

SECURITY OF CRITICAL INFRASTRUCTURE BILL

This week the Australian Government (**Government**) released an exposure draft of the *Security of Critical Infrastructure Bill 2017* (Cth) (the **Bill**) and associated *Security of Critical Infrastructure Rules 2017* (the **Rules**) which seek to manage national security risks of sabotage, espionage and coercion posed by foreign investment and involvement in Australia's critical infrastructure.

The Government is currently seeking views on the draft legislation, which (if passed) would (among other things) implement a critical infrastructure assets register (Register) and provide for a ministerial 'last resort' power to make directions in relation to assets regulated by the legislation. The Bill will also impose various reporting obligations on owners and operators of critical infrastructure assets.

Stakeholders in critical infrastructure assets, particularly within the electricity, water and ports sectors (on which the Bill is primarily focussed) should familiarise themselves with and prepare for the anticipated legislative changes described in the Bill.

BACKGROUND

The Government has a history of welcoming foreign involvement in Australia's infrastructure as an essential support to Australia's economy. While recognising the many benefits, there is a concern that foreign involvement (through ownership, offshoring, outsourcing and supply chain arrangements) may also lead to Australia's critical national critical infrastructure becoming more exposed to sabotage, espionage and coercion. Disruption to critical infrastructure assets could have a range of serious implications for business, government and the community.

In light of these concerns, in January 2017 the Government launched the Critical Infrastructure Centre (**Centre**)¹. The Centre works across all levels of government and with critical infrastructure owners and operators to identify and manage the national security risks relating to critical infrastructure. The Centre's key functions include identifying Australia's most critical infrastructure, conducting national security risk assessments, developing risk management strategies and supporting compliance.

¹ For further information, refer to the Clifford Chance client briefing available at: https://www.cliffordchance.com/briefings/2017/03/australian_criticalinfrastructurecentre.html.

Key issues

- The draft *Security of Critical Infrastructure Bill 2017* (Cth) was released this week.
- The Bill seeks to manage national security risks posed by foreign involvement in Australia's critical infrastructure, in particular in the electricity, water and ports sectors.
- If passed, the legislation would establish a critical infrastructure assets register, impose various obligations on owners and operators of critical infrastructure assets, and provide for wide information gathering and directions powers, having potential to impact owners and operators to critical infrastructure assets.
- Owners and operators of critical infrastructure assets should familiarise themselves with the requirements and prepare for the anticipated legislative changes described in the Bill.
- Interested stakeholders may make submissions on the draft Bill before **10 November 2017**.

The Centre works in close consultation with state and territory governments, regulators, and critical infrastructure owners and operators, with an initial focus on the national security risks to the four high-risk sectors of:

- electricity
- water
- ports
- telecommunications.

In September, legislation that underpins the Telecommunications Sector Security Reforms (**TSSR**) received royal assent. These reforms introduce obligations on telecommunications carriers and carriage service providers to do their best to protect networks and facilities from unauthorised access and interference. The Centre will be responsible for leading the implementation of the TSSR and is refining guidance materials to provide greater clarity for telecommunications organisations on their obligations under the legislation.

While capable of application to assets in the telecommunications sector (by Ministerial declaration or designation under the Rules, as discussed below), the focus of the new Bill is currently on electricity, water and ports, with the TSSR providing a focussed response to telecommunications security concerns.

THE BILL – AN OVERVIEW

The Bill released this week proposes three key measures to better manage the exposure of Australia's critical national critical infrastructure to security risks. If passed, it would (among other things) create:

- a **critical assets register** providing the Government with greater visibility of who owns, controls and has access to, critical infrastructure assets;
- an **information gathering power**, which would give the ability to require owners and operators of critical infrastructure assets to provide the Government with certain documents and information; and
- a **'last resort power'** which will allow the minister appointed for the purposes of the legislation (**Minister**) to issue a direction to an owner or operator of a critical infrastructure asset to mitigate significant national security risks.

As part of these arrangements, the Bill seeks to impose obligations on certain entities concerned with critical infrastructure assets to provide information to the Government in relation to the asset and notify certain events relating to the asset. Information obtained under the legislation would be protected and only capable of disclosure in certain circumstances.

The assets to which the proposed legislation would apply, the persons on whom obligations would be imposed and the nature of those obligations are discussed below.

Relevantly, the Bill does *not* change Australia's foreign investment framework under the *Foreign Acquisitions and Takeovers Act 1975* (Cth).

WHAT ASSETS ARE COVERED?

The Bill contains a range of powers, functions and obligations that would apply in relation to critical infrastructure assets. The definition of critical infrastructure assets is therefore central to the operation of the proposed legislation.

A **critical infrastructure asset** is defined under the Bill to mean:

- a **critical electricity asset** (broadly speaking this includes an electricity network, system or interconnector used for transmission or distribution of electricity as well as electricity generation stations that are critical to ensuring the security and reliability of an electricity system or network in a state or territory²);
- a **critical port** (the Bill specifies a number Australian ports to which the legislation would apply, each having strategic importance for defence, fuel reserves and/or bulk cargo. Additional ports may be declared under the Rules from time to time)³;
- a **critical water asset** (being utilities that ultimately service at least 100,000 water and/or sewage connections and where there is an entity that holds a licencing agreement with a state or territory regulator to operate the water utility);
- an **asset declared by the Minister** to be a critical infrastructure asset (the Minister is able to privately declare a particular asset to be critical infrastructure in circumstances where declaration of the asset publicly would pose a risk to national security); or
- an **asset prescribed by the Rules** to be a critical infrastructure asset (providing the regime with flexibility to include additional assets from time to time, although none are currently prescribed in the draft Rules).

WHO HAS OBLIGATIONS?

The Bill proposes to impose certain requirements and obligations on **reporting entities** and **operators** of critical infrastructure assets. The obligations are discussed further below.

A **reporting entity** for an asset means either:

- the **responsible entity** for the asset; or
- a **direct interest holder** in relation to the asset.⁴

A **responsible entity** is the entity ultimately responsible for the operation of the asset, being:

- for a critical electricity asset or a critical water asset, the entity that holds the licence, approval or authorisation (however described) to operate the asset to provide the service to be delivered by the asset;

² The Rules set out details about when an electricity generation station is critical to ensuring the security and reliability of an electricity system or network in a state or territory.

³ The specified ports set out in the Bill are the Ports of Darwin, Geelong, Port Adelaide, Rockhampton, Port Botany, Port Hedland, Brisbane, Broome, Cairns, Christmas Island, Dampier, Eden, Fremantle, Gladstone, Hay Point, Hobart, Melbourne, Newcastle, Townsville, Sydney Harbour and a security regulated port (within the meaning of the *Maritime Transport and Offshore Facilities Security Act 2003* (Cth)). The Rules may also prescribe that a specified critical port is not a critical infrastructure asset.

⁴ An entity may be both a responsible entity and a direct interest holder.

- or a critical port, the port operator (within the meaning of the *Maritime Transport and Offshore Facilities Security Act 2003* (Cth)); or
- in the case of assets declared by the Minister or prescribed by the Rules, the entity specified in the declaration or specified by the Rules.

A **direct interest holder** is an entity (which is defined to include natural persons, companies, trusts, bodies politic, partnerships, superannuation funds and certain foreign entities) holding:

- a **legal or equitable interest of at least 10%** in the asset and includes an interest that is jointly held with one or more other entities, or
- a lease of, or an interest in, the asset, that puts the entity in a position to **directly or indirectly influence or control** the asset.

Influence and control extends to the ability to materially impact the day-to-day operations of the asset, including the ability to influence or determine:

- the business or other management plan for the asset;
- appointment of key personnel involved in the day-to-day operation of the asset;
- major expenditures, major contracts or transactions in relation to the asset or its operations, or
- indebtedness of any kind in relation to the asset or its operations.

OBLIGATIONS IN RELATION TO THE REGISTER

The Register

The Bill provides for the establishment and maintenance of the Register which would contain certain information relating to critical infrastructure assets. The information to be captured on the Register is targeted at the information required by the Government to better understand who owns, controls and is in a position to influence the operation of our most critical infrastructure. Obligations to provide information are sought under the Bill to be imposed on the reporting entity best placed to supply such information.

What needs to be reported and by whom?

The Bill requires a reporting entity to provide specified information on the Register, subject to a grace period (there is a 6 month grace period following an asset becoming a critical infrastructure asset under the legislation).

Responsible entities' reporting obligations

In terms of the information to be provided, a responsible entity of a critical infrastructure asset must provide to the Register certain **operational information** in relation to the asset, being information relating to the responsible entity and any other entity that is operating the asset or part of the asset on behalf of the operator. It specifically includes:

- the location of the asset;
- a description of the area that the asset services, and
- for each entity that is the responsible entity for, or an operator of, the asset:
 - the name and address of the entity and its principal place of business;

- incorporation details (in Australia or another country) including where the entity is incorporated, formed, created in another country, the name of that country; and
- details of the arrangement under which an operator is operating the asset.

Changes to such information are also required to be notified. Operational information provided by responsible entities should provide an indication of the degree of control and access through outsourcing and offshoring arrangements, which can be difficult to establish as they are often housed in complex private contractual arrangements.

Direct interest holders' reporting obligations

Each entity which is a direct interest holder in relation to a critical infrastructure asset is required to provide **interest and control information** in relation to that entity and the asset. This information includes:

- the legal name and certain other details (jurisdiction, address and place of business or citizenship in the case of an individual) of the direct interest holder;
- the type of interest (such as a legal, equitable, lease or licence interest) and level of the interest (shareholding) the direct interest holder holds in the asset;
- details on the influence and control that the direct interest holder is in a position to directly or indirectly exercise in relation to the asset, such as voting rights and board appointments, and information on appointments to the body that governs the asset; and
- details on any relevant interest and control information, as described above, about each other entity (an ultimate interest holder or beneficial owner) that is in a position to directly or indirectly influence or control the direct interest holder.

Changes to such information are also required to be notified.

Ownership interests are often held in complex corporate structures, spanning multiple jurisdictions or through trusts, managed funds or nominee companies. The requirement to provide information on who is ultimately in a position to control the asset is designed to ensure that those interests are not hidden in complex corporate structures. The direct interest holder will bear the responsibility of reporting these ultimate interests on the Register.

Obligations on operators to report information to the Register

Only reporting entities (that is, responsible entities and direct interest holders), but *not operators*, have obligations to report information to the Register. That said, operators may be susceptible to other information provision requirements, described below.

Further action and failure to comply

Where the information provided suggests further investigation is required, other powers granted under the proposed legislation could be utilised, including a power to request information and a power to conduct a risk assessment.

Failure to comply with requirements to provide information to the Register attracts civil liability and attracts fines.

OTHER INFORMATION GATHERING POWERS

In addition to the ongoing reporting requirements on reporting entities in relation to the Register, the Bill also broadly proposes powers for the designated secretary under the legislation (**Secretary**) to require by notice in writing that a reporting entity *or an operator* of a critical infrastructure asset to provide certain information or documents where the Secretary believes the entity has information or documents relevant to the exercise of power under or performance of the legislation.

An entity receiving such a notice must comply with it and failure to comply attracts civil liability and fines.

PROTECTION OF INFORMATION

As mentioned above, the contents of the Register are not intended to be made public.

Information obtained under the legislation (including that provided to the Register, obtained following an order of the Secretary or the fact that the Minister has made private declaration of a critical infrastructure asset) is **protected information** under the Bill. The making of a record or the use or disclosure of protected information is authorised only in particular circumstances but otherwise comprises a criminal offence, carrying a potential sentence of imprisonment for up to 2 years, fines or both.

'LAST RESORT' DIRECTIONS POWER

As described above, the Bill proposes to accord wide powers to the Minister to require entities in relation to a critical infrastructure asset to do, or refrain from doing, any act or thing if the Minister is satisfied that there is a risk of an act or omission which would be prejudicial to national security. The Minister may only give such a direction if particular criteria are met and a consultation process has been undertaken.

This power is aimed at ensuring that, depending on the nature of the identified risk, the Minister is able to issue the direction to the entity best placed to take steps to manage the risk. As part of the direction, the Minister would provide the timeframe within which the entity must comply.

Given the range of national security risks that could arise, the directions power is designed to provide the Minister with flexibility and scope to issue a direction that can sufficiently manage the risk.

The explanatory document accompanying the Bill provides two examples of directions that could be made. The first example given is a direction that a critical infrastructure asset operator move corporate and operating data currently stored offshore to a more secure data storage provider. The second example given was of a direction that a critical infrastructure asset owner not out-source operations of its core network to certain providers (in perpetuity) or an order requiring that an entity must first consult the Government before entering into future outsourcing arrangements.

Failure to comply with a Ministerial direction attracts fines which escalate on a daily basis for each day of continued non compliance. Enforceable

undertakings and injunctions are also available as enforcement measures to compel compliance.

REGULATORY BURDEN AND COSTS OF COMPLIANCE

The regulatory burden of compliance with ongoing reporting requirements, requirements to provide information or compliance with Ministerial orders may vary (perhaps significantly) depending on the sector in which the critical infrastructure asset operates, the specific operational and ownership structure of the asset and the nature of any information requests or Ministerial directions given.

The explanatory document accompanying the Bill contains average regulatory compliance cost analyses modelled on certain base case scenarios, which may provide useful guidance for entities that would be impacted by the introduction of the proposed regulatory changes.

FURTHER INFORMATION

The Centre is consulting with state and territory officials and industry stakeholders on the draft legislation during October 2017. Stakeholders may provide written submissions on the draft Bill, and its supporting documents, by **10 November 2017**.

If you have any inquiries regarding the topics covered in this briefing, please contact a member of the Clifford Chance Australia team.

CONTACTS

Richard Graham
Partner, Sydney

T +61 2 8922 8017
E richard.graham
@cliffordchance.com

Richard Gordon
Partner, Sydney

T +61 2 8922 8077
E richard.gordon
@cliffordchance.com

Paul Lingard
Partner, Perth

T +61 8 9262 5575
E paul.lingard
@cliffordchance.com

Dave Poddar
Partner, Sydney

T +61 2 2922 8033
E dave.poddar
@cliffordchance.com

Tracey Renshaw
Partner, Perth

T +61 8 9262 5505
E tracey.renshaw
@cliffordchance.com

Lance Sacks
Partner, Sydney

T +61 8 9262 8005
E lance.sacks
@cliffordchance.com

Kane Barnett
Counsel, Sydney

T +61 2 8922 8090
E kane.barnett
@cliffordchance.com

Amelia Horvath
Counsel, Sydney

T +61 2 8922 8023
E amelia.horvath
@cliffordchance.com

Nadia Kalic
Counsel, Sydney

T +61 2 8922 8095
E nadia.kalic
@cliffordchance.com

This publication does not necessarily deal with every important topic or cover every aspect of the topics with which it deals. It is not designed to provide legal or other advice.

www.cliffordchance.com

Clifford Chance, Level 16, No. 1 O'Connell Street, Sydney, NSW 2000, Australia

© Clifford Chance 2017

Liability limited by a scheme approved under professional standards legislation

We use the word 'partner' to refer to a member of Clifford Chance LLP, or an employee or consultant with equivalent standing and qualifications

Abu Dhabi • Amsterdam • Barcelona • Beijing • Brussels • Bucharest • Casablanca • Dubai • Düsseldorf • Frankfurt • Hong Kong • Istanbul • London • Luxembourg • Madrid • Milan • Moscow • Munich • New York • Paris • Perth • Prague • Rome • São Paulo • Seoul • Shanghai • Singapore • Sydney • Tokyo • Warsaw • Washington, D.C.

Clifford Chance has a co-operation agreement with Abuhimed Alsheikh Alhagbani Law Firm in Riyadh.

Clifford Chance has a best friends relationship with Redcliffe Partners in Ukraine.