HERBERT SMITH FREEHILLS

SECURING AUSTRALIA'S CRITICAL INFRASTRUCTURE: GOVERNMENT REFORMS WILL LEAVE NO SECTOR UNTOUCHED, BUT QUESTIONS REMAIN

09 November 2020 | Australia
Legal Briefings – By **Julian Lincoln, Anna Jaffe and Marine Giral**

On 9 November 2020, the Department of Home Affairs released the Exposure Draft of the Security Legislation Amendment (Critical Infrastructure) Bill 2020 for consultation, with submissions due by 27 November (the **Bill**).

This Bill is a critical step in the roll out of the Federal Government's proposed reforms to the existing security frameworks for critical infrastructure, as part of its 2020 Cyber Security Strategy. It follows an initial consultation period on the Department's earlier, high level discussion paper on this topic, and provides significant additional detail on the regime and next steps.

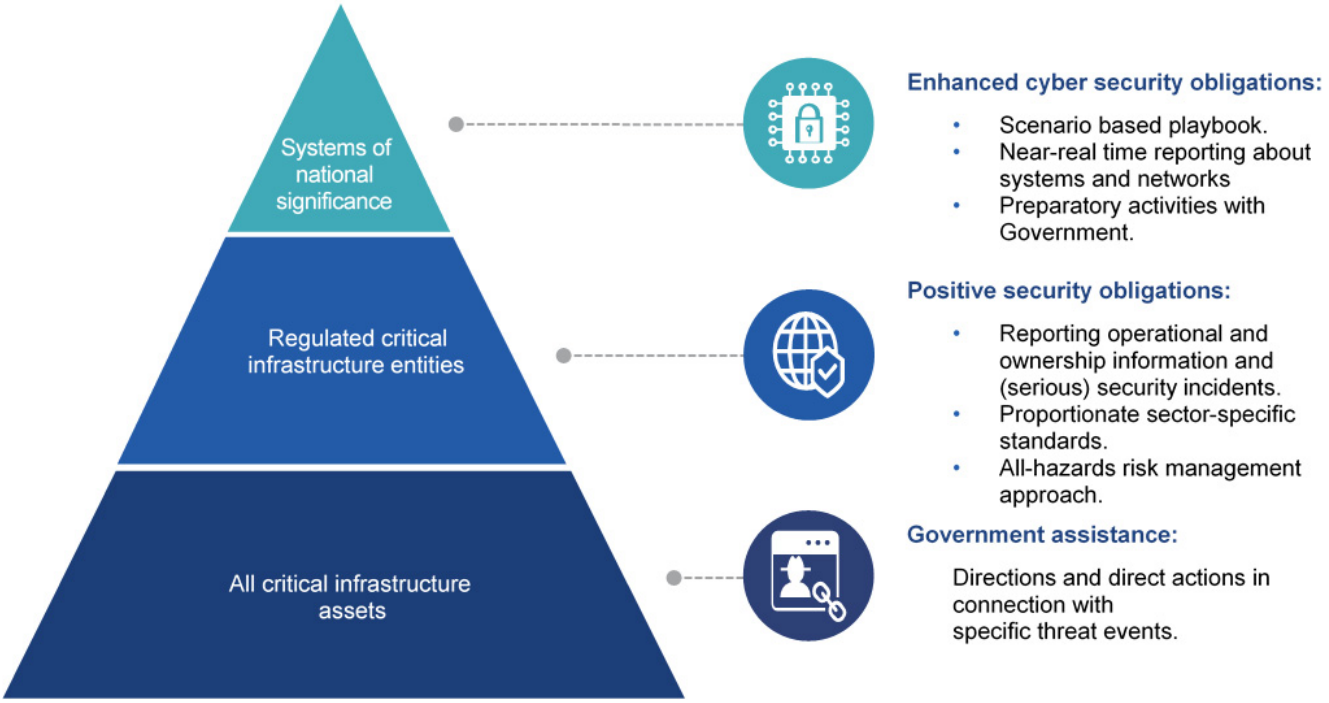
This is far from the end of the road for the reform process, with a short consultation period on this Bill prior to planned passage of the legislation by the end of this year. Further consultation on sector-specific implementation of the reforms will then continue into next year. However, it is clear from the Bill that these reforms will affect every sector of our economy and a broad range of organisations within it. The scale of their impact will depend on each organisation's market position, geographic footprint, reliance on technology and legacy systems, cyber maturity and existing regulations and standards. This means that these reforms will require detailed monitoring and engagement in order for organisations to understand how best to respond.

WHAT DO THE REFORMS DO?

The Bill introduces significant reforms to the existing Security of Critical Infrastructure Act 2018 (Cth), by both expanding the infrastructure to which it applies and the obligations imposed upon those responsible for it. That Act currently imposes limited reporting obligations on certain critical electricity, water and gas assets and ports, with some sector-specific requirements applying to specific sectors under separate regimes (for example, the Telecommunications Sector Security Reforms).

These reforms now expand the 'critical infrastructure sectors' to a total of 11, outlined as follows:

Within those sectors, the Bill specifies the types of critical infrastructure assets that are covered by its measures, and the "responsible entities" that will need to comply with them. The enhanced cyber security framework imposed on those sectors, assets and entities is summarised below.



If a responsible entity fails to comply with the reporting and positive security requirements, that failure will attract civil penalties.

The implementation of the proposed framework to different sectors will be subject to 'co-design' between industry and Government of principles-based standards, proportionate to the risk profile of each particular sector. Importantly, each aspect of the positive security obligations will only apply/be switched on once a rule is made in relation to that aspect for a critical infrastructure asset or class of critical infrastructure assets.

WHAT POTENTIAL ISSUES MIGHT ARISE UNDER THE BILL?

The Bill adds significant detail to the high-level proposals contained in the earlier discussion paper. Given the leap forward that the Bill represents from those earlier concepts, it is not surprising that the Bill itself may give rise to further issues that will need to be considered by all stakeholders. We expect the next phase of consultation to focus on at least the following key issues:

- **Striking the right balance between flexibility and clarity.** As the explanatory documentation accompanying the Bill noted, these reforms have received 'cautious support' to date. In light of the events of 2020, the need to ensure enhanced security and resilience of our nation's critical infrastructure has never been more clear. However, the implementation of reforms designed to achieve these aims need to strike a very delicate balance between ensuring the right level of flexibility to apply across the economy, in a proportionate manner and having regard to ever-evolving technological environments, while also providing responsible entities with the level of clarity they need to know exactly how to comply. It is not yet clear whether that balance has been appropriately struck. For example:
    - the scope of the 'data storage or processing' sector (previously referred to as 'data and the cloud') is not entirely clear. Key terms such as 'data processing service' are not defined, and the line between assets that are and are not 'wholly or primarily' used in connection with such services and those for which data storage and processing is 'secondary' may be difficult to determine with confidence; and
    - entities that operate in more than one sector at once will need to clearly understand where the 'lines' between obligations lie.
- **Harmonisation with other applicable regimes.** The Government has acknowledged that the reforms are likely to overlap, or potentially conflict, with a wide range of existing regimes. Even with the planned, incremental implementation approach, careful consideration will need to be given to these conflicts. For example, the Bill imposes a new security incident notification regime that relies upon a definition of 'cyber security incident' that (of necessity) differs from other equivalent regimes, and imposes new timeframes for notification — as short as 12 and as long as 24 hours after having determined the impact of that incident. For companies that are already dealing with the

impact of multiple data breach notification regimes (in Australia and globally, including sector-specific regimes) this could add a further layer to the compliance burden of differing thresholds and timeframes.

- **Overlap with other reform processes.** The consultation comes at a particularly active time for Government consultations and reviews, with reviews of the Telecommunications Sector Security Reforms and the Privacy Act already underway. It will be important to ensure that the Bill, if and once passed, remains consistent with those regimes.

- **Guardrails to avoid unintended consequences.** These reforms introduce additional, potentially broad governmental powers that can involve highly technical measures, and are likely to need to be exercised in circumstances of emergency or distress (or both). This means that the exercise of these powers can have far-reaching impacts, and can potentially give rise to unintended consequences. As a result, it is particularly critical to consider what guardrails, oversight and review measures are included in the Bill in respect of this exercise. The Bill already proposes to expressly exclude administrative review of decision-making under the *Administrative Decisions (Judicial Review) Act 1977* (Cth). It will therefore be important to understand whether the relevant powers are indeed 'clearly defined and are confined, proportionate and appropriate', as the Government has suggested. For example, should some level of technical consultation or expert advice be made available to accompany the exercise of powers with respect to the installation of specific system information software or giving of Ministerial directions on request by an entity?

WHAT NEXT?

As we mentioned above, consultation on the Bill remains open until the end of the month, with the Bill expected to be finalised and passed through Federal Parliament by the end of next year. The 'co-design' process will then continue into 2021. Given the importance of the reforms to a wide range of Australian organisations, early consideration and engagement with the reforms will help organisations appropriately plan for their eventual implementation.

View our Cyber in Australia insights

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

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

ALEX LUNDIE
SENIOR ASSOCIATE, MELBOURNE
+61 3 9288 1918
alex.lundie@hsf.com

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

KWOK TANG
PARTNER, SYDNEY
+61 2 9225 5569
Kwok.Tang@hsf.com

KATHERINE GREGOR
PARTNER, MELBOURNE
+61 3 9288 1663
Katherine.Gregor@hsf.com

LEGAL NOTICE