Australian Banking Association

Critical infrastructure reform: ABA submission on exposure draft Bill Two and draft Application Rules

The Australian Banking Association (**ABA**) welcomes the opportunity to provide input to the consultations on the Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022 (**Bill Two**) and the Security of Critical Infrastructure (Application) Rules 2021 (**draft Application Rules**).

Risk Management Program

Bill Two would establish the legal framework for the positive security obligation to have and maintain a risk management program.

ABA notes, and agrees with the decision, as notified by the Critical Infrastructure and Security Centre (**CISC**), that banks are not proposed to be subject to the requirement to have a Risk Management Program.

Moneylender exemption

ABA understands that Bill Two is intended to contain provisions to amend and clarify the obligations of moneylenders under the Security of Critical Infrastructure Act 2018 (**SOCI Act**). At the town hall of 18 January 2022, the CISC indicated that the proposed amendments were not included in the exposure draft of Bill Two but would be provided to industry on request.

ABA is yet to receive these amendments.

It is critical for the banking industry to have the opportunity to review and provide input on the drafting of this amendment, to ensure that the amended legislation would achieve the intended policy outcome from a banking perspective.

Register reporting obligations

Application to banking assets

ABA strongly supports the proposed approach, taken under the draft Application Rules, not to apply register reporting obligations to banking assets.

Application to critical infrastructure (CI) assets in other sectors

ABA seeks clarification whether register reporting obligations are intended to apply to banks, where a bank is a direct interest holder in specific CI assets in a sector specified under the Application Rules, including critical financial market infrastructure assets that are payment systems.

The draft Explanatory Statement states that 'the responsible entities for these assets have an ongoing obligation to give the Secretary operational information and to notify the Secretary of notifiable events'. No specific reference is made to direct interest holders of such assets in draft Application Rules, the draft Explanatory Statement, or the Definitions Rules.

ABA seeks clarification whether the Application Rules are intended to apply register reporting obligations under Part 2 of the Act to direct interest holders in the specified CI assets.

Impact of moneylender exemption amendment

If the Application Rules are intended to apply register reporting obligations to direct interest holders in specified CI assets, then a bank may still have obligations to report interest and control information about other CI assets, where a bank's lending activity could result in a bank being captured as a direct interest holder in a CI asset. Section 8 of the SOCI Act intends to exempt entities undertaking certain lending activities from being captured as a direct interest holder, and ABA understands this exemption is to be amended in Bill Two.

If the register reporting obligation becomes 'live' prior to Bill Two being passed by Parliament, banks may be required to report 'interest and control information' for a broader range of CI assets for a period between the commencement of register reporting and the passage of Bill Two. This timing mismatch may be more likely to eventuate during an election year, which may result in a delay to enactment of Bill Two and the rectification of the moneylender exemption.

This would result in unintended and potentially significant compliance costs, if banks were required to review a broader range of lending activities and allocate resources to verify interest and control information about each asset. ABA has previously highlighted that the information to be reported may not be easily available to a bank (for example, a bank may not be aware of 'the name of each other entity that is in a position to directly or indirectly influence or control' the critical asset), which would create need for additional resources to be allocated to determine the entities with influence or control and create the potential risk of non-compliance for affected banks who are unable to determine within the time period.

If this timing mismatch eventuates, we ask government or CISC to provide an exemption from register reporting obligations to align with the intended scope of the moneylender exemption.

Incident reporting

Alignment with APRA reporting

As ABA has highlighted previously, there is overlap between the proposed incident reporting obligations and APRA reporting.

In this context, ABA asks the government to reconsider if and how incident reporting should apply to banks. One issue for consideration is duplication with existing reporting to APRA: if a legal obligation is to apply, ABA strongly advocates for the obligation to be harmonised (including timing for reporting) with incident notification requirements in APRA Prudential Standard CPS 234 Information Security (CPS 234), and for industry to report to one regulator only.

Clarify key terms

Relevant impact: Section 30BD requires reporting for incidents having a 'relevant impact' within 72 hours. 'Relevant impact' is defined by section 8G – Bill Two adds 8G(3). ABA seeks further clarification about the term 'relevant impact'. In particular:

- Is the term intended to include a materiality threshold, so that non-material incidents are not reported and unnecessarily increase the volume of information that needs to be reviewed by a responsible entity and by government. For the banking sector, to what extent does the term 'relevant impact' align with reporting to APRA.
- Will there be different reporting requirements for cyber incidents of different criticality/priority, for example, whether an incident impacts a function or system used for marketing communications rather than for a critical banking function, the level of detail that is to be reported for less critical incidents.

Cyber security incidents: clarify that operational incidents such as hardware failures would **not** be required to be notified where they are not a result of unauthorised access, modification or impairment.

Grace period

Under the draft Application Rules, the incident reporting obligations will commence the later of 3 months after an asset becomes a CI asset, or 3 months after the final Rules are made. ABA understands and seeks confirmation that this means critical banking assets would become subject to incident reporting obligations 3 months after the final Application Rules are made.

By comparison, register reporting obligations will have a 6 month grace period. ABA asks the Government to consider giving a 6 months grace period for the incident reporting obligations as well, to allow industry and CISC to clarify questions about thresholds and other implementation questions.

Australian Banking Association

Systems of National Significance (SoNS)

Identifying and declaring a SoNS

ABA seeks more clarity on the thresholds for declaring a SoNS in the banking sector. In any case, ABA recommends the government engage with entities that may have an asset declared as a SoNS well before the formal consultation required under the bill, as this would give the entities time to prepare for the regime. We note that the Bill requires only that a 28 day consultation period be undertaken prior to the making of a declaration, or a shorter period if the Minister is satisfied that the circumstances are urgent.

ABA continues to seek further information about the approach that will be taken to identify and declare a SoNS. For example, will an entity be identified as a SoNS (ie, a large bank as a whole), or will specific systems within an entity be identified as a SoNS (ie, a system within a large bank).

Enhanced cyber obligations

We understand SoNS will be subject to enhanced cyber security obligations, on a case by case basis.

If more than one banking asset is declared, ABA believes it would be useful to consider enhanced cyber obligations on an industry basis. This consideration should take into account existing sectoral obligations:

- Under APRA Prudential Standard CPS 234 Information Security, ADIs are required to ensure they maintain cyber security incident response plans that are reviewed annually. Consistency between regulatory requirements under the Banking Act and SOCI Act will be crucial. This means clarifying to what extent CPS 234 requirements would suffice for compliance with this enhanced cyber security obligation.
- Under existing Prudential Standards, ADIs are required to test their incident response plans annually at a minimum. In addition, financial institutions are already subject to the Council of Financial Regulators' Cyber Operational Resilience Intelligence-led Exercises (CORIE) framework, released in December 2020. The CORIE framework is intended to test and demonstrate the cyber maturity and resilience of institutions within the Australian financial services industry, and has been developed to aid preparation and execution of industry-wide cyber resilience exercises. Again, it will be crucial to remove duplication or inconsistency between regulatory obligations. It would be ideal for regulators to apply cybersecurity obligations in a coordinated manner.
- For system information periodic reporting notices under s30DB and system information event based reporting notice under s30DC, ABA proposes that the Secretary should also consider whether the same or substantially similar information is already available under a sector specific regulatory regime (s30DB(4) and 30DC(4)).

In addition to industry-level considerations, it will also be critical for ASD to work with each bank to understand what is possible and how particular information can best be provided given differences in the systems and legal / contractual arrangements in each entity.

Finally, prior to issuing a system information software notice under s30DJ, ABA proposes that the Secretary also consider the:

- impact on security and reliability of the system (including confidentiality);
- impact on CI asset's ability to continue to provide critical services in an efficient and effective manner.

This is because it may not be technically possible to install the software on the SoNS or doing so may significantly reduce the performance of the SoNS or hinder its functioning in some other manner. All these factors need to be considered adequately and in equal measure as part of the consultation required to be completed with the entity before exercising such powers.

Asset definitions

Definition of responsible entity for financial market infrastructure

The definition of critical financial market infrastructure in the new section 12D of the Act is broadly drafted. When read in conjunction with the draft Application Rules, it could give rise to a legislative obligation on a large number of financial services providers (in accordance with Part 2B of the Act) who would otherwise not be considered to operate a critical infrastructure asset, to report cyber security incidents.

ABA recommends that additional guidance is provided in the rules or elsewhere, either principle-based or by way of examples as is common practice amongst financial services regulators, to provide industry with certainty as to what assets are designed to be captured by the Act and the notification regime in Part 2B.

Amended definition of Data Storage and Processing Sector

Bill Two makes a number of changes to clarify the definition of this sector.

ABA seeks clarification whether the definition will include software as a service providers, such as SalesForce, where their primary service is a Customer Relationship Management system but storage and processing of CI asset data is required.

Banking asset definition

The definition of banking asset can be read broadly. ABA seeks to work with the CISC to clarify in practical terms which banking assets are intended to be covered.

Onshore / offshore assets

ABA reiterates previous questions about whether SOCI Act would capture offshore assets. In ABA's submission to the Security Legislation Amendment (Critical Infrastructure) Bill 2020, ABA provided two examples for consideration:

- An entity uses Amazon to host their main corporate portal for customers to access and also have their critical systems hosted in Amazon. To ensure the resilience the systems and data are designed so they are replicated in different regional availability zones (e.g. Australia and the US). An attack is being perpetrated that indicates that the one of the root causes may lie within the Amazon infrastructure. Note that, given the systems are global the systems and data may be in a different region.
- An entity uses a SaaS product provided by a company located in India. Data is located in Australia with replication to Asia. An attack is being conducted against India.

Liability

Immunity: ABA welcomes the amendments to immunity provisions in items 41-44 of Bill Two. ABA considers the revised drafting still has potential gaps in immunities for the personnel and associates of regulated entities, in relation to acts done to comply with their regulatory obligations under the expanded regime. One example may be a contractor or subcontractor for a related body corporate of a responsible entity. As such, ABA continues to propose that the immunity provisions should be amended to adopt the language used in s70AA of *Banking Act 1959* (**Banking Act**) in order to provide the necessary degree of legal certainty. ABA also notes that s70AA of Banking Act is drafted broadly to protect a person from liability in relation to an action, suit or proceeding, whether criminal or civil. It is not limited to actions or proceedings for damages

Cyber insurance: ABA continues to ask for Bill Two to provide statutory protection under existing contractual relationships to ensure that, when a responsible entity for a CI asset is complying with a direction issued under the SOCI Act, a service provider to the responsible entity may not seek to terminate a contract, enforce security or accelerate a debt under an existing contract. See, for example,

s14AC of Banking Act. Among other things, this can help to ensure cybersecurity insurance contracts are not affected by a direction issued under this regime.

Implementation

As an implementation matter, ABA seeks additional information on the role of the CISC and its operation with the ACSC. Both will be able to provide technical advice to industry, however industry would appreciate information about the respective roles of the organisations in practice.