Australian Banking Association

12 February 2021

Committee Secretary
Parliamentary Joint Committee on Intelligence and Security
PO Box 6021
Parliament House
Canberra ACT 2600

Dear Senator Paterson

Review of the Security Legislation Amendment (Critical Infrastructure) Bill 2020

The Australian Banking Association (**ABA**) advocates for a strong, competitive and innovative banking industry that delivers excellent and equitable outcomes for customers. The ABA promotes and encourages policies that improve banking services for all Australians, through advocacy, research, policy expertise and thought leadership. One of the banking sector's highest priorities is to work in partnership with Government and other stakeholders to effectively mitigate cyber threats.

The banking sector values a strong and constructive relationship with government security and intelligence agencies, there is a long history of sharing and collaborating to keep customers and citizens safe.

The ABA welcomes the opportunity to make a submission to the PJCIS review of the Security Legislation Amendment (Critical Infrastructure) Bill 2020 (**Bill**).

Critical Infrastructure Bill

The Bill significantly extends the Security of Critical Infrastructure Act 2018 (**SOCI Act**) to other sectors with the aim of enhancing the existing framework for cyber preparedness in response to increasing threats in the global community. The ABA strongly supports the Government's intentions.

Financial institutions have continuously invested significant resources and capability to strengthen cyber security controls under the close supervision of the Reserve Bank of Australia (**RBA**), the Australian Prudential Regulation Authority (**APRA**) and the Australian Securities and Investments Commission (**ASIC**). Banks have also engaged in productive information sharing with the Australian Signals Directorate (**ASD**).

It is critical that any new powers or change in regulatory structure are developed with the aim of ensuring absolute clarity of authority, accountability, obligations and liability in the event of a significant cyber-attack, both for regulators and affected entities.

The proposed bill expands the Government's powers to impose rules setting out Positive Security Obligations on a new and broad range of sectors, and to issue directions or written notices requiring entities to act including potentially installing government software. The direct-action power also allows government agencies to operate or make changes to the core technology systems of large and complex organisations.

Australian Banking Association

Need for safeguards and robust protections from liability

The amended SOCI Act regime needs to be effective to threats of such magnitude, while giving the responsible entities of critical infrastructure assets legal and commercial certainty to adopt new and emerging technology to combat these threats. To achieve these outcomes, actions taken under the SOCI Act need to be taken in close coordination with sectoral regulators to ensure there is clarity about which regulator is the 'lead' regulator for each incident, and the entities would not be subject to conflicting requirements from two or more regulators. The SOCI Act needs to draw on the entities' expertise about their sector and the threats facing the infrastructure and customers of that sector. Where entities have robust cyber security and operational resilience capabilities, they are often best placed to identify or advise on ways to respond to threats and risks to their assets, and any additional considerations or constraints that may arise where critical infrastructure assets are administered or supported by services or other assets that are outside of Australia.

The Department of Home Affairs (**DHA**) has undertaken significant engagement with stakeholders including the banking sector. DHA has also provided verbal assurances that consultation will be undertaken with sectoral regulators and affected entities. However, these procedural safeguards are not reflected in the legislation. This raises the risk that requirements imposed or actions taken under the amended SOCI Act will conflict with existing sectoral regulation (such as APRA CPS 234: Information Security) or differ from the requirements or legislative obligations of sectoral regulators, (e.g. for ADIs this would include obligations in the Banking Act 1959) potentially creating confusion at a time when confidence, speed and clarity is paramount.

For these reasons, the SOCI Act needs to clearly specify:

- Rules will be written in close consultation with the affected entities and their sectoral regulators (for banks, this includes the RBA and APRA).
- Direct action should be taken, and directions issued only in very close consultation with the entities, and in coordination with sectoral regulators.
- Rules, directions or government action should not constrain an entity from adopting new and emerging technology.

The SOCI Act needs to provide robust protections from legal or regulatory liability to a broader range of persons who may need to take action to comply with a direction issued or facilitate direct action taken under the SOCI Act. This can be modelled on existing legislative models, such as section 70AA of the *Banking Act 1959*. These persons need to take action to facilitate direct action or comply with a direction, but in doing so may be exposed to liability under other legal and regulatory regimes, such as directors duties, continuous disclosure obligations or overseas regulatory obligations. A lack of clarity as to their immunity from other legal or regulatory liability can hinder an entity's response to a cyberattack, with potential flow on impact to other entities and sectors. The policy rationale for a broader scope of immunity has been articulated by Treasury and APRA in context of legislation setting out a crisis management regime for banks and insurers. The ABA also notes the recommendation from the Law Council of Australia on immunities for regulated entities and their staff, directors and officers.

Finally, the SOCI Act should provide certainty that the government can take direct action in relation to outsourced providers if necessary. Otherwise, responsible entities of critical infrastructure assets will need to review and renegotiate all relevant supplier contracts to enable the government to take direct action affecting third party software or on third party premises. This will be time consuming and costly, and may ultimately be unsuccessful with key suppliers (in Australia or overseas). This can result in a lack of uniformity in the manner and the extent to which such supplier contracts can be amended to achieve the objectives of the Bill. At the same time, the government should also seek to ensure key suppliers – including offshore entities – continue to have the incentives to invest in Australia, to maintain the availability of key suppliers and services. Reduced choice of suppliers can create concentration risk and can make it difficult for critical infrastructure assets that operate in offshore markets. These consequences may raise geopolitical questions.

Australian Banking Association

ABA proposals for the Bill

The ABA has recommended a number of changes be made to the Bill. Many of the suggestions are simply ensuring the verbal assurances provided by the Department of Home Affairs during consultation are enshrined in the legislation.

The recommendations are:

1. The Bill be amended to include a requirement to consult with sectoral regulators on proposed rules, modelled on requirements in the Bill for the Minister to consult with relevant State and Territories ministers and regulators.
2. The Bill be amended to set out an industry co-design processes for the rules.
3. The Bill be amended to include obligations and mechanisms to avoid misalignment between rules under the SOCI Act and APRA prudential standards (and other sectoral regulations and guidance, as applicable) on matters such as reporting deadlines and materiality thresholds for incident reporting. The mechanism should allow rules to incorporate prudential standards by reference, modelled on the provision in the Bill that allows rules to incorporate standards proposed or approved by Standards Australia as in force or existing from time to time.
4. The Bill be amended to provide that, before entities are required to comply with notices such as a requirement to install government software, take specified action or be subject to direct assistance from the government, the entity has the ability to appeal to an independent person or body. A model could be taken from the recent review of the Telecommunication Sector Security Reforms (TSSR) which recommended a standing panel of experts be established for this purpose. The Bill should ensure the review can be done quickly and without compromising the timeliness of any action.
5. Related to 4, the Bill be amended to provide robust protections from legal or regulatory liability to a broader range of persons who may need to take action to comply with a direction issued or facilitate direct action taken under the SOCI Act. Such protections need to extend to, for example, corporate group members, and their directors and other officers.
6. The government consult on a legislative amendment that clearly enables the government to take direct action in relation to third party software or enter third party premises where this is reasonably necessary for the purposes of the SOCI Act. This amendment should seek to remove the need for responsible entities to review and renegotiate contracts with suppliers while balancing the suppliers' interests.

ABA proposals for ongoing public-private and cross sector coordination

The ABA also recommends the government commit to taking the following steps to ensure the effective implementation of its cyber strategy and the critical infrastructure policy. This can build on existing engagement with the DHA and ASD. For example, the Bill will require the provision of sensitive information to the Government which includes details of cyber incidents, the entity's risk management programs, and system information. However, the Bill and SOCI Act do not address how government will handle the information collected and protect highly commercially sensitive information.

1. Early consultation with industry about proposed designation of and the criteria used to determine critical infrastructure assets and systems of national significance.

   Affected entities will need sufficient time and resources to ensure compliance. Where the regime imposes reporting obligations on entities relating to existing assets, investments or loans, a significant amount of time and resources will be required to assess which assets will become subject to reporting obligations. Uncertainty about whether smaller entities or assets within a critical infrastructure industry may be designated as a critical infrastructure asset or a system of national significance can affect significant business decisions such as whether to acquire or grow an asset or business.

2. Early consultation with industry, about what information the government may require from critical infrastructure entities, and when the government may issue an intervention request or take direct action. Where the legislation does not provide for thresholds to be set or rules to be made, the government should require DHA to provide guidance to industry on these matters.
3. Information sharing between government and critical infrastructure sectors under the SOCI Act, Critical Infrastructure Resilience Strategy and Cyber Security Strategy 2020 should be done under a clear, defined and documented framework. Private sector entities need to be able to use information shared by government and should not be prevented from disclosing the information where necessary within the entity and with suppliers. Private sector entities also need the ability to share anonymously, as well as confidence that commercial sensitive information shared with the government will be protected.

For the assistance of the committee, I have attached the ABA submission to the DHA process.

If you have any questions, please contact Fiona Landis, Director of Government Relations, Australian Banking Association fiona.landis@ausbanking.org.au

Yours sincerely

Anna Bligh AC
Chief Executive Officer
Australian Banking Association

Australian Banking Association

Attachment

Issue 1: Ensure full harmonisation between the SOCI regime and APRA prudential regulation

Express provision requiring consultation with sectoral regulators

The ABA notes the SOCI Act currently requires the relevant Commonwealth Minister to consult with relevant State and Territories Ministers on specified matters. A similar obligation to consult should be extended to sectoral regulators that have been identified for each critical sector.

For example, existing section 9(4) of the SOCI Act requires the Commonwealth Minister to consult with the First Minister of the State or Territory before prescribing a critical asset. The provision should also require the Minister or the Secretary to consult with identified sectoral regulators before making rules that would determine or prescribe critical assets, making rules setting out the Positive Security Obligations (PSO) that apply to a sector or part of a sector, designating Systems of National Significance (SoNS), and issuing written notices or directions.

Deferral to prudential obligations and sector co-design

The ABA has highlighted the need to eliminate differences between proposed requirements and existing regulatory regimes, particularly under prudential regulation. Any differences in detail would result in unnecessarily duplicative regulatory obligations and potentially significant compliance burden.

As such, the ABA reiterates our position that the SOCI regime should defer to financial sector regulatory obligations, particularly APRA's prudential obligations, instead of creating new obligations under the SOCI Act.

In the alternative, the ABA also reiterates that it would be critical for any rules made under the SOCI Act that apply to the banking industry to be fully harmonised with relevant prudential obligations to the maximum extent possible.

Whether the outcome of rule-making under the SOCI Act is indeed to leverage existing regulation, avoid duplication and ensure obligations are appropriate to the industry's risk profile will depend on the Department's proposed co-design of rules. The ABA asks the Department of Home Affairs (Department) to make the industry co-design process clear on the face of the law.

This can be done under section 30AL by providing that, except for circumstances set out in section 30AL(3), the Minister must not publish rules for consultation unless the Minister is satisfied the Department has taken reasonable steps to co-design the proposed rules with relevant critical assets and the industry associations representing those assets.

Align PSO rules and prudential regulation

If the government proposes to make rules applying some or all PSOs to banks, it will be critical for the rules to avoid misalignment with prudential regulation. The ABA has provided the following two examples to the Department that illustrate the potential impact if specific proposed PSOs apply as set out in the exposure draft bill in addition to prudential regulation. The ABA will be pleased to work with the Department to undertake a gap analysis and consider these and other issues.

APRA prudential standard CPS 220: Attachment A - Risk Management Declaration

For the purposes of paragraph 49 of CPS 220, the Board of an APRA-regulated institution must provide APRA with a risk management declaration of the institution. The ABA has previously provided the details of the risk management declaration to the Department.

The declaration is required to be submitted within three months of its annual balance date (para 51 of CPS 220). By comparison, section 30AG of the exposure draft bill would require an annual report

about a critical asset's risk management program to be submitted within 30 days. A 30-day notice period as required by s30AG of the exposure draft bill may require an out of session activity from Board members to sign off on the annual report.

Secondly, the requirement for each Board member to sign the risk management program annual report is inconsistent with the requirements under CPS 220 and standard procedures for board approval. The ABA does not believe that it is necessary for each member of the Board to sign the report (Board approval in accordance with ordinary practice should be sufficient). The SOCI Act should also consider leveraging existing sector regulations covering similar board approval requirements, such as in CPS 220 Risk Management. Additionally, the members of an ADI's Board would be Accountable Persons under the Bank Executive Accountability Regime, which is designed to enhance accountability for persons with significant influence over the conduct of the ADI.

Together, these requirements are likely to result in the ADI being required to prepare two reports with substantially the same information and adopt two distinct procedures for approval and sign off for the reports. This would result in a substantial increase of the compliance burden for the entity, without any meaningful difference in the level of personal accountability for the Board members.

APRA CPS 234

APRA CPS 234 has been adopted as the cyber security benchmark for the Australian banking sector. APRA regulated entities have taken significant steps in the last twelve months to foster a transparent and open dialogue with APRA. As a result of CPS 234, Boards have become formally accountable for cyber security and we believe that this has, and will continue, to drive appropriate levels of visibility, funding, and support to enhance Australian cyber resilience.

Deadline for reporting incidents: For APRA regulated entities, the timeframes for a cyber-security incident should be made consistent with CPS 234. Section 30BC(1)(d) of the exposure draft bill requires critical cyber incidents to be reported within 12 hours, and section 30BD(1)(d) requires other cyber incidents having a relevant impact to be reported within 24 hours. Paragraph 35 of APRA CPS 234 requires an entity to notify APRA as soon as possible and, in any case, no later than 72 hours, after becoming aware of a specified information security incident. The ABA reiterates reporting obligations should align in timing as well as substance, as such ask the Department to consider requiring reporting of cyber-security incidents that have a material effect as soon as possible and, in any case, no later than 72 hours.

Single reporting channel: the ABA asks the government to establish in the legislation that an APRA regulated entity's notification to APRA under CPS 234 satisfies the requirements of sections 30BC(1)(d) and 30BD(1)(d) of the exposure draft bill, and for APRA to provide that notification to the Department. The same principle might be extended to other critical infrastructure entities with an existing regulator.

Consistency of reporting: the ABA asks the government to clarify the types of incidents that would be covered by sections 30BC and 30BD, and the differences between these incidents. Greater clarity will help to ensure intra-sector and inter-sector consistency as appropriate. The threshold should be high to avoid over-reporting. The ABA also asks the government to consider aligning the scope of these provisions with the incidents covered by the term 'information security incident' in CPS 234.

In relation to requirements in the exposure draft bill that may require a SoNS to report cyber security events, it will be important to clearly distinguish between 'events' and 'incidents', which have different levels of practicability in respect of notification.

Further APRA prudential standards

The ABA submission to the consultation paper has set out the range of APRA standards that should be covered in a gap analysis. These include CPS 220 Risk Management; CPS 234 Information Security; CPS 232 Business Continuity; and CPS 231 Outsourcing.

Other reporting obligations

The ABA will be pleased to work with the Department to identify existing reporting obligations that may provide relevant information so that ADIs are not required to comply with a potentially duplicative set of register obligations. This means industry needs clarity on the level of detail required for registers.

Any additional reporting, ie, of material weaknesses, should be done using existing reporting channels or in a way that reduces compliance impact on industry. The most relevant existing channel for the banking industry would be reporting to APRA.

Proposed mechanism to ensure full alignment with prudential regulation

Other aspects of the exposure draft bill can also create misalignment with sectoral regulation. For example, the SOCI Act concept of a critical banking asset is different from the approach taken under the Banking Act of regulating the entity that carries on banking business. This could create a risk of misalignment in entity scope or the types of assets that are covered under the respective regimes.

To mitigate this risk, the ABA proposes that the exposure draft bill specify that rules made under relevant sections (including section 12G) can incorporate by reference Commonwealth legislation and legislative instruments. This would allow rules to incorporate by reference definitions and concepts from the Banking Act 1959 and APRA prudential standards made under the Banking Act.

This proposed amendment can be modelled on section 30AN of the exposure draft bill.

Detailed PSO requirements set out in regulations

In light of the potential impact of misalignment identified in the previous section, the ABA proposes that the government consider setting out such detailed PSO requirements in regulations rather than in primary legislation. Doing so would give the government more flexibility to review and calibrate these 'default' PSO requirements and minimise unnecessary misalignment, for example after the Department has undertaken sector co-design and gains a deeper understanding of industry standard practices and best practices.

Issue 2: Impact on supply chain

Our comments below highlight the concern that third-party providers to critical infrastructure assets (and their responsible entities) may have potential requirements imposed under the proposed regime. The ABA understands that the government has not identified specific concerns about the continuation of supply to critical infrastructure entities. However, the ABA proposes that the government consider making express provisions to appropriately address the matters raised below.

Guidance from government on how banks should consider supply chain risk

The benefit of the proposed regime is that regulators and government can provide consistent guidance to critical sectors about how to identify and address risk in the supply chain. The government and regulators can also play a role to provide a whole of sector or whole of economy view of supply chain risk and the impact of such risks. However, this should not duplicate existing prudential obligations such as obligations under APRA CPS 231 Outsourcing.

Vulnerability assessment of suppliers that are also critical infrastructure assets

The requirement for critical assets to undertake risk assessment of suppliers can raise difficult questions, due to commercial confidentiality concerns. These concerns may be heightened if the supplier is also a critical infrastructure asset. The government or regulators can facilitate by undertaking sector wide or whole of economy supply chain vulnerability assessment.

Breadth of 'business critical data' definition

The ABA has highlighted that 'business critical data' is broadly defined and can capture a large percentage of an organisation's supply chain.

The ABA seeks clarification on two questions:

- Whether the first entity is only required to notify a supplier (or other entity) in accordance with section 12F(3) of the exposure draft bill if the first entity is already aware of this information. In other words, the first entity is not required to look beyond its contracts to identify suppliers to the first entity's supplier.
- That the definition of data storage and processing sector is not intended to capture banks or other organisation that may hold data or provide data storage as an adjunct part of its business.

As a practical matter, some data storage and processing critical assets will receive a large number of notifications from a number of clients. The ABA also asks the Department to consider mechanisms that may alleviate the compliance cost of the proposed notification requirement in section 12F(3) particularly in such circumstances as duplicated notifications.

System information software notice

While the issue of a system information software notice is expressed as a power that would only be exercised if an entity is unable to provide system information reports, it is an unusually intrusive power that raises the following questions.

- The ABA understands the policy intention is this power would be used as a last resort. This intention should be clear on the face of the legislation. For example, section 30DJ(1) could expressly require the Secretary to be satisfied that there is no other reasonable avenue for obtaining relevant system information. Also refer Issue 3.
- This notice can have significant commercial impact on the entity. The impact includes cost of implementation. compromised system performance (in a trading environment milli-seconds matter) or, in a worst case scenario, system availability. The complexity and risk of implementing software and/or running scripts in complex banking technology environments and networks cannot be overstated, and neither can the difficulty in establishing with certainty what impact such software or script will have on targeted systems or parts of systems. Furthermore, the cost of storage of data logs if this requirement could add significantly to that associated with existing obligations to retain information and data.
- The impact can include unintended adverse impact on system security. The requirement to install third party software can increase risk. In particular, government software that is installed in multiple critical assets can itself become a source of risk. If government specified software can be used to perform multiple functions in addition to collecting limited system information there is always a risk that it could operate beyond the authorised scope or reporting.
- For service providers who run managed services on behalf of organisations, the introduction of software they don't manage or control can potentially violate their commercial obligations to the responsible entity, other customers and possibly Australian or foreign law.
- There may be uncertainties about the application of the notice to certain assets, refer Issue 4, geographical boundary of regime.
- Implementing a system information software notice can imposes material financial cost on the entity and suppliers. These costs should not be regarded as merely a 'cost of doing business' and should be weighed before a decision is taken to issue such a notice.

The ABA also seeks clarification on how the reporting system would be implemented, including answers to these questions:

- In the case of supplier system, who is responsible for requesting for a supplier to add additional items to a log?
- Will the requirement be for the entity or supplier to provide the API for the government to pull that information or does the government expect the entity to trap the log and send on.
- How long would entities need to store log data?

Also refer to next section about the need for clearer thresholds for these decisions.

Issue 3: Need for clearer thresholds, review and appeal rights

Clear thresholds for significant decisions

The exposure draft bill and the existing SOCI Act establish essential powers based on broad criteria that are open to interpretation around what is reasonable, proportionate or capable. While the exposure draft bill contemplates consultation, it also provides reasonably broad grounds for consultation not to be undertaken. The ABA welcomes the Department's assurance that these significant national security powers will be used in a proportionate manner and in consultation with industry as much as possible. However, the breadth of these provisions means these powers can be used differently by decision-makers over time, and as such the proposed powers are of concern.

To address industry concerns, the ABA proposes that the exposure draft bill provide a number of additional checks and balances to significant decisions so that the stated policy is more clearly reflected in legislation. Relevant decisions include a decision to make rules applying to a critical sector, designate critical assets or SoNS, issue system information reporting notices or system information software notices, conducting vulnerability assessments, and use of step-in or direct assistance powers.

- Consultation required with sectoral regulators (refer Issue 1).
- Section 30AL of the exposure draft bill should not limit consultation on proposed rules to 14 days. Fourteen days is a very short period to respond to rules that are likely to be complex and can have significant impact on an entity, including by introducing additional risk. The ABA proposes that section 30AL should not prescribe a maximum period for consultation on rules, noting that consultation can be undertaken very quickly where warranted.
- The threshold for not consulting should be set higher, such as that delay would *materially* frustrate the effectiveness of the minister's authorisation.
- Use rules to set more specific thresholds for prescribing critical assets or prescribing an entity as a SoNS, provide more specificity on terms such as 'material risk' and specify when vulnerability assessments are undertaken.
- Where a decision is made or power is exercised, the legislation should provide at least one avenue for the affected entity to be consulted and/or to ask for the decision to be reconsidered. The appeal should be considered by an independent expert or an external expert panel as proposed by Comms Alliance, again noting this can be done very quickly when required.
- Further procedural safeguards for ministerial actions: the ABA also supports the proposal by Comms Alliance that the Minister be required to receive and consider an adverse security assessment before making a decision to authorise an action. The ABA also supports the Comms Alliance proposal that the Minister should consider a range of additional factors, including whether the action proposed for a direction constitutes the least intrusive means of dealing with the cyber incident; the relative impact to other

entities that may be adversely affected by the direction to the responsible entity, and the legitimate interests of the responsible entity to whom the direction relates.

- The ABA considers the proposed procedural safeguards for ministerial authorisations should also apply to the issue of a system information software notice.

Governance and review of designation as critical asset and SoNS

The industry has had experience with other regimes that may designate an entity or impose obligations on an entity for national security reasons. The experience is these regimes can be opaque, it can be difficult for an entity to confirm whether the entity is captured by the regime, and more importantly there may not be a clear mechanism for the designation of certain entities to be reviewed (especially for the entity to seek a review).

Given the potential impact for entities and assets, it will be important for legislation to provide for a transparent governance and review mechanism for this proposed regime. The mechanism should provide for periodic reviews of rules, the designation of assets as critical assets, and the designation of entities as SoNS. Also refer previous section on thresholds.

Issue 4: Ensuring effectiveness and clarity of proposed regime

Security of data

The exposure draft bill would require banks, and a large number of other critical entities, to provide sensitive information to government under information notices, security incident reports and annual reports. Information is expected to include details of cyber incidents, the entity's risk management programs, and system information. However neither the exposure draft bill nor the SOCI Act addresses how government will handle the information collected.

Legislation should set out, or provide a mechanism for the government to set out, how government will protect entities' sensitive information throughout its lifecycle. This includes but is not limited to classification, handling, storage, retention and destruction.

Need for more flexibility in identifying responsible entities

Section 12L(5) appears to contemplate that only one entity can be the responsible entity in relation to a critical banking asset. The ABA considers the regime needs more flexibility to:

- Specify two entities may be the responsible entity for an asset for some purposes; or
- Specify different entities may be the responsible entity for an asset for other purposes; or
- Provide flexibility for a responsible entity to assign or otherwise pass on a specific regulatory obligation under the regime for a particular purpose.

The ABA has identified the following scenarios where such flexibility may be needed:

- The secretary has the power to issue a written notice under provisions such as sections 30CW and 30DJ; or issue a direction under provisions such as sections 35AQ and 35AX. A related party or third party may be the entity that can take some or all of the necessary action in relation to an asset. However, in all cases, it is likely the ADI still wishes to be informed of the issue of a written notice or a direction. In these cases, the regime needs flexibility to allow the secretary to issue a written notice or direction to two (or more) entities, or alternatively to issue a written notice or direction to one entity and to inform another entity of the fact that a written notice or direction has been issued.
- This example also highlights that the responsible entity has a range of obligations under the proposed regime that may need to be met by two or more entities. The ADI may be the relevant entity to comply with the register obligations under the SOCI Act, but another

entity may be the relevant entity to comply with some written notices or directions. It would be desirable for the regime to have the flexibility to address these scenarios.

- Additionally, it may be beneficial for the regime to expressly provide a mechanism for a responsible entity to assign or otherwise pass on an obligation under the proposed regime. For example, if an ADI receives a written notice or direction but considers a third party is the relevant entity to take the required action. This could be an extension or clarification of the secretary's ability to revoke a written notice or direction and issue another written notice or direction.

Ability to disclose information

Existing Part 4, Division 3 of the SOCI Act deals with the disclosure of protected information, and disclosure of some protected information, such as that an asset has been declared a SoNS, is an offence. The permitted disclosure or use of protected information under section 41 does not address all scenarios where an entity has a legitimate reason for disclosing information and the ABA asks the Department to ensure the responsible entity can disclose protected information for the following reasons.

- An ADI or a related body corporate may need to disclose protected information within the organisation or to a third party in order to comply with an obligation imposed under the proposed regime. The exception in existing section 46(4) may not cover all such scenarios, such as where the ADI is the responsible entity, and the information may relate to a related body corporate or another entity.
- Section 41 does not appear to allow an ADI to disclose protected information to other regulators in order to comply with regulatory obligations imposed under other Australia or foreign regimes. An ADI is not permitted to disclose protected information to its current Commonwealth regulators (e.g. APRA), nor any of the international regulators (e.g. the Reserve Bank of New Zealand, or the Monetary Authority of Singapore). This is incompatible with these existing regulatory arrangements, as the obligations imposed on a System of National Significance and the powers granted over those systems are likely to materially affect those systems' cybersecurity and availability posture, and that posture is regulated by various regulators under the relevant legislation.
- An entity may also need to or wish to disclose some protected information to its customers or under commercial arrangements such as correspondent banking arrangements.

The ABA proposes that section 46 be amended to permit an entity to disclose protected information, if the entity reasonably believes that doing so would assist the entity to comply with its obligations under the SOCI Act, other Australian and overseas law, or if the entity reasonably believes doing so is required under contract.

The ABA further highlights the difficulties that some entities already face in accessing classified information from government, including information necessary to understand a government action or direction affecting the entity. The ABA proposes the government establish a rapid processes to declassify information or to share classified information with critical infrastructure entities, such as via the Trusted Information Sharing Network.

Ensuring responsible entities can comply with a direction or written notice

Section 35AW of the exposure draft bill protects entities from liability or damages in relation to acts performed under action directions issued by the Government, however there is no equivalent protection for the entity under intervention requests. Instead, the exposure draft bill explicitly protects the Australian Signals Directorate (ASD) and Constable from liability. This is concerning given the potential scope of an intervention request specified in s.35AC.

The ABA proposes the exposure draft bill be amended to protect entities (and their officers, employees and agents) from actions performed by the ASD and Constable pursuant to an intervention request that might result in (i) civil proceedings against the entity or individuals (for example, where actions result in impacts to the services and service levels provided to an entity's customers and external stakeholders); or (ii) breaches of other laws by the entity (for instance banking-specific regulations relating to risk management, security and confidentiality). We recommend mirroring the protections in section 35AW.

In addition, the ABA highlights existing provisions in the Banking Act that seek to ensure the entity receiving a direction can comply with the notice or direction, and the use of step-in powers is effective. See sections 11CD and 14A of the Banking Act.

As a practical example, if the government exercises direct assistance powers and step into an entity, the legislation would need to clearly and unambiguously provide that the government steps into any contracts with other parties, the other parties are required by law to continue to perform under their contracts and accept directions from government, and this does not trigger any contractual clauses for termination of contract. The legislation may also need to deal with scenarios where a contractor may disagree with the government's proposed course of action.

As another practical example, an entity may consider that the company constitution does not permit the entity to take the action that is required by a written notice or direction.

Lastly, the ABA highlights that risks remain for assets that may have overseas connections. For example:

- If the government directs an entity to block certain traffic or switch off systems, and traffic is from certain countries, the entity may be required under overseas law to notify authorities in other countries.
- Practically, the Department has indicated the government only intends to enter premises on Australian soil. Technically, entry and action on Australian premises could create a connection to one of our overseas data centres and raise questions about liability under foreign law including regulatory obligations and contractual liability.
- Asking some data and cloud entities to bring down one of their Available Zones means some clients will automatically move to another region.

Continuous disclosure

The ABA has queried the Department whether the government may wish to have the ability to override continuous disclosure obligations for a very limited period and under strictly limited circumstances.

- There may be circumstances where the government or entity does not want to warn the attacker that the government/entity are aware what is happening.
- If legislation provides for this limited power to override continuous disclosure, it may also need to address the consequences of the override.

Ensuring intended scope of powers is reflected in primary legislation: system information vs data logs

The ABA appreciates the willingness of the Department to engage with industry and explain the intended application of the proposed regime.

The proposed requirement to provide system information under sections 30DB, 30DC and 30DJ is potentially very broad. The ABA understands that the government does not intend to ask for information or documents that may be under third party IP, and instead the intention is to ask for data logs. If this is the case, the ABA asks that the legislation be amended to:

- Specify section 30DB applies to data logs only; and
- Provide an express exemption for information under third party IP; and/or

- Allow the responsible entity to refuse to comply with some or all of a request for information on this basis.

Otherwise, this provision of the exposure draft bill would be broader than the stated intention of government policy and cause concern for industry.

Clarifying geographical boundary of regime

The ABA has asked the Department to consider and clarify whether a particular asset may be considered to be located in Australia. For example:

- 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. Will the government expect to gain access to Amazon infrastructure and premises – and if so where and how will access occur? Which entity would have obligations to ensure this is possible? Noting 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. Similar questions may arise.

Moneylending agreement and who is a direct interest holder

The ABA reiterates our submission to the August consultation paper that the existing exemption in section 8 of SOCI Act, for moneylenders, need to be revised.

The exemption as set out in section 8(2) is narrow, and only applies where a moneylender holds an interest in an asset and:

b) The holding of the interest does not put the entity in a position to directly or indirectly influence or control the asset; and

c) If the entity is holding the interest solely by way of security—enforcing the security would not put the entity in a position to directly or indirectly influence or control the asset.

The ABA has reviewed and agrees with the concerns previously raised by the Asia Pacific Loan Markets Association. Secured lending agreements which by their nature enable the lender to enforce the security could be construed as putting the lender in a position to indirectly influence or control the asset. Additionally, enforcing security under lending agreements can put the lender in a position to directly or indirectly influence or control the asset. The result of existing section 8(2) is the terms of a large number of loans may be taken to make a lender a direct interest holder in a critical asset.

As the exposure draft bill will extend the SOCI Act regime to a significant number of entities and sectors, this has legal and practical ramifications for banks.

- The bill does not limit retrospective application of the direct interest holder test. This means banks would need to review asset financing agreements to determine whether they may be a direct interest holder. This may be very difficult if the bank does not know whether a particular asset has been captured as a critical asset.
- Managing and complying with the register obligations in respect of the large number of assets would impose a significant compliance burden on banks. The ABA also questions whether this compliance burden would be justified, in particular where the bank has not enforced security and has not obtained the relevant direct or indirect control or influence.
- As direct interest holders, banks also become ‘relevant entities’ who could be subject to a direction under a number of provisions of the exposure draft bill, thus increasing legal risk

for banks. These include an information gathering direction, an action direction, or a requirement to comply with an intervention request.

The ABA understands the Minister has confirmed the legislation is not intended to have this effect. Instead, while secured finance may give a financier an 'interest' in the asset, it is not an interest for the purposes of the SOCI Act until the financier takes steps to enforce its security and through that obtains control or influence over the asset.

This stated policy intention is still not reflected in legislation. The ABA urges the department, as a matter of urgency, amend section 8(2) of the SOCI Act to give effect to the intended scope of the moneylender exemption and avoid the unintended legal and compliance risks for banks as outlined above.