protiviti®
Global Business Consulting

Australia's Critical Infrastructure Act Reforms — A Positive Step in Strengthening Industry-wide Resilience

The existing Security of Critical Infrastructure Act 2018 (SOCI Act), which requires owners and operators to take steps to safeguard defined critical infrastructure assets, has recently been amended to broaden the scope of industry sectors. This has been achieved through a combination of:

- *The Security Legislation Amendment (Critical Infrastructure) Act 2021 (Cth)* (the SLACI Act 2021), which received Royal Assent on 2 December 2021. The SLACI Act 2021 amends the SOCI Act; and was the first of a two-part Bill to become law. The Act now applies to a broad range of industry sectors and introduces significant additional security and risk management requirements for managing evolving risks to Australia's critical infrastructure assets.
- *The Security Legislation Amendment (Critical Infrastructure Protection) Act 2022 (Cth)* (the SLACIP Act 2022) received Royal Assent on 2 April 2022. Together with the amendments contained in the SLACI Act 2021, this completes the legislative reforms in this space.

Taken together, these two legislative reforms form the Commonwealth framework for critical infrastructure protection, as well as legislated last resort powers in the event of a catastrophic cyber security incident. By splitting this legislation into two parts, both of which have now become law, it allowed the urgent reforms to be implemented — first by industry sectors while providing the government with additional time to consult with the industry on the remaining elements of the proposed reform (now also legislated).

This paper presents a brief history of the legislation, its new requirements, what the legislation may mean for Australian entities across different industry sectors, and most importantly, next steps for affected Australian entities.

History: the Security of Critical Infrastructure Act 2018 (SOCI Act)

The SOCI Act was introduced in 2018 as part of Australia's Cyber Security Strategy. It brought an enhanced focus on the security of critical infrastructure within the electricity, gas, water and port sectors. Owners and operators of defined critical infrastructure assets within these sectors are required to take steps to protect that infrastructure, including registering ownership and operational information on the 'Register of Critical Infrastructure Assets[1]'. It also gives the Secretary of the Department of Home Affairs and the Minister for Home Affairs powers to seek information from owners and operators in certain circumstances, and the ability to direct an owner or operator to take action, or not take action in certain circumstances.

New requirements: what is in the SLACI Act?

The SLACI Act 2021 significantly enhances the existing framework for managing risks relating to critical infrastructure assets by introducing additional security obligations. Key updates include:

1. The introduction of seven new critical infrastructure sectors from the original four sectors (now 11 in total);
2. Redefining the scope of critical infrastructure assets to 22 different classes;
3. An obligation to provide ownership and operational information to the Cyber and Infrastructure Security Centre (an obligation that the Minister of Home Affairs can choose to enact as and when required);
4. Enforcing mandatory cyber incident reporting to the Australian Cyber Security Centre relating to critical infrastructure assets across the 22 different classes (an obligation that the Minister of Home Affairs can choose to enact as and when required); and
5. Creating "Government Assistance Measures" for owners and operators of critical infrastructure assets which can provide directions and interventions for the Department of Home Affairs to respond to a significant cyber incident if certain criteria have been met and strict authorisations have been obtained.

The table included in the **Appendix** provides more detail on each of the changes, including a list of all critical infrastructure sectors and 22 critical infrastructure assets.

The future: additional requirements through the SLACIP Act 2022

The SLACIP Act 2022 provides further amendments, including to enact a framework for a **risk management program, declaration of systems of national significance** and **enhanced cyber security obligations.**

From 15 December 2021 through to 1 February 2022, the Department of Home Affairs welcomed 70 submissions and engaged 1,300 industry stakeholders which canvassed potential areas for further amendment to the SLACIP Bill. On 16 March 2022, the Parliamentary Joint Committee on Intelligence and Security commenced reviews into the SLACIP Bill and the operation, effectiveness and implications of the SOCI Act. It received Royal Assent and came into effect on 2 April 2022.

Risk management program

The risk management program rules will apply to critical infrastructure sectors that do not have an existing regulatory system in place and will require critical infrastructure asset owners and operations to develop a risk management program. The risk management program is designed to:

- **Identify material risks** — including hazards that could have a relevant impact on assets;
- **Minimise risks** — minimise or eliminate (if reasonably practical) any material risk of such hazard;
- **Mitigate impact of realised incidents** — by having procedures in place to mitigate impacts in the event of the hazard occurring (through contingency strategies); and
- **Safeguard effective governance** — as with any risk management program, owners and operators of critical infrastructure assets will be required to have appropriate risk management oversight arrangements in place (including evaluation, testing, and maintenance).

[1] A critical infrastructure asset is a system or network that is essential to the functioning of the Australian economy, society and/or national security

Declaration of systems of national significance

The SLACIP Act 2022 proposes that the Minister may declare a critical infrastructure asset to be a 'system of national significance'. The reporting entity of the critical infrastructure asset falling under this classification could be required to comply with enhanced cyber security obligations.

Enhanced cyber security obligations

Reporting entities for 'systems of national significance' may be required to:

- Develop cyber security incident response plans;
- Undertake cyber security exercises to test cyber response plans;
- Undertake vulnerability assessments; and/or
- Provide system information to the Department of Home Affairs, so that they are able to develop and maintain a near-real time threat picture.

What is the impact of the legislation?

Entities across the included 11 industry sectors must determine if current safeguards meet or exceed the SLACI Act's requirements. Entities will vary in their level of sophistication in the protection of critical infrastructure assets and therefore the time and investment to meet the SLACI Act requirements will vary. Some entities that have never categorised themselves as a part of the nation's critical infrastructure may not have systems and controls in place to comply with these requirements; while others in highly regulated industries (such as financial services) are more likely to have established compliance measures in place that may meet these new requirements.

What should entities do now?

Entities within the 11 critical infrastructure sectors should:

- Establish a team with the appropriate capability and experience to assist in identifying the current state of compliance and implementing systems and controls to meet requirements. This will most likely require a multi-disciplinary approach across the organisation, including considerations from (but not limited to) compliance, risk management, internal audit, incident response, technology, cyber security, operations and Project Management Office (PMO);
- Determine which assets meet the critical infrastructure asset definition; and
- Assess the current state of compliance with the SOCI Act and SLACI Act, including identifying systems and controls that meet these requirements;
- Establish and execute implementation plans to optimise systems and controls, as required, across the organisation, organisational entities and defined assets, including:
  - Determining the improvements that will be required under existing policies, procedures and processes – as well as contracts with entities in supply chains;
  - Updating incident response plans, risk management processes, and asset registers;
  - Ensure reporting and governance mechanisms are updated to provide continuous compliance with the Act; and
  - For any identified gaps ensure there is an implementation plan which defines owners, actions and timeframes required to close these gaps; and
  - Monitor actions through to closure.
- Participate in additional industry consultation sessions ("Town Halls") with the Department of Home Affairs and the Cyber and Infrastructure Security Centre. Indications are that additional consultation is expected throughout 2022 with industry on the Risk Management Program requirements, as well as Systems of National Significance declarations.

How Protiviti can help

With the expansion of in-scope industries and adjusted definition for 'Critical Infrastructure Assets', organisations will be under pressure to ensure existing cyber security, resilience and risk management practices and procedures meet the required standards.

Protiviti has extensive experience helping organisations strengthen their risk and resilience practices in line with regulatory reforms through enterprise risk and resilience program implementations, compliance and cyber security assessments, including design, implementation and testing.

Appendix: Listing of Critical Infrastructure Asset Classifications

The following table provides more detail on each of the changes including a list of all critical infrastructure sectors and 22 critical infrastructure assets.

1. Critical infrastructure sectors	• Communications • Data storage or processing • Financial services and markets • Water and sewerage • Energy • Defence • Healthcare and medical • Higher education and research • Food and groceries • Transport • Space technology
2. Redefining the scope of critical infrastructure assets	22 asset classes: • Communications sector — telecommunications asset — broadcasting asset — domain name system • Data storage or processing sector — data storage or processing asset • Financial services and markets sector — banking asset — superannuation asset — insurance asset — financial market infrastructure asset • Water and sewerage sector — water asset • Energy sector — gas asset — electricity asset — energy market operator asset — liquid fuel asset • Health care and medical sector — hospital • Higher education and research sector — education asset • Food and grocery sector — food and grocery asset • Transport sector — freight infrastructure asset — freight services asset — port asset — public transport asset — aviation asset • Space technology sector • Defence industry sector — defence industry asset
3. Enforcing mandatory cyber incident reporting	• The provision of operational and ownership information to the Register of Critical Infrastructure Assets; and • Mandatory cyber incident reporting for certain assets
4. Creating "Government Assistance Measures"	• Information gathering • Action directions • The power to step-in to protect a network or system • Provide advice and assistance on mitigating damage and restoring services

Contacts

Ewen Ferguson
+61 478 491 056
ewen.ferguson@protiviti.com.au

Leslie Howatt
+61 488 301 794
leslie.howatt@protiviti.com.au

Hirun Tantirigama
+61 423 853 453
hirun.tantirigama@protiviti.com.au

Tanya Barter
+61 403 991 818
tanya.barter@protiviti.com.au