Australian Banking Association

Australian Banking Association Submission - Review of the Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022

The Australian Banking Association (**ABA**) appreciates the opportunity to provide a submission to the Parliamentary Joint Committee on Intelligence and Security review of the Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022 (**SLACIP Bill**).

ABA welcomes the steps the Government is taking to work with critical industries to enhance industries' operational and cyber resilience. ABA members already cooperate with the relevant Government agencies and with the Council of Financial Regulators (**CFR**) on cyber security matters and we look forward to strengthening those partnerships. ABA members also engages extensively with government in relation to natural disasters and the COVID-19 pandemic.

ABA has provided input to each stage of the development of this government policy and legislation giving effect to this policy. ABA acknowledges the work that has been undertaken by the Critical Infrastructure and Security Centre (**CISC**) to engage with stakeholders and to consider questions raised by the banking sector.

ABA supports the amendment to the moneylender exemption currently contained in section 8 of the *Security of Critical Infrastructure Act 2018* (**SOCI Act**) – section 1 below.

ABA has identified a number of implementation issues or issues that are likely to require further legislative amendment, sections 2-6. These would, in an ideal world, have been resolved prior to the SLACIP Bill being passed by Parliament. ABA asks the CISC and the Government to consider and resolve these issues as a matter of priority.

Finally, ABA proposes a two-year statutory review of the significant amendments introduced to the SOCI Act, section 7.

1. Timing of SLACIP Bill passage: moneylender exemption

The SLACIP Bill includes an amendment to section 8 of the SOCI Act, which the ABA supports, to remedy an error in the drafting of this provision. It is important for this amendment to be passed before the proposed Security of Critical Infrastructure (Application) Rules 2021 (**Application Rules**) applies register reporting obligations under Part 2 of the SOCI Act to additional critical infrastructure sectors.

Section 8(2) is intended to exempt banks from being a direct interest holder of a critical infrastructure asset where a bank takes security under a lending agreement (the **moneylender exemption**). There is significant uncertainty whether the current drafting achieves this intention. Item 28 of the SLACIP Bill would amend this provision to provide the required legal certainty.

If this amendment in item 28 is not passed, the effect of the Security Legislation Amendment (Critical Infrastructure) Act 2021 (**SLACI Act**) and proposed Application Rules would require banks to report information about a significantly expanded range of critical infrastructure assets even though a bank may not hold or have access to some of the required information. In addition, this expanded obligation would require resource intensive retrospective review of lending and security agreements as well as a more onerous ongoing compliance program.

2. Detail required about the Systems of National Significance (SoNS) regime

The SLACIP Bill would create a regime to declare that an asset is a SoNS (subject to consultation), and to apply enhanced cybersecurity obligations on SoNS. The regime would provide broad discretion for the Minister or Secretary, as applicable, in making these decisions.

If the SLACIP Bill is passed, it would be crucial for the CISC to provide more clarity and certainty – via published guidance as well as ongoing sectoral consultation during implementation – to industry about the administration of the regime well ahead of its application to a critical infrastructure asset. This should include information about the metrics, triggers, or other indicia that may be used to identify a SoNS and when enhanced cybersecurity obligations may be imposed. In addition, ABA has consistently

asked for further information about how duplication with existing regulatory requirements – such as the requirement to undertake cybersecurity scenario planning with the Council of Financial Regulators – would be addressed.

Providing more transparent and specific metrics, triggers or other indicia can help entities to anticipate whether they could become a SoNS and to consider whether changes (including changes in legal agreements) may be needed as a result of being declared as a SoNS – a 28-day consultation period is welcome but unlikely to be sufficient in practice. Duplication with reporting or scenario planning required by sectoral regulators can place conflicting demands that detract from the government national security objectives.

3. Implementation matters: defining critical infrastructure assets and incident reporting

ABA has asked for further clarity about certain critical infrastructure asset definitions and the duplication between incident reporting obligations and existing sectoral reporting obligations. These questions arise under the amendments introduced in the SLACI Act but can also affect implementation of the SLACIP Bill. As such ABA strongly advocates for these questions to be clarified before the expanded register reporting and new incident reporting obligations commence.

The definitions of critical infrastructure assets are broad. In relation to payments, ABA seeks clear guidance about whether any assets used by payments participants to initiate, transmit, accept and process payments could be covered. This question would crucially determine the application of incident reporting and register reporting obligations in relation to these assets, and could have implications under the SoNS regime.

The banking industry has identified likely duplication between the incident reporting obligation and sectoral reporting obligations under prudential standards issued by the Australian Prudential Regulation Authority (**APRA**). For incidents that are reportable under both regimes, industry is still seeking clarification about whether reporting under one regime may satisfy the obligation to report under the second regime or where there is a gap between the two regimes. Industry is also seeking clarification about how to identify additional incidents that may be reportable under the SOCI Act. Clarification should provide as much legal certainty as possible, for example via rules.

Finally, it would also be desirable for the CISC to work with industry to understand the approach that industry may take to identify critical assets in the financial services and markets sector.

4. Immunity

ABA has previously supported, and continues to support the Law Council's submission about the immunity provided to critical infrastructure assets, employees and contractors, where industry takes steps to comply with a direction or determination issued under the SOCI Act. The SLACIP Bill has not addressed all areas of legal uncertainty and this can undermine the effectiveness of the directions and direct assistance regimes during a cyber incident. As such, if the SLACIP Bill is passed, ABA strongly urges the CISC to continue working with industry to review and amend the relevant provisions of the law at the earliest opportunity.

The SLACIP Bill would provide immunity to some contractors and related bodies corporate. However, immunity would not apply to the contractors of a related body corporate. This legal uncertainty can risk reducing the effectiveness of government action when there is a major cyber incident.

5. Communication and coordination in a cyber incident

ABA reiterates the need for clarity about accountability and responsibility during a cyber incident. For the banking industry this would include clarity as to lines of communication and the roles of the Australian Cyber Security Centre, APRA and CFR.

6. Impact on the Foreign Acquisitions and Takeovers Act 1975 (FATA)

ABA agrees with the concern raised by the Business Council of Australia, about the need to disentangle the definition of 'national security business' in the FATA from critical infrastructure legislation.

7. Two-year statutory review

ABA strongly advocates for a two-year statutory review of the SOCI Act, focusing on the operation, effectiveness and implications of the amendments introduced in the SLACI Act and the proposed SLACIP Bill. Specific issues for review can include:

- The definitions of critical infrastructure assets including in the financial services and markets sector;
- The process for declaring SoNS and the application of enhanced cybersecurity obligations;
- Any use of notice and direct assistance powers; and
- The appropriateness of removing administrative review from certain decisions.