HERBERT SMITH FREEHILLS

PARLIAMENTARY INTELLIGENCE BODY BACKS TWO-STEP ADOPTION FOR AUSTRALIA'S NEW CRITICAL INFRASTRUCTURE BILL

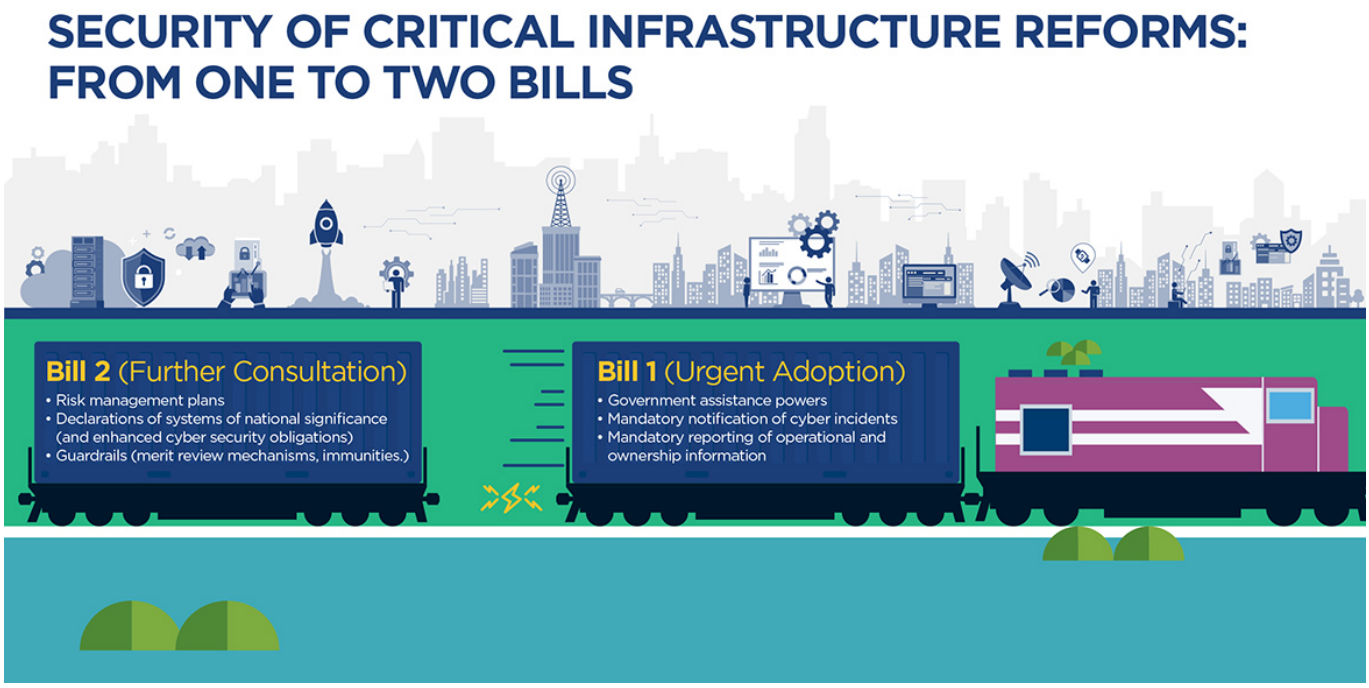
05 October 2021 | Australia
Legal Briefings – By **Julian Lincoln, Peter Jones, Christine Wong and Marine Giral**

On 29 September, the Parliamentary Joint Committee on Intelligence and Security (**PJCIS**) published its advisory report on the Security Legislation Amendment (Critical Infrastructure) Bill 2020.[1]

The PJCIS makes 14 recommendations. A key recommendation is to split the Bill in two. This would allow for the swift adoption of 'urgent elements of the reforms', including the government assistance measures and reporting obligations (**Bill 1**). Further consultation will then occur on the remaining elements of the Bill, essentially, the co-design of risk management programs and declaration of systems of national significance (this being **Bill 2**).[2]

In this briefing, we provide an overview of the PJCIS's recommendations and what this is likely to mean for organisations now and in the future.

6652O_TMT ARTICLE_LOCOMOTIVE GRAPHIC_1170PX.JPG



WHAT DOES THIS MEAN FOR ORGANISATIONS NOW?

The Government is seeking swift adoption of Bill 1 and has indicated that the Bill will likely be split into two bills consistent with the PJCIS recommendations.

Although the Opposition has raised concerns in relation to the assistance powers (including the absence of independent authorisation of those powers), it has said that it will look to the process for Bill 2 to seek any additional oversight measures. Thus, the Opposition appears likely to support the swift passage of at minimum Bill 1.

Entities responsible for assets in the expanded sectors covered by the Bill should now review their systems and processes for complying with Bill 1 on the basis this will be required shortly. In particular, there are enhanced reporting obligations requiring input from across the supply chain as well as an enterprise-wide view of critical assets. Mandatory cyber incident reporting processes must also be complied with.

Organisations should also continue to engage with the consultation process for the design of sector specific rules, including the guardrails that the PJCIS recommends be introduced as part of this process.

Those would include:

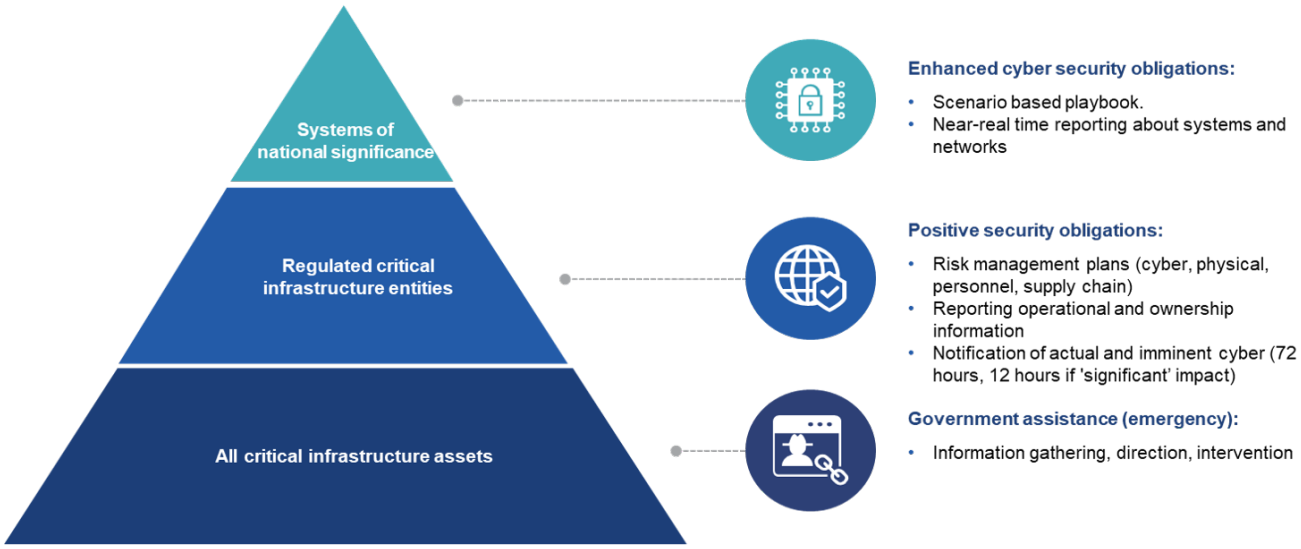
- a right of reply by entities affected by a decision or determination;

- increased transparency around declaration of systems of national significance;
- consideration of rights to merits review of administrative decisions;
- consideration of the types and breadth of immunities afforded to entities under the entirety of the SOCI Bill's proposed framework (including those in Bill 1).

SECURITY OF CRITICAL INFRASTRUCTURE BILL - RECAP

The Bill, introduced in Parliament in December 2020, proposes to bring significant reforms to the existing security of critical infrastructure legislation. It imposes enhanced security obligations on an expanded set of 22 critical infrastructure assets, as well as introducing broad government 'assistance powers'.

PROTECTING CRITICAL INFRASTRUCTURES.PNG



WHY IS THE PCJIS RECOMMENDING A SPLIT?

By recommending to split the Bill into two, the PJCIS seeks to balance the Government's insistence as to the urgency of new emergency procedures under the government assistance measures on the one hand, against industry's concerns about the proposed positive security rules on the other hand, which require further consultation. Industry has expressed valid concerns about the risk of duplication and inconsistencies with existing regimes and parallel reforms, and the PJCIS acknowledges that these concerns need to be worked through and addressed.

BILL 1 – WHAT KEY CHANGES ARE EXPECTED TO BE FAST TRACKED IN PARLIAMENT

GOVERNMENT ASSISTANCE POWERS

Broad governmental powers would be introduced including to: (i) direct owners and operators of critical assets to provide information or take specific actions; and (ii) enable law enforcement agencies to 'step in' (including by accessing, modifying or analysing proprietary IT systems), to respond to serious cyber security incidents in circumstances of emergency or distress (or both).

The PJCIS's report echoes concerns expressed in numerous submissions to its inquiry, including in relation to the breadth of these measures, the sufficiency of guardrails, oversight and review mechanisms, the hefty penalties for non-compliance and liability risk for organisations taking action in response to a direction.[3] The report notes that while Home Affairs's response to these submissions acknowledged the concerns in a general way, very few concrete suggestions for potential changes were provided.[4]

To ensure the governmental powers are actually used as a 'last resort' as intended, the PJCIS recommends that Bill 1 includes a provision that the PJCIS be notified as soon as practical each time these powers are exercised and that there be a scheduled statutory review of the legislation.[5] It also proposes to expand the role of the Cyber and Infrastructure Security Centre to include confirming whether the proposed exercise of powers is technically suitable and feasible.[6]

REPORTING OF OWNERSHIP AND OPERATIONAL INFORMATION

The definition of critical infrastructure under the Security of Critical Infrastructure Act 2018 (Cth) would be expanded to include assets in the data storage and processing, communication, health, transport, food and water, energy, financial service, education and research, defence and space sectors. Effectively, this means that entities operating those assets will become subject to the obligation to provide ownership and operational information to the Register of Critical Infrastructure Assets. This includes information about functions or systems able to control or influence the operation of critical assets and data (including outsourcing arrangements in respect thereof).

MANDATORY INCIDENT REPORTING

Entities responsible for critical assets will be required to report cyber security incidents within 72 hours from becoming aware that an incident has occurred, is occurring, or is imminent and is likely to have a relevant impact. This reduces to 12 hours for 'critical' incidents having a 'significant impact' on the availability of the asset. This is seen as a necessary component allowing for the assistance powers to be exercised when required.[7]

The report recommends some amendments to the incident notification provisions, including to clearly capture insider threats, clarify the meaning of 'significant impact', and allow extra time (up to 84 hours) for a follow-up written report after the 12-hour verbal notification for 'critical' incidents.[8]

BILL 2 – WHICH OBLIGATIONS WILL BE SUBJECT TO 'RECONSIDERATION AND CONSULTATIVE REDESIGN'?

RISK MANAGEMENT PLANS

The roll out of obligations to adopt, maintain and report on an all-hazards critical infrastructure risk management program, will require the design of sector specific rules, in consultation with the industry. Home Affairs's engagement with the different sectors, which commenced in April this year (starting with the electricity, data and cloud sectors), is not expected to complete before the middle of next year.[9] This justifies the PJCIS's recommendation to defer the adoption of that portion of the Bill. The report echoes the recommendation by some submitters to, where possible, align any elements of the positive security obligations with international standards.

SYSTEMS OF NATIONAL SIGNIFICANCE

Similar considerations support the delay of provisions enabling the Government to 'designate' systems of national significance. These are systems considered critical to the nation due to their interdependencies across sectors and consequences of cascading disruption to other critical infrastructure assets and sectors.

Systems of national significance which will be subject to enhanced obligations including development of cyber security incident response plans, undertaking of cyber security exercises to build cyber preparedness, vulnerability assessments to identify remediation actions, and the provision of access to system information to build Australia's situational awareness.

View our Cyber in Australia insights

---

1. Advisory report on the Security Legislation Amendment (Critical Infrastructure) Bill 2020 and Statutory Review of the Security of Critical Infrastructure Act 2018, available here (Report).
2. Report [2.2].
3. Report, [2.74]-[2.88].
4. Report, [3.3].
5. Report, [3.36].
6. Report [3.42].

7. Report, [3.16], [3.30].
8. Report, [3.26], [3.30].
9. Available here.

KEY CONTACTS

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

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

CHRISTINE WONG
PARTNER, SYDNEY
+61 2 9225 5475
Christine.Wong@hsf.com

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

KAMAN TSOI
SPECIAL COUNSEL, MELBOURNE
+61 3 9288 1336
kaman.tsoi@hsf.com

LEGAL NOTICE