HERBERT SMITH FREEHILLS

DEMYSTIFYING AUSTRALIA'S RECENT SECURITY OF CRITICAL INFRASTRUCTURE ACT REFORMS

14 June 2022 | Insight
Legal Briefings – By **Cameron Whittfield, Peter Jones and Marine Giral**

The 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, this reform agenda now leads the world. The Act is part of an increasingly complex cybersecurity regulatory ecosystem. This high-level summary provides a simple overview to help demystify the complexities of the new regime.

KEY TAKEAWAYS

1. The full Security of Critical Infrastructure Act reforms (split in two, in December 2021 and in March 2022) are now in force.

2. While Government intervention and direction obligations have been in place since last December, positive security obligations and enhanced security obligations are now in effect.

3. Despite the apparent simplicity of the regime, applicability remains complex and uncertain. The legislation covers a broad range of companies, arguably more than intended.

4. Given this, many Australian corporates are now grappling with multiple legislative and regulatory regimes, in addition to the critical infrastructure reforms.

5. Despite this complexity, these reforms are arguably the most ambitious and significant security reforms in Australian legislative history.

6. This summary provides a high-level overview. We look to simplify a complex regime, acknowledging that complexity exists just below the surface and will invariably require a case-by-case assessment.

Download PDF version of this article

THE REFORMS EXPLAINED...

The Act introduces broad Government direction and intervention powers in respect of assets that relate to ten critical infrastructure sectors ("critical infrastructure sector assets"). The Act also imposes positive security obligations on entities ("responsible entities") that own or operate assets in those sectors that meet certain criticality thresholds ("critical infrastructure assets").[1] and enhanced obligations apply to designated "systems of national significance". We clarify below what each obligation and power entails, and the sectors or assets in respect of which they apply.

WHAT ARE THE COVERED SECTORS AND ASSETS?

This infographic provides a simplified visual presentation of the different "critical infrastructure assets" or "critical infrastructure sectors assets" which are or will be captured by new obligations or powers under the Act.

Hover over the different obligations or powers to reveal the assets or sectors covered. For more information about how the Act will apply to a specific asset, hover over the box for that asset.

Download PDF version

WHAT ARE THE SECURITY OBLIGATIONS UNDER THE ACT AND WHEN DO THEY BECOME ENFORCEABLE?

GOVERNMENT DIRECTION AND INTERVENTION POWERS

DEMYSTIFYING THE SECURITY OF CRITICAL INFRASTRUCTURE 2018_PAGE_1.JPG

When an actual or imminent cyber security incident has or is likely to have an impact, direct or indirect, on: (i) the availability, integrity or reliability of a critical infrastructure asset; or (ii) the confidentiality of information about, or stored within, the asset ("relevant impact") posing a material security risk, the Government can,[2] issue the following directions:

- **information gathering directions** in relation to the incident and / or impact on the relevant asset;[3]
- **specific action directions** in response to the incident and the relevant asset;[4] or
- **intervention requests** authorising the Australian Signal Directorate ("ASD") to step in to respond to an incident, including by: (i) accessing, modifying or analysing computer systems or data; (ii) installing computer programs; and (iii) removing, disconnecting, connecting or adding computers or computer devices.[5]

Importantly, these powers can be enforced not only in respect of critical infrastructure assets but also against any entity that owns, operates, holds a direct interest in, or is a managed service provider for a "critical infrastructure sector asset". For example, this could capture IT systems or other equipment supplied to support / service critical infrastructure assets.

POSITIVE SECURITY OBLIGATIONS

There are three positive security obligations set out under the Act (only the first two 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, each obligation only applies to critical infrastructure asset classes in respect of which that obligation has been "switched on" (as illustrated in the below infographic) ("regulated asset"). The Government has advised it will only "switch on" the obligations where it considers there to be no sufficient and existing alternative regulatory or administrative arrangements.[6]

REGISTER OF CRITICAL ASSETS (IN EFFECT FROM 8 OCTOBER 2022)

DEMYSTIFYING THE SECURITY OF CRITICAL INFRASTRUCTURE 2018_PAGE_2.JPG

The Secretary maintains a confidential Register of Critical Infrastructure Assets. A responsible entity for, or an entity that is a direct interest holder in, a regulated asset (each a "**reporting entity**") must provide the Register certain "operational" and interest or control information. This includes information about the asset (including its location), the entity, and contractual arrangements for the operation of core functionalities of the asset or the maintenance of "business-critical data".[7] Reporting entities not already captured under the previous legislation must comply with these obligations from 8 October 2022 (or 6 months after an asset becomes a "regulated asset").

NOTIFICATION OF CYBER SECURITY INCIDENTS (IN FORCE FROM 8 JULY 2022)

DEMYSTIFYING THE SECURITY OF CRITICAL INFRASTRUCTURE 2018_PAGE_3.JPG

Responsible entities for a regulated asset must **report actual or imminent cyber security incidents** to the Australian Signals Directorate within **72 hours** of the entity becoming aware of it. This timeframe is reduced to **12 hours** if the incident has had, or is having, a "significant impact"[8] on the availability of the asset. These obligations apply from 8 July 2022 (or 3 months after an asset becomes a "regulated asset").

RISK MANAGEMENT PROGRAMS (WITH FURTHER CONSULTATION IMMINENT)

DEMYSTIFYING THE SECURITY OF CRITICAL INFRASTRUCTURE 2018_PAGE_4.JPG

Responsible entities for regulated assets must, subject to the adoption of implementing rules,[9] create, maintain and comply with a "risk management program" (with associated annual reporting obligations).
A risk management program is a written program that contains:

- a process or system for identifying the operational context of each relevant asset;
- a principles-based risk identification process used to identify risks to the asset;
- a risk management process or system that includes, for each material risk to the asset, a process or system to consider the risk and minimise or eliminate the risk; and
- a process for reviewing the program, and for keeping the program up to date,

- and takes an “all-hazards” approach, requiring 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,[10] will be exempt from the risk management program obligations.[11]

ENHANCED CYBER SECURITY OBLIGATIONS

A responsible entity for a critical infrastructure asset declared by the Government as “system of national significance” may be required to comply with one or multiple “enhanced cyber security obligations”:

- **Statutory incident response planning obligations** – adopt, maintain and comply with an incident response plan with respect to its assets;
- **Requirement to undertake cyber security exercises** – conduct cyber security exercises to test the entity’s ability and preparedness to respond to, and mitigate, cyber incidents with reporting relating to the exercise (and in some circumstances, external audits);
- **Requirement to undertake vulnerability assessments** – undertake a vulnerability assessment in respect of the relevant asset; and / or
- **Provision of access by ASD to system information** – provide the ASD periodic or event-based reports, or install software that transmits system information to the ASD.

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

FOOTNOTES

1. Thresholds will depend on the sector but generally will be based on the size, revenue or number of end users of the asset.

2. There must a material risk that the incident has seriously prejudiced, is seriously prejudicing or is likely to seriously prejudice (i) the social or economic stability of Australia or its people, (ii) the defence of Australia or (iii) national security; and no existing regulatory system could be used to provide a practical and effective response to the incident.

3. To give an information gathering direction, the Minister must be satisfied that it is likely to facilitate a practical and effective response to the incident.

4. To give an action direction, the Minister must be satisfied that all of the following criteria are met: (a) 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

5. To give an intervention request, the Minister must be satisfied that 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.

6. For example, telecommunication carriers and carriage service providers are already subject to certain security requirements under the Telecommunication Act, and the Department of communication is considering introducing specific telecommunication rules that would impose equivalent reporting obligations on those providers to that imposed on other sectors under the Act.

7. 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.

8. An incident will have a significant impact if it has materially disrupted the availability of essential goods or services.

9. The draft risk management program rules containing the detailed requirements under, and entities covered by, the risk management program obligations, are to be the subject of further industry consultation.

10. Current list of certified service providers is available here.

11. 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.

- TECH, DIGITAL & DATA

- GEOPOLITICS AND BUSINESS

- NEW BUSINESS LANDSCAPE

RELATED ARTICLES

Tax in M&A in the UK and Europe – What you need to know

Crypto winter is here – what does it mean for insolvency practitioners?

Deal or no deal? Bring disputes lawyers in early to close that deal

KEY CONTACTS

If you have any questions, or would like to know how this might affect your business, phone, or email these key contacts.

CAMERON WHITTFIELD
PARTNER, MELBOURNE
+61 3 9288 1531
cameron.whittfield@hsf.com

JULIAN LINCOLN
PARTNER, HEAD OF TMT & DIGITAL AUSTRALIA, MELBOURNE
+61 3 9288 1694
Julian.Lincoln@hsf.com

PETER JONES
PARTNER, SYDNEY
+61 2 9225 5588
peter.jones@hsf.com

MARINE GIRAL
SOLICITOR, MELBOURNE
+61 3 9288 1496
marine.giral@hsf.com