure asset.

Further, within 12 months following the end of the above 6-month grace period, the responsible entities of these specified critical infrastructure assets must comply with the cyber and information security requirements specified in subsections 8(4) and 8(5) of the CIRMP Rules relating to compliance with a framework.

This means that for (a) above, compliance with the cyber and information security requirements framework will be required by 17 August 2024, and for (b), by 1 September 2024.



# SYSTEMS OF NATIONAL SIGNIFICANCE

## Declaration of Systems of National Significance

Part 6A of the SOCI Act provides that the Minister may personally<sup>53</sup> and privately declare a critical infrastructure asset to be a system of national significance (SoNS).

SoNS are a subset of critical infrastructure assets that have an additional element of criticality based on their national significance.

This is determined by the following factors:<sup>56</sup>

- The consequences that would arise for the social or economic stability of Australia or its people, the defence of Australia, or national security, if a hazard were to occur that had a significant relevant impact on the asset.
- If the Minister is aware of one or more interdependencies between a particular asset and one or more other critical infrastructure assets, the Minister should have regard to the nature and extent of those interdependencies. This is because the interconnectedness of several critical infrastructure assets creates a new set of vulnerabilities. By virtue of the interconnectedness, the compromise of one of these assets could have first, second and third order consequences, which may cascade and compromise other critical infrastructure assets.
- Any other matters the Minister considers relevant to determining the national significance of the asset.

## Notification requirement

The Minister must notify, in writing, each reporting entity for an asset that is a declared SoNS within 30 days after making the declaration. This notification is important due to the enhanced obligations on SoNSs under Part 2C of the SOCI Act.

The declaration of SoNS can be reviewed<sup>57</sup> or revoked.<sup>58</sup>

## Offence to disclose

It is also an offence to disclose that an asset has been declared a SoNS.<sup>59</sup> Due to the security vulnerabilities that may emerge if the extent of the assets' national significance were widely known, it would be inappropriate and negligent to publicly disclose the identity of a system of national significance.

## Enhanced cyber security obligations of SoNS

Part 2C sets out the enhanced cyber security obligations that relate to SoNS. The Responsible Entity for a SoNS may be:

- subject to statutory incident response planning obligations;
- required to undertake a cyber security exercise;
- required to undertake a vulnerability assessment; and
- required to give access to the ASD of system information, including the installation of system information software that transmits system information to the ASD, if a computer is a SoNS or is needed to operate a SoNS.

Before issuing a notice<sup>60</sup> requiring the Responsible Entity for a SoNS to comply with the statutory incident response planning obligations, undertake a cyber security exercise, undertake a vulnerability assessment or give access to the ASD of system information, the Secretary must consider:

- the costs that are likely to be incurred by the entity in complying with this obligation;
- the reasonableness and proportionality of applying obligation to the entity in relation to the system and cyber security incidents; and
- such other matters (if any) as the Secretary considers relevant, including any international trade obligations that apply, whether the entity is, or has been, subject to any other enhanced cyber security obligation, and whether the entity is subject to another regulatory regime under Commonwealth, state or territory law that is similar.<sup>61</sup>

There is also a consultation requirement with the entity and regulator before any such notice is given.<sup>62</sup> There are also civil penalties imposed for non-compliance with the enhanced cyber security obligations.



# OTHER REFORMS

### Government Assistance and Intervention Regime

Part 3A of the SOCI Act sets out a regime for the government to provide assistance and/or intervene in relation to *serious* cyber security incidents.

The regime may apply where:

- a. a cyber security incident has occurred, is occurring or is imminent;
- b. a cyber security incident has had, is having, or is likely to have, a relevant impact (on the availability, integrity, reliability or confidentiality of the asset) on a critical infrastructure asset (primary asset);
- c. there is a material risk that the incident has seriously prejudiced, is seriously prejudicing, or is likely to seriously prejudice the social or economic stability or the defence of Australia or national security; or
- d. no existing regulatory system of the Commonwealth, a state or territory could be used to provide a practice and effective response to the incident;

Where this occurs, the Minister may, in order to respond to the incident, authorise the Secretary to issue the following directions or request:

**1. Information gathering direction:** issue a direction (orally or in writing) to the relevant entity to give information to the Secretary. The Minister has to be satisfied that the directions are likely to facilitate a practical and effective response to the incident. A failure to comply will result in civil penalties of 150 penalty units or \$33,300 for individuals and 750 penalty units or \$166,500 for a body corporate.<sup>63</sup>

**2. Action direction:** issue a particular direction (orally or in writing) to the relevant entity to take particular measures. An action direction must not be given unless:

- the specified entity is unwilling or unable to take all reasonable steps to respond to the incident;
- the direction is reasonably necessary and a proportionate response to the incident; and
- compliance with the direction is technically feasible.

A relevant entity commits an offence if it breaches the action direction and may result in imprisonment for 2 years and/or a fine of 120 penalty units or \$26,640 for individuals and 600 penalty units or \$133,200 for a body corporate.<sup>64</sup>

**3. Intervention request:** issue a request (orally or in writing) to the chief executive of the Australian Signals Directorate (ASD) to take specified action to respond to the serious cyber security incident, subject to the agreement of the Prime Minister and Defence Minister. An intervention request must not be given unless:

- an action direction would not amount to a practical and effective response to the incident;
- the specified entity is unwilling or unable to take all reasonable steps to respond to the incident;
- the request is reasonably necessary and a proportionate response to the incident; and
- compliance with the request is technically feasible.

The Explanatory Memorandum states that this is a last

resort option, within a last resort regime, and will only be used in extraordinary circumstances.

The ASD may be authorised to intervene in the following ways:

- Access to various types of data and information, such as systems logs and host images.
- Install investigation tools, such as host-based sensors or network monitoring capabilities, to analyse the extent of malicious activity and inform effective remediation actions.
- Provide ASD staff with access to premises.
- Alter/remove data in a computer.
- Implement blocking of malicious domains, disable internet access or implement other specified mitigations.
- Require systems to be patched (altering data) or a change in network configurations, to alter the function of the system, to prevent a similar activity.

A failure to comply with an intervention request by a relevant entity will result in civil penalties of 150 penalty units or \$33,300 for individuals or 750 penalty units or \$166,500 for a body corporate. It is also an offence to obstruct, hinder, intimidate or resist an ASD staff member, which may result in imprisonment for two years.<sup>65</sup>

The Ministerial authorisations (directions and intervention request) can be made in relation to the incident, the primary asset or a specified critical infrastructure sector asset<sup>66</sup> and issued to the “relevant entity” of the primary asset or a specified critical infrastructure sector asset.

## SOCI ACT EXPLAINED

A relevant entity in relation to an asset means the Responsible Entity or Direct Interest Holder or operator of the asset or a managed service provider for the asset.

This recognises that, as a result of the complex and extensive interdependencies of critical infrastructure assets, a cyber security incident can significantly compromise the functioning of an asset by targeting a crucial dependency in its supply chain, thus causing the primary asset to be inoperable. Therefore, there may be a need to undertake defensive action not just on the primary asset itself.

For example, if a critical infrastructure sector asset is used as a vector for an attack on a primary asset due to the interconnectivity of the assets' systems, then an effective response to the incident may require measures to be taken in relation to that critical infrastructure sector asset.

Further, pursuant to section 35AAA, directions made under Part 3A prevail over any obligation that a Responsible Entity for a critical infrastructure asset may have in relation to its critical infrastructure risk management program.

### Enhancing the framework for the use and disclosure of protected information

Finally, the reforms have also enhanced the protected information regime by enabling the appropriate and lawful exchange of protected information<sup>67</sup> among oversight and compliance assurance bodies.

**Firstly**, the new section 42A provides that the Secretary may make a record of or disclose protected information to an entity for the purpose of developing or assessing:

- proposed amendments to the SOCI Act,

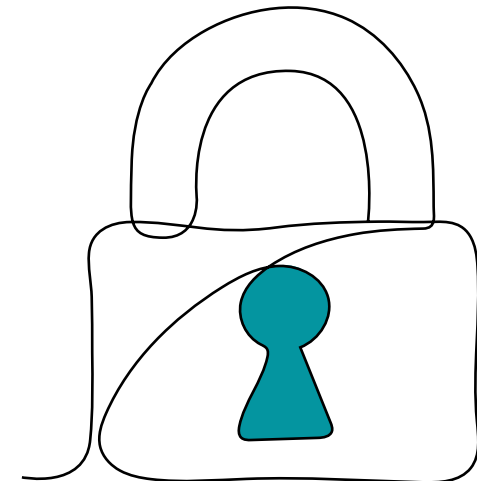
- proposed rules under the SOCI Act, or
- proposed amendments to rules under the SOCI Act.

This is to address a gap where sections 41 and 42 are both linked to the exercise of powers under the SOCI Act, and do not capture circumstances where protected information may need to be shared but for the purpose of sharing the information that is not linked to the exercise of powers under the SOCI Act, but is a related purpose.

**Secondly**, the new section 43AA provides that the Secretary may disclose protected information to an ombudsman official for the purposes of exercising powers, or performing duties or functions, as an ombudsman official, and that the Secretary may make a record of or use protected information for the purpose of that disclosure.

**Thirdly**, section 43E sets out three authorisations under which an entity can disclose protected information relating to the entity (i.e. protected information relating to itself):

1. **Disclosure to a regulator** - an entity may disclose protected information to whom the protected information relates, to a Minister (Commonwealth or state or territories), head of agency or person employed by a minister or agency, that is responsible for the regulation or oversight of a relevant critical infrastructure sector;
2. **Secretary consent in writing** - an entity may disclose protected information relating to itself if the Secretary has consented in writing to the disclosure;
3. **Protected information carve-out** - an entity may disclose protected information relating to itself if the protected information is not covered by certain categories of protected information including those relating to SoNS (which cannot be disclosed).



# CRITICAL INFRASTRUCTURE SECTORS\*

## Country comparison

	Australia <sup>68</sup>	China <sup>69**</sup>	Singapore <sup>70</sup>	EU <sup>71</sup>	US <sup>72</sup>	UK <sup>73</sup>	Canada <sup>75***</sup>
Energy	●	●	●	●	●	●	●
Transport	●	●	●	●	●	●	●
Communications	●	●	●	●	●	●	●
Financial services	●	●	●	●	●	●	
Health	●		●	●	●	●	
Water	●		●	●	●	●	
Space and research	●			●		●	
Defence	●	●			●	●	
Government		●	●		●	●	
Food and agriculture	●			●	●	●	

\* There is some overlap between the country's definitions of each category. This is a rough guide and the sub-categories of each industry assigned by the countries should also be examined.

\*\* China's list is not exhaustive. In addition to the listed industries, any other "important industries and fields" that may seriously endanger national security, the economy, people's livelihoods and public interest in the event they are damages or suffer a loss of function / outage are included.

\*\*\* Not currently law at the time of publication. Bill C-26 introduced to Parliament on 14 June 2022.

# CRITICAL INFRASTRUCTURE SECTORS\*

	Australia <sup>68</sup>	China <sup>69**</sup>	Singapore <sup>70</sup>	EU <sup>72</sup>	US <sup>72</sup>	UK <sup>73</sup>	Canada <sup>74***</sup>
Nuclear				●	●	●	●
Emergency services			●	●	●	●	
Chemicals				●	●	●	
Higher education and research	●						
Data storage and processing	●						
Media			●				
Public & legal order and safety				●			
Public services		●					
Commercial facilities					●		
Critical manufacturing					●		
Dams					●		
Banking systems							●
Clearing and settlement systems							●
Information technology					●		

\* There is some overlap between the country's definitions of each category. This is a rough guide and the sub-categories of each industry assigned by the countries should also be examined.

\*\* China's list is not exhaustive. In addition to the listed industries, any other "important industries and fields" that may seriously endanger national security, the economy, people's livelihoods and public interest in the event they are damages or suffer a loss of function / outage are included.

\*\*\* Not currently law. Bill C-26 introduced to Parliament on 14 June 2022.



# COUNTRY COMPARISON OF CRITICAL INFRASTRUCTURE LAW

## Cyber incident notification requirements

**Obligation** Reporting cyber security incidents to the relevant authority

Country	Legislation / regulation	Requirement	Penalty
Australia	SOCI Act Part 2B	Critical incidents - Initial report <b>within 12 hours</b> , final report <b>within 84 hours</b> of initial notification. Other incidents - initial report <b>within 72 hours</b> , final report <b>within 48 hours</b> of initial notification.	50 penalty units or \$11,100 for individuals or 250 penalty units or \$55,500 for a body corporate.
China	Regulations on the Security Protection of Critical Information Infrastructure Art. 18	The critical infrastructure operators are to notify and provide a report on major cybersecurity incidents or the discovery of major cybersecurity threats to the critical information infrastructure (CII) security protection work department, who shall, after reviewing the report, promptly report to the State Internet Information Department or the State Counsel public security department.	Fines between 100,000 and 1 million yuan (\$21,034AUD to \$210,336AUD), and the directly responsible managers are to be fined between 10,000 and 100,000 yuan.
Singapore	The Singapore Cybersecurity Act 2018. s. 14 Cybersecurity (Critical Information Infrastructure) Regulations 2018 r. 5	Prescribed incidents only (unauthorised hacking, malware, unauthorised interception and denial of service attacks). <b>Within 2 hours</b> after becoming aware of the occurrence, and supplementary details in writing within 14 days later.	Guilty of an offence and liable on conviction to a fine of up to \$100,000 or imprisonment for up to two years, or both.
EU	NIS2 Directive Art. 20 (Directive on security of network and information systems to repeal and replace the EU's existing cyber security directive (Directive 2016/1148) - compliance likely required in 2024)	Two-stage approach to incident reporting. Initial report by affected companies from when they first become aware of an incident <b>within 24 hours</b> and final report within 1 month. <sup>75</sup>	A minimum list of administrative sanctions whenever entities breach the rules regarding cyber security risk management or their reporting obligations laid down in the NIS Directive. These sanctions include binding instructions; an order to implement the recommendations of a security audit; an order to bring security measures into line with NIS requirements; and administrative fines (up to €10 million or 2% of the entities' total turnover worldwide, whichever is higher).



# COUNTRY COMPARISON OF CRITICAL INFRASTRUCTURE LAW

## Cyber incident notification requirements

**Obligation** Reporting cyber security incidents to the relevant authority

Country	Legislation / regulation	Requirement	Penalty
US	Cyber Incident Reporting for Critical Infrastructure Act s 2220A(d)(1)	<p>CIRCIA has two reporting requirements—one for “covered cyber security incidents,” and one for “ransom payments.”</p> <p><b>Covered cyber security incidents</b></p> <p>A covered entity that experiences a covered cyber security incident will be required to report the incident to the Department of Homeland Security (DHS) and CISA (an agency within DHS) <b>by not later than 72 hours</b> after the covered entity “reasonably believes that the covered cybersecurity incident has occurred.”</p> <p>At a minimum, a covered cyber security incident includes unauthorised access to an information system or network that leads to a loss of confidentiality, integrity or availability of the system or network; disruption of business or industrial operations by a denial of service attack, a ransomware attack or exploitation of a zero-day vulnerability; or unauthorised access or disruptions due to compromise of a cloud-service provider or supply-chain attack.</p> <p><b>Ransom payments</b></p> <p>A covered entity that makes a ransom payment as the result of a ransomware attack against the covered entity will be required to report that payment to DHS and CISA <b>not later than 24 hours</b> after making the payment.</p>	<p>If CISA has reason to believe that a company was required to notify of a covered cyber incident or ransom payment under CIRCIA but failed to do so, the agency may request additional information from that company to determine whether such an incident or payment occurred.</p> <p>If the company fails to respond to CISA’s request for information with 72 hours, CISA may issue a subpoena to compel a response.</p> <p>If the company fails to comply with the subpoena, CISA may refer the matter to the Department of Justice for civil action, potentially including contempt of court proceedings.</p>

# COUNTRY COMPARISON OF CRITICAL INFRASTRUCTURE LAW

## Cyber incident notification requirements

**Obligation** Reporting cyber security incidents to the relevant authority

Country	Legislation / regulation	Requirement	Penalty
UK	NIS Regulations 2018 r.11	Requirement to notify any incident that has a significant impact on the continuity of the essential service (a network and information systems (NIS) incident).  The notification is to be provided without undue delay and in any event <b>within 72 hours</b> after the operator is aware that a NIS incident has occurred.	There are different penalties depending on the nature of any 'material contravention'. Penalty for failure to comply with duty to notify a NIS incident is likely a fine of up to £1,000,000.
Canada	Bill C-26 ss 17, 18.	Requirement to <b>immediately</b> report a cyber security incident in respect of any of its critical cyber systems to the Communications Security Establishment and appropriate regulator.	Pursuant to section 136(1), every person who contravenes section 17 or 18 is guilty of an offence punishable on summary conviction.

## FOOTNOTES

1. [ACSC Annual Cyber Threat Report 2021](#)
2. Attorney-General's Department (AGD), [Critical Infrastructure Resilience Strategy: Policy Statement](#), (Canberra: AGD, 2015), pg 4
3. Parliament passed the SLACIP Act on 31 March 2022.
4. [Advisory report](#) on the Security Legislation Amendment (Critical Infrastructure) Bill 2020 and Statutory Review of the Security of Critical Infrastructure Act 2018
5. In this context, 'significantly' means an event or incident that puts at risk public safety and confidence, threatens our economic security, harms Australia's international competitiveness, or impedes the continuity of government and its services.
6. Attorney-General's Department (AGD), [Critical Infrastructure Resilience Strategy: Policy Statement](#), (Canberra: AGD, 2015), pg 3.
7. The [16 critical infrastructure sectors in the USA](#) are chemical, commercial facilities, communications, critical manufacturing, dams, defense industrial base, emergency services, energy, financial services, food and agriculture, government facilities, healthcare and public health, information technology, nuclear reactors, materials, and waste, transportation systems, water and wastewater systems.
8. In May 2021, CISA formed the space systems critical infrastructure working group, "a mix of government and industry members that will identify and develop strategies to minimize risks to space systems that support the nation's critical infrastructure."
9. Section 51 of the SOCI Act.
10. For the purposes of Section 9(1)(f), the *Security of Critical Infrastructure (Australian National University) Rules (LIN 22/041) 2022*, which commenced on 16 March 2022, prescribes an asset owned or operated by the Australian National University that is used in connection with the undertaking of a program of research that is critical to a critical infrastructure sector (other than the higher education and research sector), or the defence of Australia or national security, as a critical infrastructure asset.
11. Defined in Section 12L of the SOCI Act. The definition has been separated into 25 subsections representing the 22 classes of assets listed in the definition of critical infrastructure asset (subsection 9(1)), as well as assets that are prescribed under section 9(1)(f) or assets that are declared under section 51 by the Minister.
12. Defined in section 8 of the SOCI Act.
13. MSPs are entities that deliver, operate, or manage ICT services and functions for their customers via a contractual arrangement, such as a service level agreement. In addition to offering their own services, an MSP may offer services in conjunction with those of other providers. Offerings may include platform, software, and IT infrastructure services; business process and support functions; and cybersecurity services. MSPs typically manage these services and functions in their customer's network environment—either on the customer's premises or hosted in the MSP's data center. MSPs provide services that usually require both trusted network connectivity and privileged access to and from customer systems. Many organizations—ranging from large critical infrastructure organizations to small- and mid-sized businesses—use MSPs to manage ICT systems, store data, or support sensitive processes. Many organizations make use of MSPs to scale and support network environments and processes without expanding their internal staff or having to develop the capabilities internally. [Learn more.](#)
14. <https://www.jdsupra.com/legalnews/the-cyber-incident-reporting-for-6058324/>
15. UK Information Commissioner's Office - [Incident reporting](#)
16. CyberSecurity Connect - [Cyber breach notification within 6 hours mandated in India](#)
17. Statutory incident response planning obligations of SoNS.
18. Merits review is the process by which a person or body, other than the primary decision-maker, reconsiders the facts, law and policy aspects of the original decision, and determines what is the correct (made according to law) and preferable (the best decision that could have been made on the basis of the relevant facts) decision.
19. The Register is managed by the Cyber and Infrastructure Security Centre. The Register enables the Government to identify who owns and controls critical infrastructure assets, board structures, ownership rights of interest holders, and operational, outsourcing and offshoring information.
20. Section 24 of the SOCI Act.
21. Section 4(1) of the Application Rules. The 13 assets are: a critical broadcasting asset; a critical domain name system; a critical data storage or processing asset; a critical financial market infrastructure asset that is a payment system; a critical food and grocery asset; a critical hospital; a critical freight infrastructure asset; a critical freight services asset; a critical public transport asset; a critical liquid fuel asset; a critical energy market operator asset; a critical electricity asset that was not a critical infrastructure asset immediately before the commencement of section 18A of the Act; a critical gas asset that was not a critical infrastructure asset immediately before the commencement of section 18A of the Act.
22. Invicta Sugar Mill (Giru, Qld), Pioneer Sugar Mill (Brandon, Qld), Racecourse Sugar Mill (Racecourse, Mackay, Qld), South Johnstone Sugar Mill (South Johnstone, Queensland).
23. Section 12M of the SOCI Act.
24. Section 5(1) and (2) of the Application Rules - 20 asset classes.
25. See footnote 15 above. Sugar mills owned or operated by these entities may fall within the definition of 'critical electricity asset' under section 10 of the Act and the Definitions Rules. The electricity generators

## FOOTNOTES (CONT.)

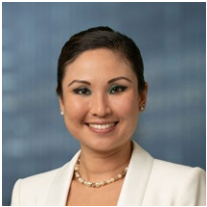
- run by The Haughton Sugar Company Pty Ltd, Pioneer Sugar Mills Pty Ltd, Mackay Sugar Ltd and MSF Sugar Pty Ltd are non-scheduled, seasonal generators, and would be unlikely to impact the electricity network in any significant way if they were unavailable so are appropriate to exclude from the definition.
26. Subsection 5(4) will exclude certain assets from the requirement to comply with Part 2B of the Act after the passage of the *Transport Security Amendment (Critical Infrastructure) Bill 2022* (the TSACI Bill). TSACI Bill would make amendments to the *Aviation Transport Security Act 2004* (ATSA) and the *Maritime Transport and Offshore Facilities Security Act 2003* (MTOFSA) to create a cyber incident reporting obligation in the legislation that is tailored and fit-for-purpose for the aviation and maritime transport sectors.
27. Section 30AC of the SOCI Act.
28. Section 30AD of the SOCI Act.
29. Section 30AE of the SOCI Act.
30. This allows the responsible entity greater discretion to determine the frequency with which this should occur, with the Explanatory Memorandum noting they are best placed to understand the context of the environment in which the asset operates.
31. Section 30AF of the SOCI Act.
32. We note a decision has been made to limit the application of the CIRMP Rules to “designated hospitals”, with a list provided at Schedule 1 of the CIRMP Rules, rather than “critical hospitals”. Designated hospitals represent a subset of critical hospitals that are considered appropriate for the application of Part 2A of the SOCI Act following consultation.
33. The Australian Government and Australia’s higher education providers have jointly formed the University Foreign Interference Taskforce (UFIT) to enhance safeguards against the risk of foreign interference. The UFIT will deliver the same outcomes as intended by the critical infrastructure risk management program obligation for critical education assets. However, should these alternative regulatory regimes be found wanting, the Government will reserve the ability to ‘switch on’ any or all of the PSOs to address any gaps and ensure that entities are subject to suitable and reasonable regulation.
34. Subsection 30AB(4) of the SOCI Act.
35. Subsection 30AB(5) of the SOCI Act.
36. Subsection 30AB(6) of the SOCI Act.
37. Section 30AQ(2) of the SOCI Act.
38. Section 30AQ(3) of the SOCI Act.
39. Section 30AH of the SOCI Act.
40. Section 8G(1) of the SOCI Act will apply—as a direct or indirect impact on the availability, integrity, reliability or confidentiality of the critical infrastructure asset.
41. What actions constitute minimising or eliminating the risk can be defined by the rules.
42. What actions constitute mitigating the relevant impact of the risk can be defined by the rules.
43. Section 30AH(7) of the SOCI Act. This adopts the commonly-known method of assessing risk as a function of likelihood and potential outcome. Hazards which are incredibly improbable, even if the potential outcome would be significant, or for which there would be an inconsequential impact, even though highly likely, are unlikely to be considered material risks.
44. The ‘approved form’ is defined in section 5 of the SOCI Act to be a form approved by the Secretary of the Department of Home Affairs. The approved form will be made publicly available on the Cyber and Infrastructure Security Centre’s website ([www.cisc.gov.au](http://www.cisc.gov.au)).
45. Where no relevant Commonwealth regulator exists, the Department of Home Affairs will be the default regulator.
46. If the entity has a board, council or other governing body, the annual report must be approved by the board, council or other governing body.
47. If a hazard had a significant relevant impact on one or more assets during the relevant period, the annual report is also required to include a statement that identifies the hazard, evaluates the effectiveness of the program in mitigating the significant relevant impact of the hazard on the assets concerned, and outline any variation to the critical infrastructure risk management program that is made as a result of the occurrence of the hazard.
48. Section 30AG(3) of the SOCI Act.
49. *Crimes Act 1914*, section 4AA and the Notice of Indexation of the Penalty Unit Amount made under that section set the current value of a penalty unit at \$222. Section 49 of the SOCI Act provides that each civil penalty provision in that Act is enforceable under Part 4 of the *Regulatory Powers (Standard Provisions) Act 2014*. Subsection 82(5) of that Act provides that the maximum penalty that may be imposed on a body corporate is five times the penalty specified for the relevant provision.
50. This penalty is commensurate with the non-compliance for an obligation on aviation and maritime industry participants to comply with reporting obligations under ATSA and MTOFSA. The penalty reflects the importance of governing bodies certifying that appropriate risk management practices are in place and that security is being considered by the most senior officers for these assets.
51. A critical worker is defined in the SOCI Act as individual, where the following conditions are satisfied:
- the individual is an employee, intern, contractor or subcontractor of the responsible entity for a critical infrastructure asset to which Part 2A applies;
  - the absence or compromise of the individual:
    - would prevent the proper function of the asset; or

## FOOTNOTES (CONT.)

- could cause significant damage to the asset;
  - as assessed by the Responsible Entity for the asset;
  - the individual has access to, or control and management of, a critical component of the asset.
52. A critical component of a critical infrastructure asset is defined to mean a part of the asset, where absence of, damage to, or compromise of, the part of the asset:
- would prevent the proper function of the asset; or
  - could cause significant damage to the asset;
- as assessed by the Responsible Entity for the asset
53. Trusted insiders can intentionally or unknowingly assist external parties to conduct malicious activities or, in the most extreme circumstances, can commit intentional acts of self-interest. The hazards that trusted insiders represent can undermine or severely impact the availability, integrity, reliability or confidentiality of critical infrastructure assets and, as a result, may undermine Australia's social or economic stability, defence and national security.
54. See also Section 34AH(4) of the SOCI Act.
55. The Minister's decision under section 52B can only be made by the Minister personally, and there is no statutory power of delegation of the Minister's powers under the SOCI Act.
56. Section 52B(2) of the SOCI Act.
57. Section 45 of the SOCI Act.
58. Section 52E of the SOCI Act.
59. Section 52F of the SOCI Act.
60. Sections 30CB(1), 30CM(1), 30CU(1), 30DB(1), 30 DJ(1) of the SOCI Act.
61. Sections 30CB(4), 30CM(3), 30CU(3), 30DB(4), 30 DJ(4) of the SOCI Act.
62. Sections 30CB(5), 30CM(5), 30CU(5), 30DD, 30DK.
63. Section 35AM of the SOCI Act.
64. Section 35AT of the SOCI Act.
65. Section 149.1 of the *Criminal Code* (which deals with obstructing and hindering Commonwealth public officials).
66. See section 8E of the SOCI act for meaning of critical infrastructure sector asset.
67. As defined in Section 5 of the SOCI Act.
68. SOCI Act.
69. Critical Information Infrastructure Security Protection Regulations (released 30 July 2021), [Article 2](#). The critical infrastructure sectors include: public communications and information services (公共通信和信息服务), energy (能源), transportation (交通), water conservancy (水利), finance (金融), public services (公共服务), e-government (电子政务), defence technology industry (国防科技工业等重要行业和领域的), and any other important network facilities and information systems that, once damaged, disabled or suffer a data disclosure, may severely threaten the national security, national economy, people's livelihood or public interest (以及其他一旦遭到破坏、丧失功能或者数据泄露,可能严重危害国家安全、国计民生、公共利益的重要网络设施、信息系统等).
70. Cybersecurity Act 2018, [Schedule 1](#). The 11 critical infrastructure sectors in Singapore are: energy, info-communications, water, healthcare, banking and finance, security and emergency services, aviation, land transport, maritime, functioning of Government and media.
71. See [Council Directive 2008/114/EC](#) of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. An indicative list of Critical Infrastructure sectors and services identified by the EU Member States are Energy, Information Communication Technologies (ICT), water, food, health, financial, public and legal order and safety, transport, chemical and nuclear industry, space and research.
72. CISA - [Critical infrastructure sectors](#). The 16 critical infrastructure sectors in the US are chemical, commercial facilities, communications, critical manufacturing, dams, defense industrial base, emergency services, energy, financial services, food and agriculture, government facilities, healthcare and public health, information technology, nuclear reactors, materials, and waste, transportation systems, water and wastewater systems.
73. CPNI - [Critical national infrastructure](#). In the UK, there are 13 national infrastructure sectors: Chemicals, Civil Nuclear, Communications, Defence, Emergency Services, Energy, Finance, Food, Government, Health, Space, Transport and Water. Several sectors have defined 'sub-sectors'; Emergency Services for example can be split into Police, Ambulance, Fire Services and Coast Guard.
74. Parliament of Canada - [BILL C-26](#). It is proposed that the Vital Services and Vital Systems are Telecommunications services, Interprovincial or international pipeline and power line systems, nuclear energy systems, transportation systems that are within the legislative authority of Parliament, banking systems, clearing and settlement systems.
75. [https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689333/EPRS\\_BRI\(2021\)689333\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689333/EPRS_BRI(2021)689333_EN.pdf)

## KEY CONTACTS

---



**Melissa Tan**  
*Partner, Head of Cyber Insurance*  
**Insurance Law and Litigation**

**D** +61 2 8020 7691  
**E** mtan@landers.com.au



**Lisa Fitzgerald**  
*Partner*  
**Corporate**

**D** +61 3 9269 9400  
**E** lfitzgerald@landers.com.au



**Robert Neely**  
*Partner*  
**Corporate**

**D** +61 2 8020 7857  
**E** rneely@landers.com.au

# ABOUT US

*Founded in 1946, Lander & Rogers is one of the few remaining truly independent Australian law firms and a leader in legal tech innovation.*

With offices across the eastern seaboard of Australia, Lander & Rogers has grown organically resulting in a unified firm with a strong focus on client and staff care.

We believe legal services involve more than just the law – practical, commercial advice and exceptional client experience are equally important to our clients and to us.

Lander & Rogers advises corporate, government, not-for-profit and private clients in insurance law and litigation, family law, workplace relations & safety, real estate, corporate transactions, digital & technology and commercial disputes.

The firm is global in approach, working closely with a network of leading firms to provide advice to clients, both domestically and abroad. Lander & Rogers is also the exclusive Australian member of the largest worldwide network of independent law firms, TerraLex.

## Melbourne

Level 15 Olderfleet  
477 Collins St  
Melbourne VIC 3000

**T** +61 3 9269 9000  
**F** +61 3 9269 9001

## Sydney

Level 19 Angel Place  
123 Pitt St  
Sydney NSW 2000

**T** +61 2 8020 7700  
**F** +61 2 8020 7701

## Brisbane

Level 11 Waterfront Place  
1 Eagle Street  
Brisbane QLD 4000

**T** +61 7 3456 5000  
**F** +61 7 3456 5001



[landerson.com.au](https://www.landerson.com.au)