KPMG

STEPPING UP INFRASTRUCTURE SECURITY

KPMG Board Leadership Centre

With an amendment to the Security of Critical Infrastructure Act 2018 due, KPMG Chairman Alison Kitchen spoke to Michael Pezzullo, Secretary for The Department of Home Affairs, about what it will mean for Australia's organisations.

Australia has experienced first-hand, particularly through bushfires and floods, just how urgent it is to fiercely protect critical infrastructure due to its central role in social, economic and national security.

In recognition of this, an amendment to the Security of Critical Infrastructure Act 2018 (SOCI), the 2020 Security Legislation Amendment (Critical Infrastructure) Bill, is due to come into effect in late 2021.

The amendment requires more from organisations that own or run critical infrastructure assets to ensure they are secure from threats such as cyber attacks, terrorist attacks, or extreme weather events. It expands scope to industries not traditionally thought of as infrastructure, such as health care and higher education. There are enhanced expectations to focus on the security of data and assets, as well as to have a clear risk management program and mandatory cyber incident reporting. It also defines when government assistance would be provided in the event of a cyber attack on a critical infrastructure asset.

To learn more about the amendments and what board leaders need to know to be prepared, Alison Kitchen, Chairman, KPMG Australia, held a KPMG Board Leadership Centre discussion with Michael Pezzullo, Secretary for The Department of Home Affairs, in mid-November 2021. Here are some of the key points raised.

Impetus for infrastructure protection

The new Bill is designed to put more stringent frameworks around how organisations can work to protect Australia's critical infrastructure assets, particularly from cyber-related attacks, Pezzullo explained. He said with assets now highly interconnected and digitally driven, Australia's risk exposure and the potential for far-reaching impact from a security breach have increased.

"... everything from cyber attacks that can either be for extortion purposes or for other purposes, perhaps from different kinds of actors, some of which might be state actors and some might be non-state actors, could render our way of life difficult to sustain if we're constantly and persistently being the subject of cyber attacks," he said.

Pezzullo said that in the past, shutting down a power station or a water storage dam, for example, "would have required a war-like action" on behalf of the adversary.

"Now, it's within the realm of not just imagination, but the realm of possibility for similar catastrophic impacts… in circumstances short of what we would have classically thought of as war."

For the Australian Government, this means that it needs to work closely with private infrastructure providers to ensure that asset protection standards are optimal, he explained.

"...any government that's responsible for sovereignty, for national security, for protection of the population, that is certainly front of mind."

However, he added that much like a traditional war, "no-one can look away and say, 'I'm not part of that situation…' Our great infrastructure providers are actually 'on the field', whether they are water companies, electricity companies, gas companies, transportation, logistics, and so on."

Regulation within reason

While the need to increase infrastructure asset security is well accepted, Kitchen asked Pezzullo about the regulatory burden this might have on already heavily regulated sectors. He responded that the amended Bill is designed to provide a level of protection to satisfy the Home Office from a national security perspective, and that effort had been made to ensure it complements the work organisations are already doing in terms of operational resilience.

"How do you put a security overlay over that (operational resilience), in as light-a-touch as possible so that you don't overburden those critical sectors with price and cost that then has to flow down ultimately to the consumer…which is cognisant of all the risks and interdependencies and the vulnerabilities?" he said, emphasising the challenge of getting the balance right.

He said the SOCI amendment has received bi-partisan support, and is designed to work in harmony with expectations from existing industry regulators such as APRA or the RBA. It makes clear what assets are deemed "critical", the 11 sectors that need to be involved, and the specific parts of an organisation that need greater protection. It also outlines events that could happen to organisations in which the Australian Signals Directorate (ASD) could step in "as a rescue force or a remediation force when all other avenues have been exhausted".

Kitchen clarified with Pezzullo what level of involvement board leaders could expect the ASD to have in the event of a threat incident.

"...is that support you, as in, come and help, or come and take control? And, how is that shared responsibility, liability and obligations?" she asked.

Pezzullo responded that "they don't want to take anything over...the immunities and protections that will be legislated for...really recognise that it's got to be done as a co-partnership, because a bank or a telco, or a gas company know their infrastructure much better than that rescue force."

The ASD would be appropriate in the event that an adversary has been either close to or successful, Pezzullo explained, enabling a higher level of response to either deter or punish an attacker as necessary.

Overseas reach

When it comes to infrastructure assets that may have, or in future could have, significant overseas shareholders, Kitchen asked Pezzullo what complexities might arise when it comes to the amendments. He said that the legislation is designed to be complementary to the Foreign Acquisitions and Takeovers Act 1975.

"SOCI itself will not interfere with the foreign investment decision process," he said.

He added that for assets already owned by overseas shareholders, it may require that areas of a company that have intimate access to sensitive control systems meet certain standards.

"I don't want to speculate what a future Minister might decide, but it could be a citizenship requirement, because it might be in a control room or control system. There might be the requirement to share sensitive intelligence that only can be shared with Australian citizens who hold certain types of clearances," he said.

Consolidation of information

Turning to the ever-growing issue for boards of managing compliance, Kitchen asked if there is a way that organisations will be able to consolidate the new information that they share with Government and regulators.

"We're starting to (think about it), as we think about operationalising the full suite of SOCI measures. So... how do we work with our co-regulators to come up with, I wouldn't say a template, but certainly a modality whereby, 'tell us once and we will then adjust as required within the regulatory family'."

Kitchen affirmed the benefits of this idea: "I think that would be very helpful – otherwise every company is going to be asking every other company the same thing."

Ready to launch

Will the new regulations lead to helpful, collaborative relationships, Kitchen asked, or could there be a more adversarial "gotcha" style of outcome?

Pezzullo replied that if the Government becomes an auditor of behaviour, "we'll have failed". He said while auditing is of course useful, "the model is using a regulatory tool to create a partnership."

With one part of the Bill due to be in place before the end of 2021, there is plenty for boards of infrastructure-based organisations to prepare for. One example given was to think about who has security clearance to deal with a more classified level of issues, such as how an adversary may have breached security. Another was to engage early with the changes and make the most of help available.

"We are very committed to a partnership model. So, we want to be flooded (with questions)," he said.

KPMG.com.au

March 2022. 789206282FIRM