Critical Infrastructure Reform

DSPANZ

Patrick Fair ASSOCIATES

Outline

- Outline of the existing rules
- Outline of new rules
- Coverage consultation
- Rule making consultations
- Issues for industry and summary of new requirements

Outline of existing rules

Who is covered by the existing law?

- Listed ports, nominated water, electricity, gas and other critical infrastructure assets privately declared by the Minister.
- Broadly, regulated water, gas and transmission assets need to serve more than 100,000 customers per day.
- Electricity generators above certain thresholds: New South Wales – 1400MW, Victoria – 1200MW, Queensland – 1300MW, Western Australia – 600MW, South Australia – 600MW, Tasmania – 700MW, Northern Territory – 300MW.
- Others declared in secret by the Minister
- Regulated assets are place on a restricted register maintained by Home Affairs.

What are critical assets owners/operators required to do?

- Owners must give the Secretary operational information in relation to the asset.
- Direct interest holders in relation to a critical infrastructure asset must give the Secretary interest and control information in relation to the entity and the asset.
- The reporting entity for the asset must notify the Secretary of any change in the information provided and provide certain updating information.

Powers to enforce asset security

- The Secretary of the Department can require certain owners and operators to provide information or documents.
- The Secretary can undertake an assessment of a critical infrastructure asset to determine if there is a risk to national security relating to the asset.
- The Minister for Home Affairs can to require owners and operators 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.
- Enforced by a range of civil penalties.

Secrecy obligation

Protected information:

- is a document or information that:

  (a) is obtained by a person in the course of exercising powers, or performing duties or functions, under this Act; or

  (b) records or is the fact that an asset is declared under section 51 to be a critical infrastructure asset [i.e. by the Minister or made by the rules]; or

  (c) was a document or information to which paragraph (a) or (b) applied and is obtained by a person by way of an authorised disclosure under Division 3 of Part 4 or in accordance with section 46.

- May only be recorded, used or disclosed for the purposes of performing functions or duties under the Act.
- However, can be widely used within government.

Impact of the proposed reform

Coverage is significantly expanded

- Regulatory obligations can apply to "Critical Infrastructure Sector[s]" (**CIS)**
- A "Positive Security Obligation" can be applied in whole or part to assets in the sector.
- An asset can be subject to a rule if it "relates to" a CIS.

The CIS are:

Communications	Data storage and processing	Defence Industry
Energy	Financial services and markets	Food and grocery
Health care and medical	Higher education and research	Transport
Space technology	Water and sewerage	

Introduction of a two tier system

- First tier existing requirements and positive security obligations apply to nominated Critical Infrastructure Assets (**CIAs**).
- Second tier rules and controls apply for Systems of National Significance (**SoNS**) also apply.

What is a CIA?

- Each sector has its own test or is to be prescribed.
- The Act says a the telecommunications CIA is:

(a) a telecommunications network that is:
    (i) owned or operated by a carrier; and
    (ii) used to supply a carriage service; or
(b) a telecommunications network, or any other asset, that is:
    (i) owned or operated by a carriage service provider; and
    (ii) used in connection with the supply of a carriage service.

- The Act defines a Critical Data Storage and Processing Asset in section 12F as used wholly or primary to provide a service to:

    - federal or state government.
    - an entity responsible for a CI and relates to "business critical data"

What is business critical data

business critical data means:

(a) personal information (within the meaning of the *Privacy Act 1988*) that relates to at least 20,000 individuals; or

(b) information relating to any research and development in relation to a critical infrastructure asset; or

(c) information relating to any systems needed to operate acritical infrastructure asset; or

(d) information needed to operate a critical infrastructure asset; or

(e) information relating to risk management and business continuity (however described) in relation to a critical infrastructure asset.

Regulation depends on the rules and other matters

- An asset is only regulated if it is "specified in the rules".
- Rules can be made if:
  - "required or permitted by this Act" or
  - "necessary or convenient to be prescribed for carrying out or giving effect to this Act."
- The Minister retains the power to prescribe or declare additional assets from these sectors if "critical to the social or economic stability of Australia or its people, the defence of Australia or national security".
- Entities responsible for CIS are proposed to be included in the definition of "national security business" in the *Foreign investment Reform (Protecting Australia's Nations Security) (National Security Business) Regulations 2020*.
- This will subject the responsible entities to direct ongoing regulation regarding the extent of foreign ownership/investment via FIRB.

Obligations apply to the responsible entity

Industry	Responsible entity
Communications	Carrier or Carriage Service provider
Data Storage and processing	A provider to a Commonwealth, State or Territory Government or another CIS responsible entity
Financial services and markets	Authorised deposit taking institution, registered superannuation or insurance provider, holder of a financial services licence.
Food and grocery	Declared to be critical supermarket or food or grocery wholesaler
Health care and medical	Public hospital operator or private hospital licence holder
Transport	State government owner or operator
Energy	Holder of the licence, approval or authorisation to operate.
Space Industry	The holder of the carrier licence for the communications network supported by the carrier.

Positive security obligations

- Adopt and maintain a risk management program, if asset specified under section 30AB.
- Mandatory reporting of serious cyber incidents, if asset is specified under 30BB.
- Providing ownership and operator information, if asset is specified under section 18A.

Risk management program

- Obligation to have a risk management program applies to the responsible entity for the nominated asset.
- Purpose is to:
  - Identify each hazard where there is a material risk that the occurrence of the hazard could have a relevant impact on the asset.
  - As far as reasonably possible- to minimise or eliminate the risk of the hazard occurring.
  - Mitigate the relevant impact on the hazard.
- Other requirements can be specified in the rules.
- The Minister must consult on making or amending the rules.

Reporting

- Applies to responsible entities.
- File to industry regulator or the Secretary within 30 days of the end of each financial year.
- Annual report must:
  - State that the Critical Infrastructure risk management program of the responsible entity is or is not up to date, as may be the case.
  - If a hazard had a significant relevant impact on one or more assets:
    - Identification of the hazard
    - Evaluation of the effectiveness of the program in dealing with the hazard
    - If the program varied during the year, how the program varied.
  - Be signed off by the Board, Council or Governing Body of the responsible entity.

Mandatory incident reporting

- Obligation to report relates to a cyber security incident meaning unauthorised, access, modification or impairment of a computer or computer program or communication to or from a computer.
- The obligation to report arises:
  - If the incident had or is having "a significant relevant impact" (direct or indirect) on the availability of the asset as soon as practicable, and in any event within 12 hours of becoming aware of an incident.
  - If the incident has occurred, is occurring or is imminent and has or is likely to have a "relevant impact" as soon as practicable, and in any event within 72 hours of becoming aware of an incident.

What is a “relevant impact”

A relevant impact is an impact on:

- Availability of the asset
- Integrity of the asset
- Reliability of the asset; and/or
- Confidentiality of:
  - Information about the asset
  - Information stored on the asset; or
  - If the asset is computer data, computer data.

What is a "significant relevant impact"?

Paragraph 569 of the Explanatory Memorandum says this:

- "…will vary between assets and across sectors and it will be up to the entity to determine when a relevant impact is significant for the purposes of this reporting obligation."
- "It is expected that a significant impact would include one that affected the functioning of the asset or its ability to deliver intended services."

Systems of National Significance (SoNS)

The Minister can declare a critical infrastructure asset a SoNS after:

- Having regard to one or more interdependencies with other assets and the nature and extent of the interdependences and "other matters".
- Consulting with the relevant entity after giving notice of the intention to declare.

Obligations that apply to a SoNS

- Statutory incident response planning automatically applies: to adopt and maintain incident response plan that applies to the system and cyber security incidents.
- Secretary may, by at least 30 days' written notice, require the responsible entity to engage in a cyber security exercise.
- Secretary may by written notice require the responsible entity to undertake a vulnerability assessment.
- Secretary may require period or event-based reporting of system information.
- Secretary may require installation of system information software.

Cyber security exercise

- The purpose of a cybersecurity exercise is in relation to a cybersecurity incident:
  - Test the ability to respond appropriately
  - Test the preparedness to respond appropriately
  - Test the ability of the entity to mitigate the relevant impacts
- The cyber security exercise must comply with such other requirements as are specified in the rules.
- Designated officers may observe (including by access to premises and information).
- After the exercise an internal evaluation report must be prepared and provided to the secretary. If the Secretary believes the evaluation report was not prepared appropriately, the Secretary can require a external evaluation report.

Powers for response to serious cyber incidents

The Minister may authorise the Secretary to:

- Issue an "information gathering direction" requiring the relevant entity to give information to the Secretary
- Issue an "action direction" which requires the relevant entity to do or refrain from doing a specified Act or thing.
- Issue an "intervention request" which can require an agency to do specified acts or things in relation to the asset.

Preconditions for exercise of new powers

The new powers can be used if:

- a cyber security incident has occurred, is occurring or is considered imminent;
- The cyber security incident is likely to have a relevant impact on a critical infrastructure asset; and
- There is a material risk of serious prejudice to:
  - The social or economic stability of Australia or its people;
  - The defence of Australia; or
  - National security; and
- No existing regulatory system no existing state or federal system could be used to provide a practical and effective response to the incident.

Preconditions for exercise of new powers

The new powers can be used if:

- a cyber security incident has occurred, is occurring or is considered imminent;
- The cyber security incident is likely to have a relevant impact on a critical infrastructure asset; and
- There is a material risk of serious prejudice to:
  - The social or economic stability of Australia or its people;
  - The defence of Australia; or
  - National security; and
- No existing regulatory system no existing state or federal system could be used to provide a practical and effective response to the incident.

Coverage consultation

Consultation paper proposes sector coverage

In April 2021 Home Affairs issued a consultation paper regarding definition of CIAs including how coverage would be applied in the rules:

- Submissions closed on 14 May 2021.
- Submissions have not been published.
- Home affairs appear not to have acted on the submissions.
- Home Affairs has proceeded with Sector Specific Co-Design of the Rules.

To be defined in rules to be taken as is

Communications sector:
- critical telecommunications asset
- critical broadcasting asset
- critical domain name system

Data storage or processing sector
- critical data storage or processing

Energy sector
- critical electricity asset
- critical gas asset
- critical energy market operator asset
- critical liquid fuel asset.

Financial services and markets sector:
- critical banking asset
- critical financial market infrastructure asset
- critical insurance asset
- critical superannuation asset

Water and sewerage sector:
- critical water asset

Health care and medical sector:
- critical hospital

Higher education and research sector
- critical education asset

Food and grocery sector
- critical food and grocery asset

Defence industry sector
- critical defence industry asset

Transport sector:
- critical port
- critical freight infrastructure asset
- critical freight services asset
- critical public transport asset
- critical aviation asset

Note these definitions to apply to the Tech Sector

Telecommunications [**As mentioned** : All networks used to supply a carriage services and “any other asset” used in connection with a carriage service]

Data Storage and Processing [As mentioned: Any data storage or processing provider that: “wholly or primarily” provides a data storage or processing service to government or an entity established by federal or state government (e.g., a University); or an end user that is the responsible entity for a critical infrastructure asset and the service related to business-critical data)]

Note these definitions are proposed for the finance sector

Critical financial market infrastructure asset is: Prescribed by the rules as critical and owned or operated by the holder relevant licence in Australia and critical to the operation of a financial market

Critical banking asset is: Prescribed by the rules as critical to the carrying on of banking business by the authorised deposit-taking institution

Critical insurance asset is: Prescribed by the rules as critical to the carrying of insurance business health or prescribed

Critical superannuation asset is: Prescribed as critical to operation of registrable superannuation entity

Rule making consultation

Consultation on Critical Data Storage and Processing Rules

- Consultation commenced with a “Town Hall on 29 June”
- There have been 3 sector specific consultations with only asset owners permitted to attend.
- Energy and Water and Sewerage also underway.
- Consultation for other sectors has not commenced.

Outline of draft rules

- Cybersecurity hazards: compliance with a listed standard and level 2 maturity in the Essential 8 Maturity model
- Personnel hazards: background checks for those who may pose a risk to the asset or business.
- Supply chain hazards: standards compliance
- Physical hazards: specify contents of risk management program
- Natural hazards: specify contents of risk management program
- Material risk: rules specify risks to be addressed and contents of risk management program
- No clarification of asset classes, no express application or exemption from positive security requirements.

Advice regarding what will be "switched on"

The Government's decision to turn on the Asset Register, Risk Management Program and Cyber Risk Reporting obligations will be specific to each sector. The Department intends to make this clear on the face of the legislative instrument, accompanying explanatory materials and throughout on-going industry engagements to ensure industry understand their obligations under the Amending Bill. At this time, the Government intends to turn on Cyber Risk Reporting obligations for all critical infrastructure sectors captured by the Amending Bill. The Asset Register and Risk Management Program obligations will be turned on for the majority of sectors.

Overview and key issues for industry

Issues open for resolution

Lack of response by Home Affairs on proposed regulatory coverage requirements:

- Can the regime be restricted to only genuinely critical assets?
- Will it be possible to isolate assets covered from those outside scope?
- Will it be possible to manage the application of standards, risk management and personnel requirements for the identified subset of assets?

Overview: changes that seem likely

- Need to implement risk management program that complies with the rules.
- Need to comply with cyber incident reporting regime.
- Need to comply with new annual reporting regime.
- Possible declaration as a SoNS:
  - The need to participate in a supervised cybersecurity exercise.
  - Being subject to a vulnerability assessment.
  - Potential use of highly intrusive government powers.

Questions and discussion