Security of Critical Infrastructure Act 2018

General Guidance for Critical Infrastructure Assets

What is the *Security of Critical Infrastructure Act?*

The Australian Government is committed to working with industry to protect the essential services all Australians rely on by uplifting the security and resilience of our critical infrastructure. Threats ranging from natural hazards (including weather events) to human induced threats (including interference, cyber attacks, espionage, chemical or oil spills, and trusted insiders) all have the potential to significantly disrupt critical infrastructure.

The *Security of Critical Infrastructure Act 2018* (SOCI Act) was amended in 2021 and 2022 to more appropriately capture those assets that are critical to Australia's defence, national security, economy and social stability. The amendments also responded to the deteriorating threat environment related to cyber attacks.

The SOCI Act was further amended in 2024 by the *Security of Critical Infrastructure and Other Legislation Amendment (Enhanced Response and Prevention) Act 2024* (ERP Act) in response to significant incidents impacting critical infrastructure to uplift existing obligations for captured entities and enhance the government's ability to industry manage the consequences of all hazards incidents on critical infrastructure assets. The ERP Act also harmonises Australian telecommunications security regulation.

The SOCI Act is designed to manage risks to critical infrastructure assets by:

- ensuring owners and operators of critical infrastructure assets are taking appropriate steps to secure their assets
- ensuring the Government has the information required to manage national security risks and appropriate and proportionate powers to respond to risks.

Details on which obligations apply to different asset classes is available on the next page.

What are the obligations for responsible entities under the SOCI Act?

1. ***SOCI Act Subsection 12(F):*** Obligation to notify data service providers – Entities must notify external data service providers if they are storing or processing business critical data. This ensures that companies that are handling sensitive data for critical infrastructure assets are aware that they may themselves also have obligations under the Act and that they treat the security of the data appropriate.

2. ***SOCI Act Part 2:*** Register of Critical Infrastructure Assets – Entities must register certain information related to critical infrastructure assets with the Cyber and Infrastructure Security Centre. Registration provides the Centre with a comprehensive understanding of the ownership and operational arrangements of critical infrastructure across the Australian economy. This helps the Government to better identify and respond to security risks.

3. ***SOCI Act Part 2A***: Risk Management Program – Entities must have and comply with a Risk Management Program for their critical infrastructure assets. This will ensure responsible entities have a comprehensive understanding of the threat environment, and develop processes and procedures to effectively respond to the material risk of any hazard impacting their asset. This includes submitting an Annual Report 90 days after the end of the financial year.

4. ***SOCI Act Part 2B:*** Mandatory Cyber Incident Reporting – Entities must report cyber security incidents that have a significant or relevant impact on their asset. This information will support Government to develop an aggregated threat picture to inform both proactive and reactive cyber response options – from providing immediate assistance to working with industry to uplift broader security standards.

5. ***SOCI Act Part 2C***: Enhanced Cyber Security Obligations (ECSO) – The Minister for Home Affairs, after consultation with the responsible entity and others, may declare an asset to be a 'System of National Significance'. These assets are those that are most crucial to the nation, by virtue of their interdependencies across sectors and consequences of cascading disruption to other critical infrastructure assets and sectors. If declared to be a system of national significance, the responsible entity may be notified that they are subject to four additional obligations focused on cyber preparedness and resilience.

6. **SOCI Act Part 2D:** Enhanced security regulation for critical telecommunications assets
Entities responsible for a critical telecommunications asset must protect their asset from all hazards, including security risks and notify the Department of certain changes which may have a material effect on their ability to meet this requirement..

Contact Us | 1300 27 25 24 | enquiries@CISC.gov.au | CISC.gov.au
| CISC on Twitter | LinkedIn | Instagram

Australian Government
Department of Home Affairs
CYBER AND INFRASTRUCTURE SECURITY CENTRE

April 2025

The obligations apply differently to each asset class. Which obligations do you need to comply with?

Sector	Asset class	Obligation to notify data service providers (Subsection 12F(3))	Register of Critical Infrastructure Assets (Part 2)	Notification of cyber security incidents (Part 2B)	Critical Infrastructure Risk Management Programs (Part 2A)[3]	**Notification obligation and obligation to protect asset (Part 2D)**	Enhanced cyber security obligations (ECSO) (Part 2C)
Energy	Critical electricity assets	✓	✓	✓	✓		
	Critical gas assets	✓	✓	✓	✓		
	Critical energy market operator assets	✓	✓	✓	✓		
	Critical liquid fuel assets	✓	✓	✓	✓		
Communications	Critical telecommunications assets	✓	✓[3]	✓[3]	✓	✓[3]	
	Critical broadcasting assets	✓	✓	✓	✓		
	Critical domain name system assets	✓	✓	✓	✓		
Data Storage & Processing	Critical data storage or processing assets	✓	✓	✓	✓		
Financial services & markets	Critical banking assets	✓		✓			
	Critical superannuation assets	✓		✓			
	Critical insurance assets	✓		✓			
	Critical financial market infrastructure assets	✓	✓[1]	✓	✓[1]		
Water & sewerage	Critical water assets	✓	✓	✓	✓		
Healthcare & medical	Designated hospital	✓	✓	✓	✓		
	Critical hospital assets	✓	✓	✓			
Higher education & research	Critical education assets	✓		✓			
Food & grocery	Critical food and grocery assets	✓	✓	✓	✓		
Transport	Critical ports	✓	✓	✓			
	Critical freight infrastructure assets	✓	✓	✓	✓		
	Critical freight services assets	✓	✓	✓	✓		
	Critical public transport assets	✓	✓	✓			
	Critical aviation assets	✓		✓[2]			
Space technology	**Note**: No assets currently defined						
Defence industry	Critical defence assets	✓					

ECSO only applies to assets declared systems of national significance

[1] That is a payment system

[2] certain aviation assets. See application rules carrier assets and certain carriage service provider assets only

Contact Us | 1300 27 25 24 | enquiries@CISC.gov.au | CISC.gov.au | CISC on Twitter | LinkedIn | Instagram

Australian Government
Department of Home Affairs

CYBER AND INFRASTRUCTURE SECURITY CENTRE

April 2025

How do I comply with the obligations?

1

Obligation to notify data service providers (Subsection 12F(3))

A **responsible entity** for a critical infrastructure asset that has **business critical data** processed or stored by a third party on a commercial basis must, as soon as **reasonably practicable**, take **reasonable steps** to inform the third party that they are processing or storing business critical data of a critical infrastructure asset.

2

Mandatory Reporting of Cyber Security Incidents (Part 2B)

If a cyber security incident has a relevant or significant impact on a critical infrastructure asset subject to this obligation, the **responsible entity** for the asset must notify the Australian Cyber Security Centre (ACSC) (at Report a Cyber Security Incident or via 1300 CYBER1). Incidents which have a significant impact must be reported within 12 hours of the entity becoming aware of the incident, or within 72 hours of becoming aware of an incident having a relevant impact.

For more information on this obligation see Mandatory Cyber Incident Reporting.

3

Reporting to the Register of Critical Infrastructure Assets (Part 2)

Reporting entities (**Responsible Entities and Direct Interest Holders**) for critical infrastructure assets covered by this obligation must provide certain information to the Centre:

- **Responsible entities** must supply operational information.
- **Direct interest holders** must supply interest and control information.

The Reporting entity must update the Centre within 30 days if information relating to the asset changes. Registrations and changes can be done through Resources - Online Forms.

For more information on this obligation, see Register of Critical Infrastructure Asset Guidance.

4

Maintaining a Critical Infrastructure Risk Management Program (Part 2A)

Responsible entities for critical infrastructure assets must have and comply with a Risk Management Program which supports the entity to identify, and as far as is reasonably practicable, minimise or eliminate material risks that could impact the asset. These risks could come from any hazard, including cyber, personnel, natural disasters and supply chains. Responsible entities must also provide an annual report to the Centre in the approved format attesting that the obligation is being met.

Risk Management Programs found to be seriously deficient may face Ministerial directions to remedy these deficiencies (see section 30AI(1) of the SOCI Act for more information).

For more information on this obligation, see Guidance for the Critical Infrastructure Risk Management Program and and Guidance for the Telecommunications Security and Risk Management Program.

5

Dependent on declaration

Enhanced cyber security obligations (Part 2C)

The Minister for Home Affairs may notify the responsible entity for a critical infrastructure asset that the asset has been declared a System of National Significance. If this has occurred, you may be notified by the Secretary of the Department of Home Affairs (or a delegate) that you are required to do one or more of the following:

- Create an incident response plan in preparation for a cyber security incident
- Undertake cyber security exercises to build cyber preparedness
- Undertake vulnerability assessments to identify areas for remediation
- Provide, or install software to facilitate the provision of, system information to the Australian Signals Directorate.

For more information on this obligation, see The Enhanced Cyber Security Obligations Framework.

Contact Us | 1300 27 25 24 | enquiries@CISC.gov.au | CISC.gov.au | CISC on Twitter | LinkedIn | Instagram

Australian Government
Department of Home Affairs

CYBER AND INFRASTRUCTURE SECURITY CENTRE

April 2025

How have my obligations changed under the ERP Act reforms?

Mandatory from:

5 April 2025

1

Obligation to protect business critical data and secondary data storage systems

Entities must protect certain data storage systems that hold business critical data as part of a critical infrastructure asset, regardless of the asset's primary function. Impacts to these systems must be reported under cyber incident reporting and Register of Critical Infrastructure Assets obligations, and be considered in risk management programs. These amendments are enacted by the Security of Critical Infrastructure Amendment (Measures No. 1) Rules 2025.

Implement a harms based approach to protected information provisions

Critical infrastructure entities and government may now make a harms based assessment to inform the use and disclosure of information, including through reference to the non exhaustive list of 'relevant information'. These amendments also clarify entities may make a record of, use or disclose protected information where the purpose relates to the continued operation of an asset or to mitigate risks to that asset.

For more information on this obligation, see the Guidance for Protected Information.

2

Simplifying Notification of declaration of systems of national significance

The Minister for Home Affairs is no longer required to notify each direct interest holder of a SoNS declaration and is only required to notify the responsible entity to be notified within 30 days.

Responsible entities for a SoNS are no longer required to notify the Secretary of Home Affairs of changes to direct interest holders. The responsible entity will still be required to notify the Secretary of changes to the responsible entity.

For more information on this obligation, see The Enhanced Cyber Security Obligations Framework.

3

With effect from 5 April 2025

Security regulation for critical telecommunications assets

Telecommunications security obligations under Part 14 of the *Telecommunications Act 1997* has moved to the SOCI Act.

Mandatory cyber incident reporting and the obligation to provide information to the Register of Critical Infrastructure Assets are now under the SOCI Act, and equivalent obligations under the *Telecommunications Act 1997* switched off. The obligation for carriers to protect their assets and notify of changes to their network has been uplifted and harmonised into the SOCI Act.

A subset of critical telecommunications assets are required to maintain and comply with a bespoke critical infrastructure risk management program, which is applied through the Telecommunications Security and Risk Management Program (TSRMP) Rules 2025.

For more information on this obligation and important compliance dates for critical telecommunication assets, please see the Telecommunications Guidance.

Contact Us | 1300 27 25 24 | enquiries@CISC.gov.au | CISC.gov.au | CISC on Twitter | LinkedIn | Instagram

Australian Government Department of Home Affairs | CYBER AND INFRASTRUCTURE SECURITY CENTRE

April 2025

What powers exist under the *SOCI Act* ?

For all sectors

Currently in force

1 Ministerial Directions (Part 3)

The Minister for Home Affairs may **require a reporting entity** for, or an **operator** of, a critical infrastructure asset to do, or refrain from doing, an act or thing, if the Minister is satisfied that there is a risk of an act or omission that would be prejudicial to security.

2 Government assistance to respond to serious cyber security incidents (Part 3A)

These powers of last resort provide the Government with the ability to take action to support critical infrastructure entities in response to a significant incident impacting critical infrastructure and the cascading consequences that it may cause.

Amendments to the SOCI Act no longer require the incident to be of a cyber related cause, allowing the Minister to authorise action, or information gathering directions, for all-hazard incidents such as climate disasters or sabotage. The legislative requirements relating to intervention requests remain unchanged and can only be used in the event of a cyber security incident.

3 Information gathering powers (Part 4)

The Secretary of the Department of Home Affairs, or a delegate, may require a **reporting entity** for, or an **operator** of, a critical infrastructure asset to provide certain information or documents.

4 New powers to direct an entity to vary critical infrastructure risk management programs

The ERP Act amended the SOCI Act to give the regulator powers to issue a formal written direction to a responsible entity to vary their critical infrastructure risk management program where the program contains a serious deficiency that poses a material risk to Australia's national security, defence or socio-economic stability.

The use of such regulatory powers will be used as a absolute last resort. The government continues to prioritise working collaboratively with industry to address concerns before enforcing regulatory action.

5 Ministerial directions for critical telecommunications assets (Part 2D)

Section 30EF of the SOCI Act allows the Minister to direct an entity to do or not do a thing that is prejudicial to security. This power is an absolute last-resort power typically reserved for suspected espionage, sabotage or foreign interference.

The Minister may provide direction to a responsible entity for a critical telecommunications asset if the entity uses for themselves, or supplies, a carriage service, and that use or supply could be prejudicial to security. Such a direction can only be issued if an adverse security assessment in respect of the carrier or carriage service provider has been given to the Minister.

Further information is available in the telecommunications guidance.

Contact Us | 1300 27 25 24 | enquiries@CISC.gov.au | CISC.gov.au | CISC on Twitter | LinkedIn | Instagram

Australian Government
Department of Home Affairs

CYBER AND INFRASTRUCTURE SECURITY CENTRE

April 2025

Where can I find out more?

More information on the protection of Australia's critical infrastructure can be found on the Cyber and Infrastructure Security Centre's website.

The key **legislative instruments** can be found here:

— Security of Critical Infrastructure Act 2018

— Security of Critical Infrastructure (Application) Rules

— Security of Critical Infrastructure (Definitions) Rules

- Security of Critical Infrastructure (Telecommunications Security and Risk Management Program) Rules 2025

For more information on each of the **obligations** see the following fact sheets:

— CISC Guide - Mandatory Cyber Incident Reporting

— CISC Factsheet - Register of Critical Infrastructure Assets

— CISC Fact Sheet – Risk Management Program ; SOCI (CIRMP) Rules

— CISC Factsheet – Cyber Incident Response Government Assistance Measures

— CISC Factsheet - Systems of National Significance and Enhanced Cyber Security Obligations

— CISC Factsheet - Use and Disclosure of Protected Information

For more information on the **definitions** of critical infrastructure assets, see What the Changes Mean for Me.

Contact Us | 1300 27 25 24 | enquiries@CISC.gov.au | CISC.gov.au | CISC on Twitter | LinkedIn | Instagram

Australian Government
Department of Home Affairs
CYBER AND INFRASTRUCTURE SECURITY CENTRE

April 2025