SHARPE & ABEL

The Big Holes in Critical Infrastructure Resilience

THE AUSTRALIAN SECURITY LEGISLATION AMENDMENT (CRITICAL INFRASTRUCTURE) BILL 2020

The twenty-first century: first 9/11, then the Global Financial Crisis and now COVID-19. Hunker down, grin and bear it, this century certainly has not been for the faint of heart! Government policies turning to security, protection and keeping out intruders is no surprise: nothing unites like a common enemy.

In 2018, Australia passed the Security of Critical Infrastructure Act 2018 (Cth) (CI Act). Just before the end of December 2020, the Parliamentary Joint Committee on Intelligence and Security released an exposure draft of the Security Legislation Amendment (Critical Infrastructure) Bill 2020 (Cth) (2020 CI Bill). The companies and people we work with are smart enough to figure out what they need to do and do not need a law firm to tell them how to comply with legislation. Our perspective on this critical infrastructure legislation is that there are two questions that need to be asked:

1. Does the CI Act address the real risk to critical infrastructure?

2. Will the CI Act be effective in what it sets out to do?

THE AUSTRALIAN SECURITY LEGISLATION AMENDMENT (CRITICAL INFRASTRUCTURE) BILL 2020

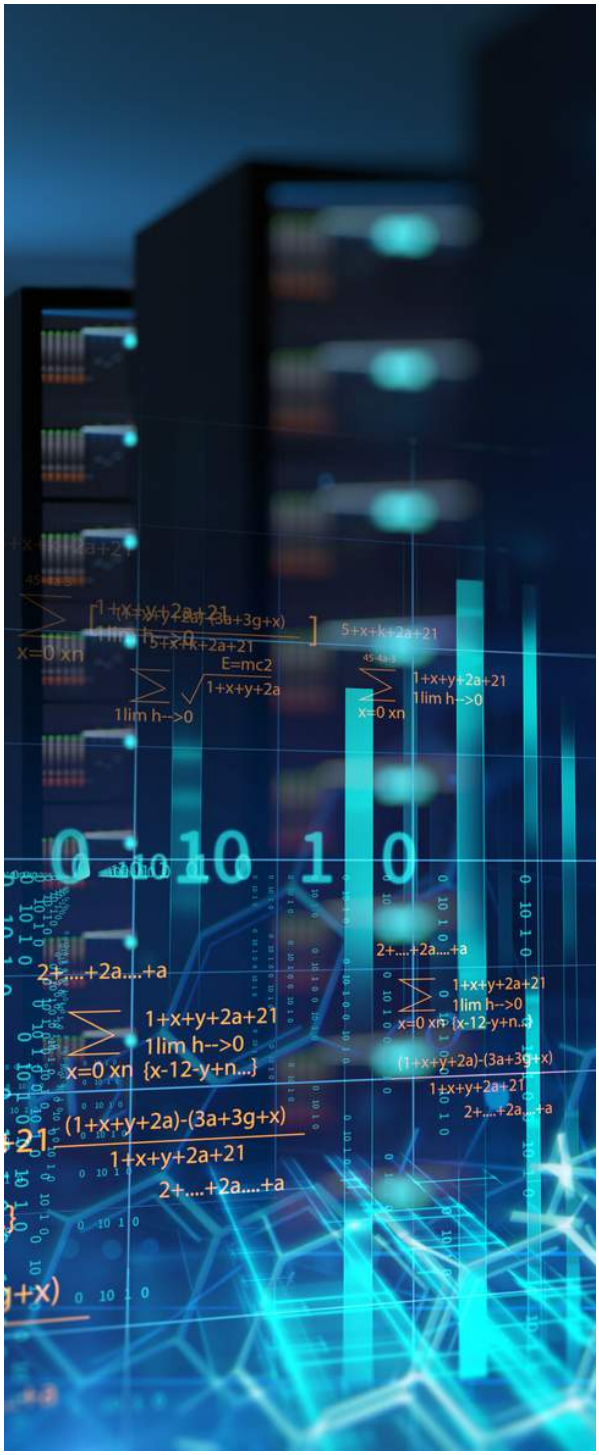
Cheat sheet summary of the CI Act and the 2020 CI Bill

The CI Act sets up an asset register of critical infrastructure assets and basically does three things:

1. Gives the Australian Government information about who owns and controls the assets;
2. Allows the Government to obtain more information (including by having the Australian Security Intelligence Organisation (ASIO)) carry out a security assessment on an entity); and
3. Obliges asset owners to provide information and notify the Government if anything happens that makes the information provided to the government incorrect or incomplete.

The original CI Act applied only to electricity, port, water or gas assets. The 2020 CI Bill plans to apply the CI Act scheme to a total of 11 sectors, including data centres, the transport sector and financial services. In addition, it plans to add three more strings to the Government bow:

1. Owners of critical assets will need to adopt and maintain a critical infrastructure risk management program;
2. Owners will be obliged to notify of cyber security incidents; and
3. The Government will have step in rights where a cyber security incident is in the national interest.



DOES THE CI ACT ADDRESS THE REAL RISKS?

In a 2019 report, the OECD recommended moving from an asset protection approach to a system resilience approach. A systems approach allows governments and infrastructure operators to address asset interdependencies and prioritise resilience measures for critical hubs and nodes whose failure would cause the most damage.

In contrast to this systems approach, the CI Act is very much about asset protection and information gathering - particularly on foreign owners. This emphasis on protection and external threats is carried through in the 2020 CI Bill, with its focus on expanding the scope of information that Government can require, and dealing with cyber security threats to protect Australia's "national interests."

External cyber-attacks are a very real threat to critical infrastructure assets: the recent SolarWinds hack and penetration into the US government demonstrate this. But a more philosophical and less tactical approach should have us consider why certain infrastructure is critical (however defined). Approached this way, the design of the CI Act and the 2020 CI Bill seems somewhat off-centre.

The purpose of critical infrastructure is to provide essential services to society and allow the economy to run continuously. The reason why certain infrastructure is deemed as critical is because disruption to the systems it is part of, tends to have economic effects far beyond the directly affected area. Disruption can occur for many reasons, including industrial accidents, malicious attacks and natural hazards. Both bushfires and the ongoing COVID-19 pandemic have shown how disruption can happen.

Looked at in this light, the CI Act and even the 2020 CI Bill seem rather preliminary, as if the Government were still carrying on a conversation with infrastructure operators and gathering information. Premised on identifying assets, the CI Act and the 2020 CI Bill focus on protection and security with a view to prevention rather than management. This focus leaves a few gaps if we want our critical infrastructure to keep our society and economy functioning:

- What happens when disruptions are to systems rather than assets?
- What happens when disruptions cannot be prevented? Who and how do we manage the systemic risk?
- Is the Government stepping in to deal with cyber security incidents of "national interest" the best way to deal with these incidents?
- How can the services that critical infrastructure provide continue in the light of climate change-related risks?

These gaps are no surprise: the design and the focus of the CI Act and the 2020 CI Bill reflect the Government's own propensities. A shortage of system-thinking skills, reliance on private sector consultants, silos over systems, a belief in centralisation and a resistance to any real acknowledgement or action regarding climate change.

So we cannot claim to be surprised if, for example, there's an electricity black out due to extreme weather and ageing infrastructure- the CI Act and the 2020 CI Bill will not deal with this.

WILL THE CI ACT BE EFFECTIVE?

What the CI Act and the 2020 CI Bill really do is give Government more information. They do this by placing compliance obligations on asset owners and prescribing penalties for failure to comply.

Again, this policy angle is no surprise. The CI Act, passed in 2018, was modelled on the Telecommunications and Other Legislation Amendment Act 2017.

The 2020 CI Bill simply builds on that foundation. Neither take into account the shift in other OECD countries away from security and protection to system resilience. So in effect, we are starting from scratch and building on an outdated regulatory model.

Whether the CI Act will be effective in securing and protecting critical assets will very much depend on what the Government does with the information it extracts from the private sector. However, what happens here we will likely never know: most of the information that is gathered and even the fact of "adverse security assessment" will be protected for reasons of national security.

Neither the CI Act or the 2020 CI Bill will deliver critical infrastructure that continuously supports the needs of our society and economy: that is not what the Government has designed the legislation for. We can expect the Government to receive a lot more information about critical infrastructure. What the Government will do with that information remains to be seen - or not.

Sharpe & Abel are lawyers and strategists who pre-empt and solve problems for industrial innovators. Our clients are creating the future. They're producing intelligent built environments and infrastructure that keep us safe and comfortable.

You produce smart solutions. We support clever companies.
Contact us to find out more.