Demystifying Australia's recent Security of Critical Infrastructure Act reforms

Recent amendments to the *Security of Critical Infrastructure Act 2018* ("the **Act**'") constitute some of the most significant cybersecurity reforms in Australia's history. In many respects, Australia is leading the way globally in this area of reform, amongst an increasingly complex cybersecurity regulatory ecosystem. This high-level summary provides a simple overview to help demystify the new regime's complexities.

Key takeaways

1. The *Security of Critical Infrastructure Act 2018* reforms are now in force, after its two tranches were passed in December 2021 and March 2022. These reforms are arguably the most ambitious and significant security reforms in Australian legislative history.
2. While Government assistance, intervention and direction obligations have been in force since December 2021, positive security obligations are being progressively switched on and enhanced security obligations are now in force.
3. Despite the apparent simplicity of the regime, assessing applicability remains complex. The legislation covers a broad range of assets and a broad range of roles relating to those assets.
4. Many Australian corporates are now grappling with multiple regulatory regimes and regulators, in addition to the critical infrastructure reforms.
5. This summary provides a high-level overview of the recent reforms. We look to simplify the regime, acknowledging that complexity exists below the surface and will invariably require a case-by-case assessment.

The reforms explained...

Following an extensive engagement and consultation process, and a decision to pass the reforms in two tranches, the *Security Legislation Amendment (Critical Infrastructure) Act 2021* (Cth) came into force on 3 December 2021, followed by the *Security Legislation Amendment (Critical Infrastructure Protection) Act 2022* (Cth) on 1 April 2022.

The reforms materially expand the scope of the Act, which now covers 11 "critical infrastructure sectors"[1] and 22 categories of "critical infrastructure assets".

Last resort broad Government information gathering, direction and intervention powers apply in respect of 11 "critical infrastructure sectors" (subject to various checks and balances described below). Reporting and other positive security obligations, apply, or will apply (when implementing regulations come into force) in relation to certain "critical infrastructure assets", and "enhanced cyber security obligations" now apply to designated "systems of national significance".

Obligations extend to various participants in the supply chain including "responsible entities", "reporting entities", "direct interest holders", "managed service providers" and "operators".

Below we explain key obligations and powers, and the impacted entities, sectors and assets.

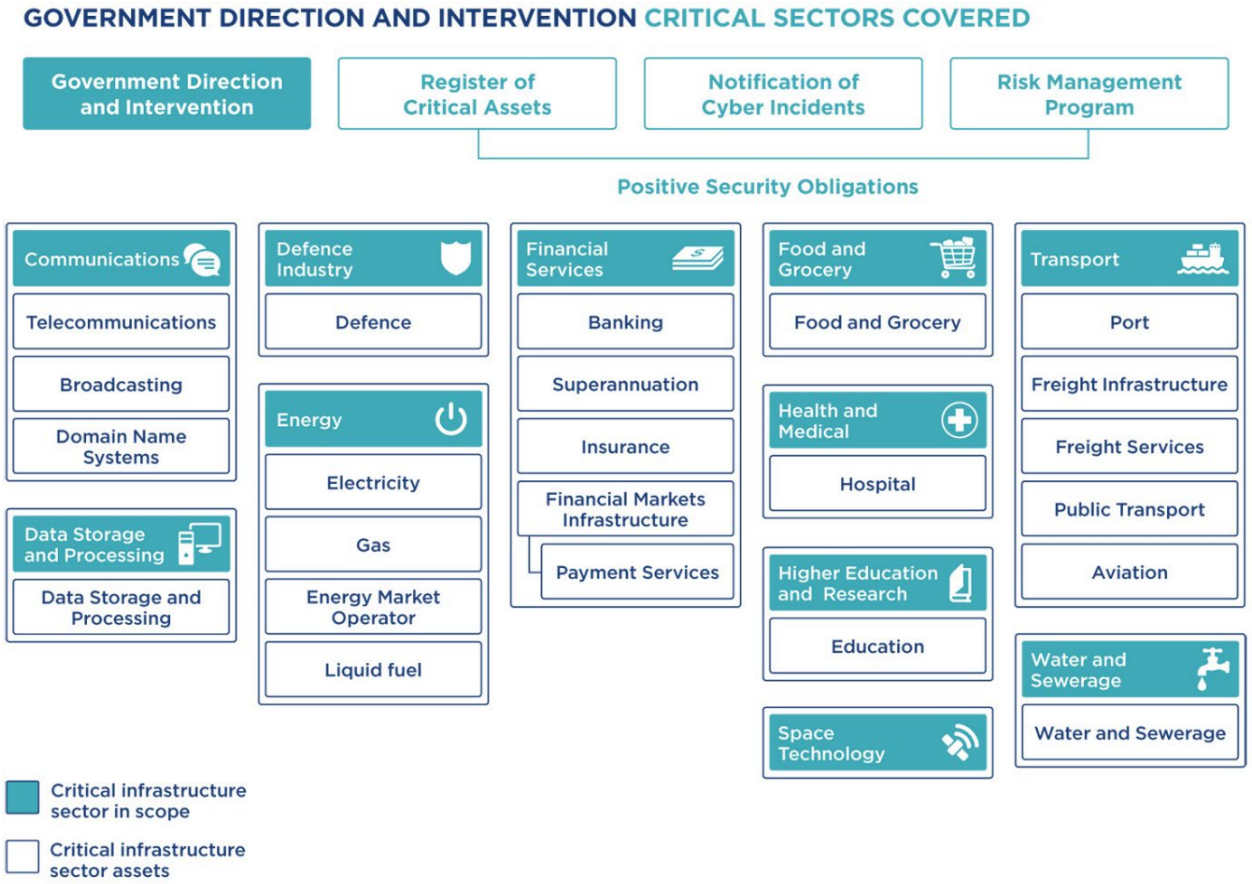
[1] Terms in quote in this briefing are defined term under the SoCI Act.

Entities – Who is captured by the reforms?

Entity	Definition	Key obligations
Responsible Entity	Definitions is asset specific, but generally the responsible entity will be the entity that owns, or is licensed or responsible for operating, the asset.	Reporting of operational information. Notification of cyber incidents. Risk management plans.
Direct Interest Holder	Entity that (a) together with any associates of the entity, holds a legal or equitable interest of at least 10% in a critical infrastructure asset (including if any of the interests are held jointly with one or more other entities); or (b) holds an interest in the asset that puts the entity in a position to directly or indirectly influence or control the asset.	Reporting of interest information.
Reporting Entity	Responsible Entity. Direct Interest Holder	Reporting of interest and operational information.
Relevant Entity	Responsible Entity. Direct Interest Holder. Operator (entity that operates the critical infrastructure asset or part of the asset). Managed service provider (entity that manages (part of) a critical infrastructure sector asset, aspect of the asset, or the operation of the asset).	Response to Government information gathering, direction and intervention powers.

Government information gathering, direction and intervention powers (*in effect since 3 December 2021*)

Triggering Cyber Security Event	Powers and Safeguards
When • A cyber security incident has occurred, is occurring or is imminent, AND • That incident has or is likely to have a "relevant impact"* on a "critical infrastructure asset" AND; • There is a material risk to social / economic stability, defence or national security of Australia. *What constitutes a "relevant impact" varies, but in relation to a cyber security incident it includes direct or indirect impacts on the availability, integrity or reliability of the asset; or the confidentiality of information about or stored on the asset.	Minister may authorise the Secretary to issue to a relevant entity for the impacted asset or another specified "critical infrastructure sector asset" *: 1. Information gathering directions in relation to the incident and/or impact, *where this is likely to facilitate a practical and effective response to the incident.* 2. Specific action directions in response to the incident, *where (a) the relevant entity the specified entity is unwilling or unable to take all reasonable steps to resolve the incident; (b) the direction is reasonably necessary for the purposes of responding to the incident; (c) the direction is a proportionate response to the incident; and (d) compliance with the direction is technically feasible.* 3. Intervention requests, authorising the Australian Signal Directorate ("ASD") to step in to respond to an incident, *where an action direction would not constitute a practical and effective response to the incident and be satisfied that the same criteria required for an action direction are met.* Step in powers may include (i) accessing, modifying or analysing computer systems or data; (ii) installing computer programs; and (iii) removing, disconnecting, connecting or adding computers or computer devices. "Critical infrastructure sector" assets include "critical infrastructure asset" and any other asset that "relates to" a "critical infrastructure sector". For example, this could capture IT systems or other equipment supplied to support or service "critical infrastructure assets".



Positive security obligations

There are three positive security obligations set out under the Act (only the first two listed below have been switched on at this time):

- the provision of "operational" and ownership information to the Register of Critical Infrastructure Assets;
- the notification of actual or imminent cyber security incidents with an actual or likely relevant impact; and
- implementing and complying with a "risk management program".

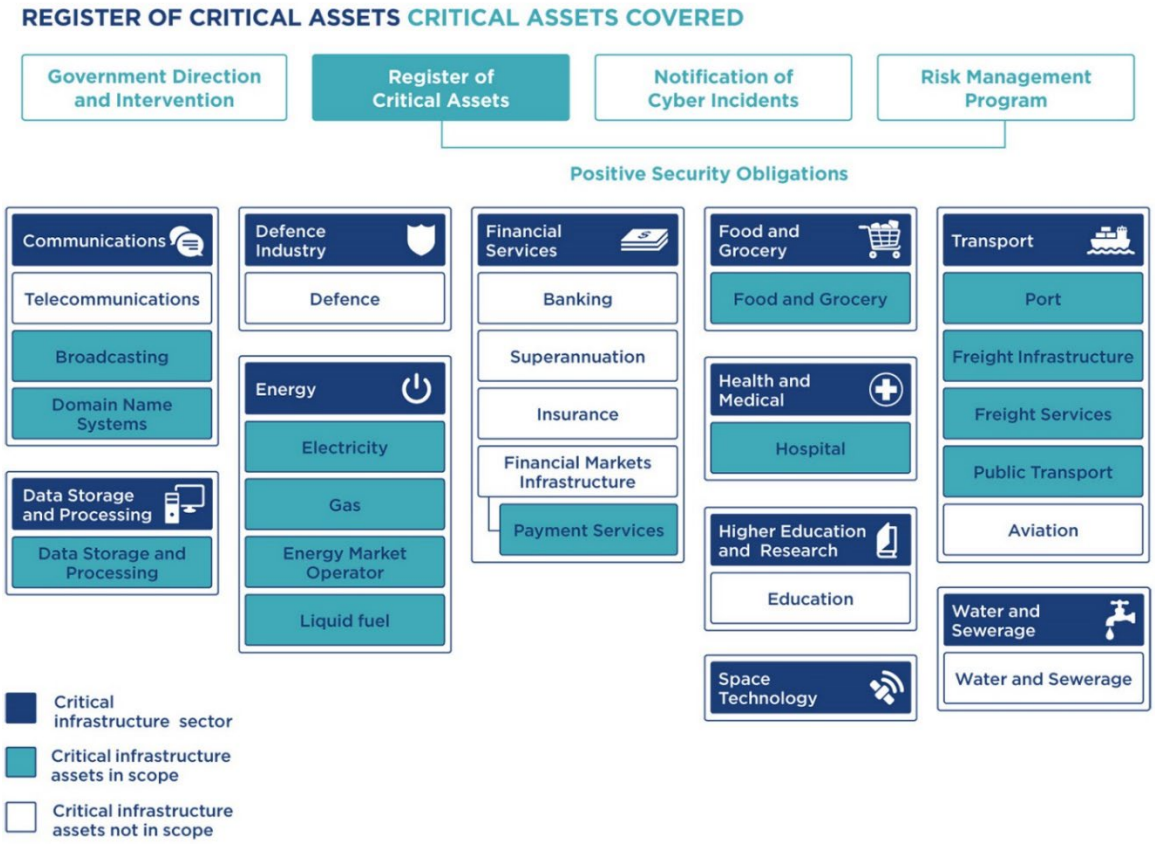
Importantly, these obligations only apply to a "critical infrastructure asset" if the obligation has been switched on (as illustrated in the below infographics). The Government will only switch on the obligations where it considers that sufficient existing alternative regulatory or administrative arrangements are not already in place.[2]

Register of Critical Assets (now switched on – in effect from 8 October 2022)

The Cyber Infrastructure Security Centre ("CISC") maintains a confidential Register of Critical Infrastructure Assets.

A "responsible entity" for, or a "direct interest holder" in an applicable "critical infrastructure asset" (each a "reporting entity") must provide the CISC certain "operational" and "interest and control" information. This includes "operational" information about the asset, "interest and control" information about the entity and the asset, and contractual arrangements for operating the asset's core functionalities or maintaining "business-critical data". "Business-critical data" is defined to include (i) personal information about more than 20,000 individuals or is sensitive information; (ii) information relating to any research and development in relation to, systems needed to operate, risk management and business continuity in relation to, a critical asset.

"Reporting entities" not already captured under the previous legislation must comply with these obligations from 8 October 2022 (or 6 months after the asset becomes a "critical infrastructure asset").



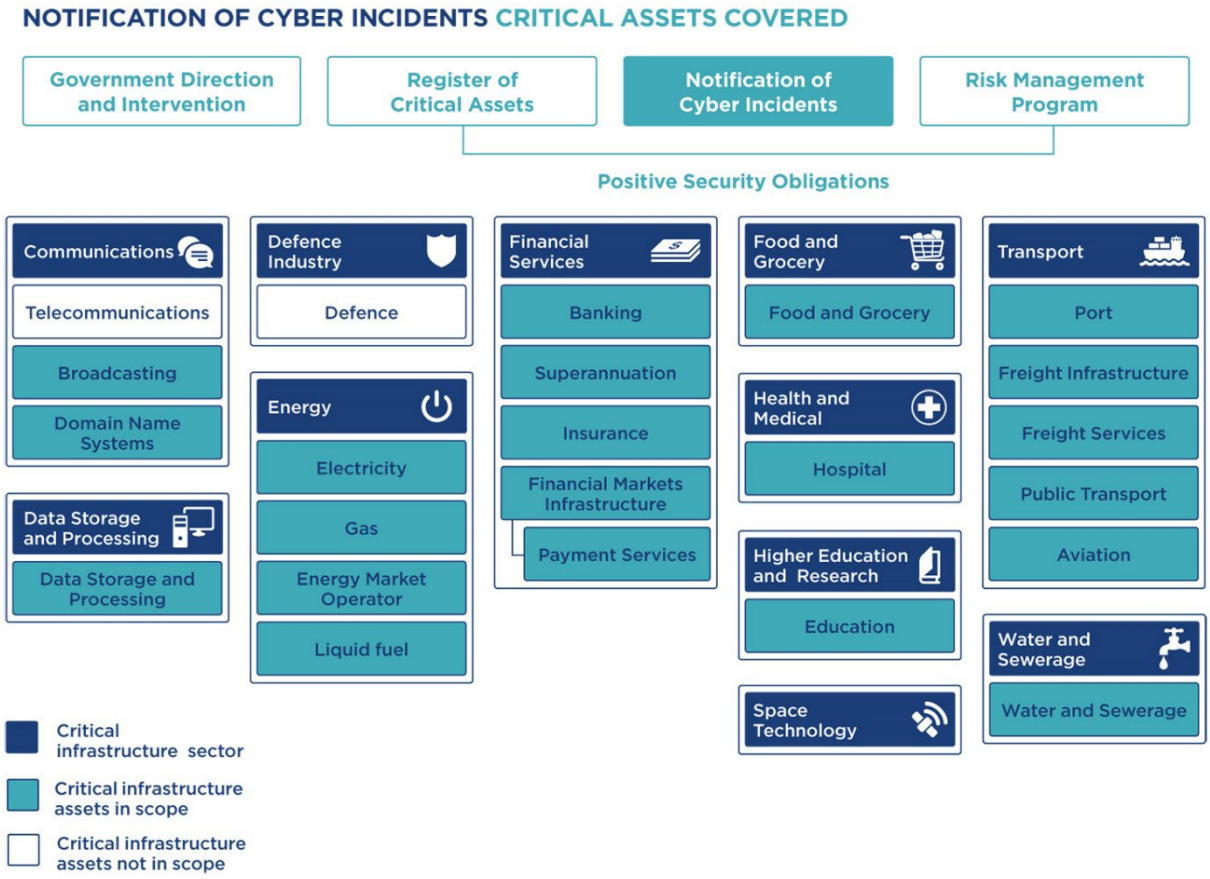
[2] For example, telecommunication carriers and carriage service providers are already subject to certain security requirements under the Telecommunication Act, and the Department of Communication recently introduced specific telecommunication rules that would impose equivalent reporting obligations on those providers to that imposed on other sectors under the Act.

Notification of cyber security incidents (now switched on – in effect from 8 July 2022)

A "responsible entity" for an applicable "critical infrastructure asset" must report actual or imminent cyber security incidents to the ASD.

If the incident has a "relevant impact" (i.e. directly or indirectly impacts the asset's availability, integrity or reliability, or the confidentiality of information about or stored on the asset) reporting must occur within 72 hours of the entity becoming aware. This timeframe is reduced to 12 hours if the incident has had, or is having, a "significant impact" on the availability of the asset (i.e. is materially disrupts the provision or availability of essential goods or services). These obligations apply from 8 July 2022 (or 3 months after an asset becomes a "regulated asset"). Cyber security incidents can be reported over the phone if a written report is also provided.

"Responsible entities" must comply with these obligations from 3 months after the asset becomes a "critical infrastructure asset".



"Risk management programs" (yet to be switched on, with further consultation imminent)

A "responsible entity" for an applicable "critical infrastructure asset" must adopt, maintain and comply with a "risk management program" (with annual Board approved reporting).

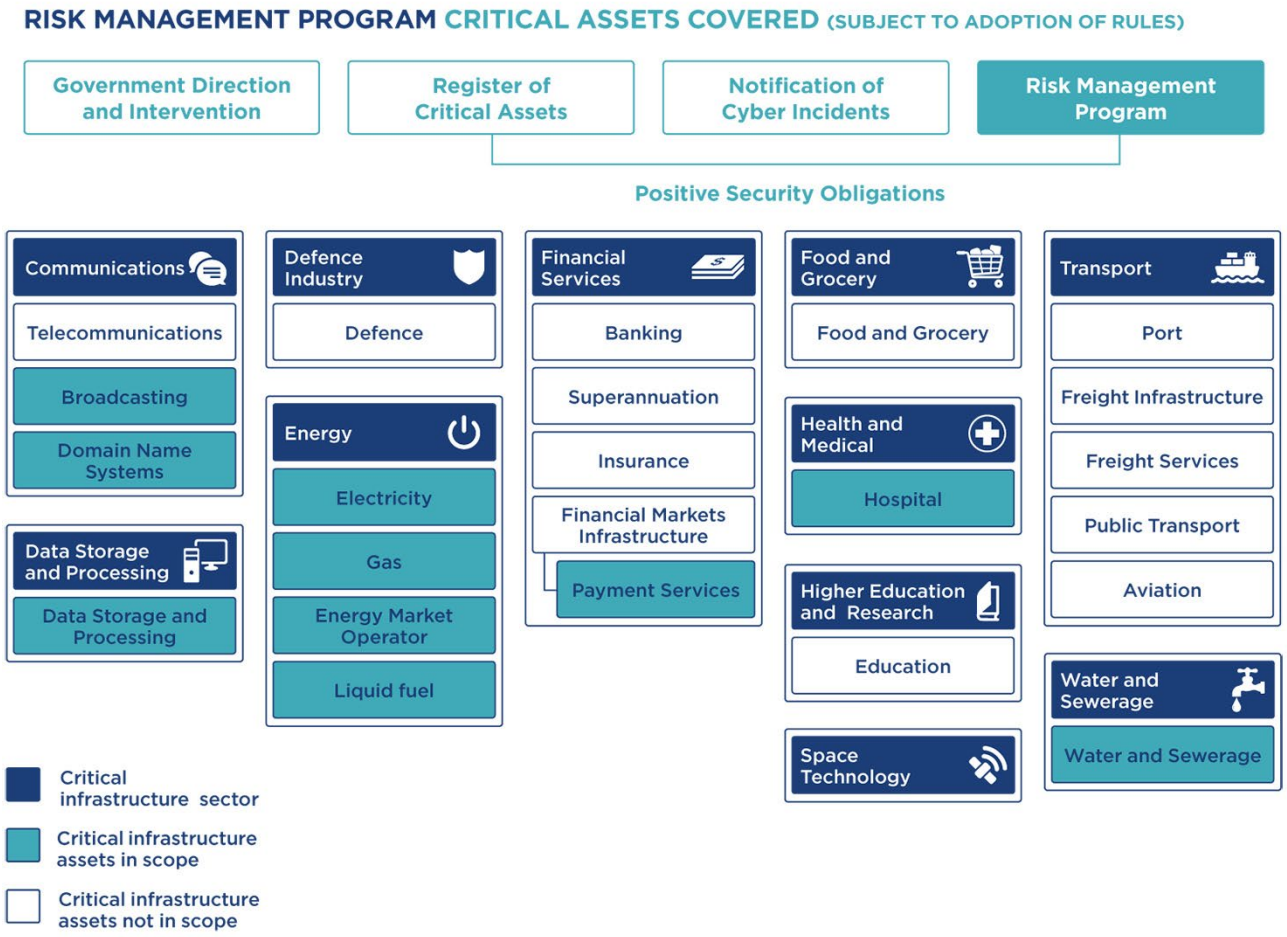
A "risk management program" is a written program, adopting an "all-hazards" approach to the asset, that:

- identifies each hazard where there as a material risk of a "relevant impact"; and
- minimises, mitigates or eliminates any material risk from the hazard (to the extent reasonably practicable).

Consultation in relation to the "risk management program" is ongoing and the rules will confirm the relevant "critical infrastructure assets" and the principles-based processes.

The “all-hazards” approach requires consideration of both natural and man-made hazards, including cyber and information security, personnel, supply chain, physical security and natural hazards.

Data storage or processing providers that hold a certificate of hosting certification (at a strategic level), under the Hosting Certification Framework of the Australian Government Digital Transformation Agency,[3] are exempt from the “risk management program” obligations.[4]



“Enhanced cyber security obligations”

After following a notification and consultation process, the Government may declare a particular asset to be a “system of national significance”.

A “responsible entity” for a “system of national significance” may be required to comply with one or more “enhanced cyber security obligations”, including:

- incident response planning – adopting, maintaining and complying with an incident response plan for its assets;
- cyber security exercises – conducting cyber security exercises testing the entity’s ability and preparedness to respond to and mitigate cyber incidents, including reporting relating to the exercise (and in some circumstances, external audits);
- vulnerability assessments – undertaking a vulnerability assessment in respect of the relevant asset; and/or

[3] Current list of certified service providers is available here.
[4] However, they must, within 90 days after the end of each financial year, report on their assets and any hazards that had a significant relevant impact on one or more of those assets during the relevant period.

- system information – providing the ASD with periodic or event-based reports and / or installing software to transmit system information directly to the ASD.

These obligations apply from the date set by the declaration and may apply to any “critical infrastructure asset”.