Australian Banking Association

ABA submission: Protecting Critical Infrastructure and Systems of National Significance

Introductory comments

- The Australian Banking Association (ABA) welcomes the opportunity to work with the Government to enhance cyber security and protections for critical infrastructure.
- The ABA also strongly support the Government's desire to build on rather than duplicate existing regulation. A harmonised approach is critical to the implementation of these reforms in the banking industry. This means a single regulator having a clear mandate and a transparent system in place for regulatory co-ordination for banks, This model may be relevant for other parts of the banking and financial services sector and for other sectors.
- The banking industry look forward to supporting the next stages of implementation including the analysis of existing regulation against proposed positive security obligations.

Mapping and key concepts

- **Mapping:** The ABA has assisted the Department of Home Affairs (DHA) to map parts of the banking and financial services sector, to identify key activities, services and networks.
- The ABA urges DHA to undertake further, more detailed, mapping, before setting positive security obligations (PSOs) or advising the Minister on designating systems of national significance (SoNS). Further mapping would help to ensure the obligations respond to the resilience and security issues relevant to the sector. The ABA would like to coordinate with other banking, financial services and payments industry bodies, and the Council of Financial Regulators, to provide input into the development of sector mapping.
- The ABA draw DHA's attention to potential ambiguity between the obligations of a critical infrastructure entity relating to supply chain, and any PSOs or enhanced cyber security obligations that may be imposed directly on third parties. These are particularly acute for the 'data and the cloud' sector, and managed service providers, or third parties that are based in overseas jurisdictions.
- As described, supply chain obligations under the PSOs and the exercise of government direct action could be used to limit the choice of third party suppliers for a critical infrastructure entity. If so, this potential outcome may be concerning to a number of industries and entities and would warrant further consideration.
- **Key concepts:** The ABA seeks clarification about the key concepts of 'owners' and 'operators' of a critical infrastructure entity, and whether these terms are likely to be defined broadly in line with the concept of 'direct interest holder'. If so, this can have unintended consequences.
- 'Direct interest holder' is defined broadly; while it contains an exception for moneylending agreements, this exception is narrowly drafted and excludes moneylending agreements that would put the person in a position to directly or indirectly influence or control the critical asset. If 'owners' and/or 'operators' are defined in a similarly broad manner, banks can be captured as 'owners' or 'operators' of other critical assets and become responsible for those assets' compliance with PSOs or enhanced cyber obligations.
    - This unintended consequence could be addressed by having a narrower definition of 'owner' and 'operator', and/or providing broader exceptions within these definitions for moneylending agreements or persons taking security.

- Secondly, direct interest holders have reporting obligations in relation to the critical asset that they hold a relevant interest in. Under an expanded *Security of Critical Infrastructure Act 2018* (SOCI Act), if banks may be captured as direct interest holders of a larger number of critical assets, this can also create additional reporting obligations for banks. This may also be a concern for other entities. As such it may be helpful if the SOCI Act could clarify when a direct interest holder is required to report information: for example, if the responsible entity of an asset indicates it does not have information that is required to be reported, and the information is within the possession of the direct interest holder.

Positive security obligations

- Overall, the ABA support the proposal to ensure critical infrastructure entities are subject to security obligations that provide a consistent standard of operational resilience and cyber security across sectors.
- The ABA note the consultation paper highlights cyber security risks that relate to information theft. In the banking and financial services sector and across the economy more broadly, cyber security risks also relate to data modification, destruction or corruption, and the risks of business disruption and financial loss. These risks should be recognised in proposed PSOs.
- The ABA strongly support the proposal for PSOs to cross reference or rely on existing regulations and industry standards as much as possible to avoid duplication. However, regulators have differing mandates and sector-specific legislation contains different definitions of key concepts such as business disruption and third party providers. These differences may need to be considered and/or addressed via coordination between DHA and relevant sectoral regulators.
- For the banking industry, the ABA consider that APRA's prudential standards provide comprehensive coverage of the proposed PSOs. Many of these apply to all APRA-regulated entities. Prudential standards include:
  - CPS 220 Risk Management;
  - CPS 231 Outsourcing;
  - CPS 232 Business Continuity Management; and
  - CPS 234 Information Security.
- Prudential guidance includes CPG 233 Pandemic Planning and CPG 235 Data Risk.
- These are part of a comprehensive prudential regulation regime that also covers authorisation, financial management, governance and board accountability.
- A harmonised approach where a single regulator has a clear mandate, and has transparent regulatory coordination arrangements with other relevant agencies, is critical to ensure effective implementation of PSOs. This approach would avoid legal or operational confusion resulting from different or even conflicting obligations imposed by different regulators on these important matters. The ABA views APRA as the relevant regulator for banks' PSOs, and to the extent existing regulations do not address all aspects of PSOs, these existing regulations should be enhanced in lieu of new obligations under the SOCI Act.
- Where entities may operate across two or more critical infrastructure sectors, consideration should be given to reducing regulatory overlap or establishing a hierarchy of obligations between sector specific PSOs.
- In both scenarios, having one primary regulator for the PSOs should not prevent relevant regulators delegating the role of leading an incident response to another regulator, where appropriate. For example, it may be appropriate for other financial sector regulators to

delegate response to an incident relating to payments to the Reserve Bank of Australia (RBA) even though incident response would involve banks and other financial sector entities. Having this flexibility in the regime can enable a more responsive and targeted approach to incident response.

- **Reporting obligations**: The ABA note that regulated critical infrastructure entities will have an additional obligation to report ownership information, and information about operational and cyber incidents. This reporting obligation is likely to duplicate banks' reporting to APRA and ASIC to a significant extent. As such the ABA ask the Government to consider ways to remove duplication and would be happy to provide further information to support the Government's consideration of reporting obligations.
- **Summary of applicable prudential standards**: The ABA understands APRA has provided details of prudential standards to the DHA. At high level:
  - Banks are required to have a comprehensive risk management framework to identify, measure, evaluate, monitor, report and control or mitigate all internal and external sources of material risk. Material risks are those that could have a material impact, both financial and non-financial, on the institution or on the interests of a bank's depositors. The risk management framework must include forward-looking scenario analysis and stress testing programs, commensurate with the institution's size, business mix and complexity, and which are based on severe but plausible assumptions.
  - The risk management framework must address certain risks including operational risk, and other risks that, singly or in combination with different risks, may have a material impact on the institution. The framework must also have management information system(s) that can provide accurate and timely information, based on robust data, to management and APRA both during normal circumstances and periods of distress.
  - Banks are required to ensure that all outsourcing arrangements involving material business activities entered into by an APRA-regulated institution and a Head of a group be subject to appropriate due diligence, approvals and ongoing monitoring. Outsourcing agreements for material business activities must address the risks arising from sub-contracting. Significantly, an outsourcing agreement must include a clause that allows APRA access to documentation and information related to the outsourcing arrangement, and must include the right for APRA to conduct on-site visits to the service provider if APRA considers this necessary in its role as prudential supervisor.
  - Banks are required to implement a whole-of-business approach to business continuity management, to ensure that critical business operations can be maintained or recovered in a timely fashion, in the event of a disruption. Critical business operations are the business functions, resources and infrastructure that may, if disrupted, have a material impact on the institution's business functions, reputation, profitability, depositors and/or policyholders. Banks are required to maintain, review and test a business continuity plan that addresses specified issues including recovery strategies, levels and time targets for critical operations, infrastructure and resources required, roles, responsibilities and authorities to act. Banks are also required to maintain communication plans with staff and external stakeholders.
  - Banks take extensive measures to maintain resilience against information security incidents (including cyber-attacks) by maintaining an information security capability commensurate with information security vulnerabilities and threats, and which enables the continued sound operation of the entity. Banks are required to classify information assets by criticality and sensitivity, implement information security controls to protect information assets (which are tested using a systematic

testing program), implement threat detection mechanisms and maintain information security response plans. These requirements also apply to information security assets that are managed by a related party or third party.

Voluntary information sharing with Government

- Banks are already coordinating with relevant Government agencies on cyber security, and welcome the opportunity to enhance these partnerships. Existing partnerships include information through the Australian Cyber Security Centre (ACSC), Joint Cyber Security Centre (JCSC) and Trusted Information Sharing Network (TISN).
- The banking industry provides a number of suggestions for enhancing the role of TISN and the effectiveness of Government-industry partnerships. Rhe ABA proposes that Government establish a centralised point of coordination information sharing and operational matters for critical infrastructure entities.
- The banking industry also suggests that Government clarify or resolve a number of questions about government-industry information sharing and coordination. In particular, to encourage further sharing and certainty around the continued safety of sensitive information shared by critical infrastructure entities to Government, the ABA requests the SOCI Act clearly state how shared information will be managed securely by Government throughout the information lifecycle.
    - The experience in the United Kingdom (UK) and the European Union is informative. Requiring mandatory information sharing from certain sectors led many entities to share larger volumes of information in order to avoid breaching the mandatory requirement. This made it more difficult to identify the most relevant information.
- For these reasons, the banking industry asks the Government for a policy commitment to initially focus on enhancing voluntary information sharing, before considering imposing any mandatory information sharing obligations. Clearer government guidance about the information that would be most valuable would help to improve consistency of information sharing across sectors.

Enhanced Cyber security obligations

- The ABA would like to continue working with DHA to understand which entities in the banking industry could be considered to be a SoNS, and whether this would align with categories and designations already used under the prudential regulatory regime. This will help all parties to better understand the policy objective of an entity being designated as a SoNS, and to what extent existing reporting obligations and cybersecurity preparatory exercises may already meet these objectives.
- If the Government makes a decision to designate entities in the banking and financial services sector as SoNS, the ABA urges DHA to fully consider the role that APRA and the RBA should have under this regime. This will help to harmonise cyber security obligations so as to minimise regulatory burden. APRA and the RBA are able to consider data reported by designated entities in context of information and data reporting about cyber matters from the rest of the sector. Their consideration would be informed by existing cyber security preparatory exercises under the Cyber Operational Resilience Intel-led Exercises (CORIE) framework.
- The ABA and any relevant members would be pleased to work with the Government on these questions if required. For the purposes of the SOCI amendments, one way to preserve the flexibility for regulatory coordination as described may be to include a regulation-making power. This would enable regulations to establish a sector-specific regime that allocates responsibility for supervision of enhanced cyber obligations to sectoral regulators.

Directions and direct action (step-in powers)

- The ABA proposes that Government create a regulation-making power in the SOCI Act that can be used to establish tailored arrangements for specific sectors in relation to enhanced cyber obligations and direct assistance obligations. This would give Government and industry time to conduct a gap analysis of when direct action is required and the types of direct action that may be taken, and what powers sectoral regulators already have under relevant sectoral legislation. This exercise would be essential to determine the appropriate regulatory arrangement for banking.
- Tailored arrangements can include parameters about when and how the direct action powers can be used and coordination obligations, when these are invoked.
- When there is a serious cyber incident, it will be critical to have one regulator that is adequately structured and with a clear mandate to take the actions necessary. The coordination of actions in the event of a serious cyber event would be critical to enable a rapid response. It is also critical to connect banks with the right government support – this requires both cyber security capability and an understanding of the broader financial system.
- If two regulators took action on an incident, operationally this would significantly increase the risk of inconsistent advice or directions, and potentially result in delays due to differences of opinion between regulators, or conflicting requirements being imposed.
- A tailored regime would also offer greater flexibility, and potentially allow for a bank to proactively accept assistance from Government. It would also provide the industry with greater clarity on consequential questions in relation to issues such as insurance, liability under contracts, the impact on other regulatory obligations and continuous disclosure.
- Finally, the ABA notes that the potential for the government to take direct action in relation to third party suppliers could affect Australian entities' ability to acquire such service from overseas suppliers.

Australian Banking Association

Responses to specific questions

1) Do the sectors above capture the functions that are vital to Australia's economy, security and sovereignty? Are there any other sectors that you think should be considered as part of these reforms (e.g. manufacturing)?

The ABA does not seek to identify additional critical sectors, however would like clarity on how the expanded regime would address supply chain. For example, supply of health and medical supplies.

2) Do you think the current definition of Critical Infrastructure is still fit for purpose?

Defining critical services: The ABA has provided information to DHA about the limitations of this concept of 'critical infrastructure' as applied in the banking and financial services sector. The ABA has also proposed that identifying 'critical services' may ensure the SOCI Act recognises that the focus of regulation should be on the services provided, rather than the infrastructure that may be used to provide those services (and which may change over time). This approach would also be more aligned with existing licensing and regulatory regimes in banking and financial services, but may require a new definition of 'critical services' to be included in the SOCI Act.

Impact on third parties: The ABA understands suppliers to critical infrastructure entities could also be subject to Government direction and direct action. Large entities such as banks can have a large number of suppliers, only some of which are material or may receive sensitive data from a bank. The ABA seeks clarification about whether the legislation or other elements of the regime will limit the scope of the direct action regime to material suppliers or specific categories of third parties, so as to minimise potential impact on procurement activities.

3) Are there factors in addition to interdependency with other functions and consequence of compromise that should be considered when identifying and prioritising critical entities and entity classes?

The ABA has not identified additional factors. However the concept of 'consequences of compromise' may need to be specified for each sector and recognising that it will not be possible to anticipate the full range of possible consequences of an incident.

4) What are the common threats you routinely prepare for and those you have faced/ experienced as a business?

The banking industry has experienced and demonstrated capacity to respond to a range of events in recent years. These include natural disasters, cyber incidents and the COVID-19 pandemic.

Natural disasters: In response to recent natural disasters including the bushfires, banks have provided a range of assistance programs for individual and business customers. From an operational perspective, banks have taken a range of actions including establishing emergency relief and recovery funds for individuals, farmers and small businesses; offering support and counselling to customers through the banks' assistance programs, supporting staff by providing extended leave and expanding organisational volunteering policies; providing grants or donations to not for profit organisations; and supporting staff initiatives.

Pandemic: During COVID-19, banks have adapted their operating models in response to public health requirements and the need to support customers. Banks have introduced a range of support for customers and worked with the Government to implement targeted assistance schemes. In operational terms, banks have assigned additional staff and resources to respond to increased customer demand, implemented Covid-safe plans at workplaces, including bank branches, and responded to jurisdiction-specific requirements such as the Victorian Government's essential worker permit regime.

Cyber security: Banks have robust arrangement and infrastructure to respond to cyber security threats. Banks prepare for different types of cyber attacks, both those that have a high likelihood of being attempted, but a less material impact (e.g. denial of service attacks, sending phishing emails with malware etc.) and those where the impact could be more material (e.g. loss of a critical system) and therefore the preparation and training of staff to respond is important. Responses can include:

- Implementing controls to prevent the attack and isolate and mitigate its impact;
- Contracting for services that can be provided in the event of an attack. (e.g. support for customers who have had personal details stolen or expert forensic support);
- Documenting incident response processes and plans, cyber incident playbooks and business recovery plans; and
- Testing plans and playbooks.

Banks' systems, processes, and infrastructure for responding to these and other threats are governed by APRA's prudential standards and prudential guidance addressing risk management. We refer to the high level summary provided above.

5) How should criticality be assessed to ensure the most important entities are covered by the framework?

Please refer to our introductory comment about mapping the banking and financial services sector.

ABA members, and other associations in this sector, welcome the opportunity to work with DHA on mapping and assessing criticality and would welcome doing so in coordination with the CFR.

Also refer comments about impact on third party suppliers in question 9.

6) Which entities would you expect to be owners and operators of systems of national significance?

The banking industry is already subject to extensive ownership controls under the *Financial Sector (Shareholdings) Act 1998 (Cth)* (FSSA). This legislation requires the Treasurer to be satisfied of a national interest test. The FSSA operates concurrently with the *Foreign Acquisitions and Takeovers Act 1975* (FATA).

If a bank is designated as a system of national significance, the ABA's strong view is that the FSSA (and the FATA) should continue to be the legislation used to regulate ownership matters.

7) How do you think a revised TISN and Critical Infrastructure Resilience Strategy would support the reforms proposed in this Consultation Paper?

The ABA have the following suggestions:

- The TISN has existing arrangements for information exchange, with a crisis management and organisational resilience focus. These exchanges could offer more targeted briefings on specific hazard types (e.g. cyber, supply chain), in addition to general briefings.
- Building on existing informal initiatives, briefings and information exchanges could be informed directly by key threats. The TISN can be used to identify and consider responses to key threats on a dynamic basis, align entities' and industries' threat mapping activities and guide sector or cross-sectoral responses to new trends and threats.
- Improve whole of government coordination: improved coordination between government agencies and departments would improve the responsiveness of the TISN and the effectiveness of the Critical Infrastructure Resilience Strategy. For example, showing how tactical cyber information sharing coordinated by the Australian Cyber Security Centre

(ACSC) is linked to the strategic, all-hazards resilience approach which has been TISN's traditional focus.

- Operational role: currently there is no central model to support operational responses. Query whether the TISN or another agency can take on this role. Operational coordination can include devising methods for sharing information across industries, particularly where a response may impact on other critical industries to enable those other affected critical industries to respond. For example, blocking internet traffic will require cooperation with network providers and at the same time may have significant impact for other industries.

8) What might this new TISN model look like, and what entities should be included?

There are a number of initiatives happening in this area, particularly within the JCSC, ACSC and AustCyber. It would be preferable to work alongside these initiatives and seek ways to provide centralised direction and guidance across sectors and agencies, rather than create a new program. Having multiple initiatives may hinder the process of information sharing and overcomplicate processes and requirements in this area.

The ABA note and welcome the Government's announcement on 30 June 2020, about the Cyber Enhanced Situational Awareness and Response (CESAR) package which will include investment in a new cyber threat sharing platform.

9) How else should government support critical infrastructure entities to effectively understand and manage risks, particularly in relation to cross sector dependencies? What specific activities should be the focus?

The ABA would like to have more clarity about how any PSOs or enhanced cyber obligations would apply in relation to cloud service providers, and how the Government may address risks such as concentration risk.

Many of these providers are large overseas entities and can hold unequal bargaining power. It is worth noting that the banks have experienced challenges in re-negotiating commercial contracts with outsourced providers as part of implementing new prudential regulation that would impose additional regulatory obligations on these third parties, such as the right of regulators to conduct audits of the third party. These issues can have consequences for Australian entities' ability to change contracts to comply with regulatory obligations about the cloud and/or procure these services.

As such clarity from the Government about whether these entities are directly subject to obligations under the SOCI that would be supervised by the DHA or another regulator would be helpful to a large number of entities covered by an amended SOCI and in the economy more broadly. In addition, as far as possible, enhanced obligations should be implemented under legislative instruments such as rules, rather than relying on renegotiation of commercial contracts.

10) Are the principles-based outcomes sufficiently broad to consider all aspects of security risk across sectors you are familiar with?

Yes, in relation to banks. The ABA also consider APRA prudential standards and guides provide comprehensive and detailed coverage of the principles-based outcomes.

11) Do you think the security obligations strike the best balance between providing clear expectations and the ability to customise for sectoral needs?

Yes. The ABA welcome the Government's stated approach to avoid duplication with existing regulatory obligations, and reiterate our strong view is that APRA prudential standards and guidance provide comprehensive coverage of the proposed PSOs, and sector-specific regulations should defer to the

prudential requirements. The ABA also ask the Government to consider ways to minimise duplicative reporting obligations.

12) Are organisations you are familiar with already operating in-line with these principles, or do you think there would be a significant time and/or financial cost to meet these principles?

Yes, the ABA consider banks are already operating in line with the proposed principles based on the size, scale and complexity of each entity.

Also refer our recommendation to remove duplicative reporting obligations.

13) What costs would organisations take on to meet these new obligations?

The proposed reporting obligations can impose material costs on banks as it may require designated banks to establish a new reporting regime. The reporting obligations would duplicate to a significant extent banks' existing reporting to APRA and ASIC, as such the ABA reiterate our recommendation to remove duplicative reporting obligations and extend existing information gathering mechanisms to meet these new reporting obligations.

If sector-specific regulation defers to APRA prudential standards and guidance, and if reporting obligations for critical infrastructure entities also leverage existing mechanisms to the greatest extent possible, the ABA considers there would not be significant additional cost for banks to meet these proposed obligations. If there is limited or no deference to APRA prudential standards and guidance, and/or the regime introduces duplicative or significantly enhanced reporting obligations, there can be significant additional cost to implement changes to system and technology, staff training, and potentially negotiating changes to a large number of contracts with third parties.

14) Are any sectors currently subject to a security obligation in-line with these principles? If so, what are the costs associated with meeting this obligation? Does this obligation meet all principles, or are enhancements required? If so, what?

The ABA consider that under APRA prudential standards and guidance, banks are currently subject to a high standard of obligations that are in line with these principles. Also refer our comments and recommendation about additional reporting.

15) Would the proposed regulatory model avoid duplication with existing oversight requirements?

Yes, in relation to obligations imposed under prudential standards and guidance. The ABA reiterate our comments and recommendation about removing duplicative reporting and also reiterate our offer to assist with a gap analysis of regulatory and reporting obligations.

16) The sector regulator will provide guidance to entities on how to meet their obligation. Are there particular things you would like to see included in this guidance, or broader communication and engagement strategies of the regulator?

If sector-specific regulation defers to APRA prudential standards and guidance, then the ABA consider APRA's existing guidance to be comprehensive.

If the Government considers further enhancements should be made to APRA prudential standards to meet the proposed PSOs, then the ABA would request the Government coordinate with APRA to provide clear and comprehensive guidance about what is required to meet the enhanced requirements, supported by clear guidance about how regulatory agencies will coordinate. Such guidance can be provided using APRA's existing communication channels with the sector.

17) Who would you consider is best placed to undertake the regulatory role for sectors you are familiar with? Does the regulator already have a security-related regulatory role? What might be the limitations to that organisation taking on the role?

APRA, for the reasons described above.

The ABA does not see limitations to APRA taking on this role as it is an existing function.

Also refer our interim submission relating to the directions and direct action proposals.

18) What kind of support would be beneficial for sector regulators to understand their additional responsibilities as regulators?

As above, the ABA does not consider there would be additional responsibilities for APRA. If the Government considers further enhancements are needed to APRA prudential standards, the ABA recommend the Government work with APRA to provide clarity to APRA and the sector about what is required. Any additional work could be done under existing partnerships between the financial sector regulators and the ACSC.

19) How can Government better support critical infrastructure entities in managing their security risks?

Refer to our response to question 7.

The ABA also raise three issues for further consideration:

- Whether competition law may prevent entities that are competitors from coordinating on cyber security activities or coordinating to respond to cyber threats;
- The Government's capacity to enhance engagement with and contribution to the Australian Financial Crimes Exchange (AFCX); and
- Whether there is benefit in having Government develop a list of jurisdictions which it considers have laws that have "the effect of protecting the information in a way that, overall, is at least substantially similar to the way in which the Australian Privacy Principles protect the information.

20) In the AusCheck scheme, potential and ongoing employees in the aviation, maritime, health and major national event security sectors undergo regular national security assessments by the Australian Security Intelligence Organisation and criminal history assessments to mitigate the risk of insider threats. How could this scheme or a similar model be useful in the sectors you are familiar with?

Government sharing information with private sector: If the Government wishes to share information with cleared individuals in an entity, this should be done through existing confidentiality deeds and clearances established between the entity and Government (for example within the JCSC).

Vetting of personnel: Banks have a range of existing processes for hires, including probity checks, background financial and criminal checks. These are complementary to the AusCheck scheme. Banks' processes comply with prudential and regulatory requirements such as obligations under the BEAR (and under the FAR). It will be a decision for Government and regulators whether these existing obligations are sufficient.

21) Do you have any other comments you would like to make regarding the PSO?

The ABA strongly supports giving affected industries and entities adequate time to implement and comply with any PSOs that go beyond existing regulatory requirements.

22) Do you think there are other preparatory activities that would assist in proactively identifying and remediating cyber vulnerabilities?

Refer to response to question 7, about considering threats on a dynamic basis.

The ABA also provide a specific comment about APRA prudential standard APS222, Associations with Related Entities. The ABA propose that APRA should amend APS222 paragraph 10(a) and (b) to allow a risk-based approach to uncapped liability and cross default in supply arrangements in order to permit greater enterprise wide use of a full range of cloud solutions. Disaggregation of such services in response to these requirements can make it harder for Australian based ADIs with global operations to architect their use of first tier cloud providers in a way which maximises use of Australian based data centre capacity. It also increases the risk of attackers, and complicates monitoring of, and responses to, cyber threats.

23) What information would you like to see shared with critical infrastructure by Government? What benefits would you expect from greater sharing?

The ABA welcome the initiative that the JCSC has taken to facilitate information sharing in recent cyber incidents and provide the following suggestions on potential improvements:

- Industry would benefit from a coordinated central platform or arrangement that can be used for Government to share information with industry, to facilitate industry voluntarily sharing information with Government and enable faster and more consistent responses to industry wide threats. The ABA welcome the Government's announcement on 30 June 2020 of investment in a cyber threat information sharing platform.
- For cyber threat information in particular, the ABA encourage the Government to ensure that these information sharing efforts prioritise timely (in real time wherever possible) sharing of both attack indicators and context, to give entities the best possible chance of preventing fast-moving attacks from being successful.
- This coordination can help to identify threats and risks with cross-sectoral relevance. This can be part of the proposal under question 7 for the TISN or other arrangement to consider and identify threats.
- Enhanced information sharing should at the same time address protections and security of the information shared with government, as highlighted in question 28. For example, if an entity shares information with the Government about a successful exploit, a leak or disclosure of the information can be significantly detrimental to the entity's cyber security framework.
- Government information sharing circles (ie, ASIO BLU, ACSC NIE) should include all critical infrastructure entities if practicable.
- These information sharing initiatives should encourage critical infrastructure entities and industries to aim for industry best practice and improving outcomes, rather than focus on baseline regulatory compliance.

24) What could you currently contribute to a threat picture? Would you be willing to provide that information on a voluntary basis? What would the cost implications be?

A number of banks already have strategic partnerships with Government on a voluntary basis. Under the strategic partnership, banks are providing operational data and sharing other information. The banking industry would welcome additional information from Government as to what additional material

would be valuable to contribute to a threat picture.

The ABA consider an effective approach to building a 'threat picture' is to take a framework approach rather than a documentation approach. An example of a framework approach is the Australian Criminal Intelligence Commission's report, *Organised Crime in Australia 2017*. One way to achieve this could be by producing a critical infrastructure-specific version of the ACSC's Annual Cyber Threat Report.

If there is enhanced coordination across government agencies and across all entities in critical infrastructure sectors (ie the ACSC NIE), this approach can help to build up a whole of economy single threat picture/framework.

The optimal implementation is to provide and receive information in a readily consumable form. Ideally information should be shared in a standard machine readable format which can facilitate automated analysis, response and workflow and by machines and at the same time be readable by humans where human intervention is required.

Finally, the ABA ask the Government to clarify when the Government and private sector may share information about cyber breaches that may contain personal information, to minimise delays in investigating and responding to a breach. Such sharing of information should be subject to appropriate safeguards for individuals including how any information relating to an individual can be used and for what purpose.

25) What methods should be involved to identify vulnerabilities at the perimeter of critical networks?

The ACSC already perform some scanning of Australian networks to identify vulnerabilities. Continuing this is prudent to ensure a level of hygiene amongst critical infrastructure entities.

26) What are the barriers to owners and operators acting on information alerts from Government?

The key issues to consider and address are:

- Providing context for an alert;
- The timeliness of the alert;
- A clear set of rules that enable the entity to share information within the organisation or with third party providers so the relevant teams and personnel can act on it. If the information is subject to national security restrictions it will make it very difficult for the entity to respond appropriately; and
- An entity's resourcing to respond to an alert.

The ABA also wish to highlight the need for Government to recognise that owners and operators may be best placed to determine the appropriate course of action in response to an alert.

Government vulnerability alerts and instructions may not take into account the complexity and internal controls/mitigations that an entity may have in place. Whilst certain vulnerabilities may appear to be critical from the outside, they are often mitigated or controlled using other internal measures. Enforcing action on their alerts could prove to be problematic for larger organisations. For example, forcing a bank to apply a patch could result in the bank having to take down networks which would disrupt services or move a system to a state which is not supported by its vendor. The bank may already have a mitigation control in place which means they don't need to act on the vulnerability.

The approach taken by the UK National Cyber Security Centre can be informative, particularly the findings reflected in the Vulnerability Disclosure Toolkit.

27) What information would you like to see included in playbooks? Are there any barriers to co-developing playbooks with Government?

Having a consistent approach across sectoral 'playbooks' or frameworks can help to identify cross-sectoral risks and threats. But playbooks ultimately need to be tailored to the entity as the environment and context is different for each – refer to the summary of banks' risk management, BCP and information security obligations. Also refer to response to question 24.

Barriers: the ABA draw two potential barriers or risks to the Government's attention:

- Banks receive information about risks and threats from commercial vendors. The terms of the commercial contract may constrain the information that banks can share or how information is shared. There are likely to be circumstances in which threat intelligence is provided as part of contracted services for commercial return which could be undermined if the intelligence is required to be provided more broadly.
- Information that may be shared with Government as part of these exercises will be sensitive. The release or loss of some such information to the wrong audience or at the wrong time could exacerbate the threat and/or hamper investigation activities.

The ABA also encourage the Government to consider how it can engage further with existing industry initiatives addressing cyber security, such as the AFCX.

28) What safeguards or assurances would you expect to see for information provided to Government?

The ABA consider a number of safeguards and assurances are important. These include:

- Protection for information that can expose vulnerabilities in a bank's system or in a sector. As explained in question 27, leak or disclosure of the information shared by entities can cause significant detriment. It may not be sufficient for information to be subject to classifications including national security classifications, as these still allow information sharing within an agency, and between departments and agencies. Rather, information should be subject to further controls about who can access the information and for what purpose.
- Protection for commercial confidential information. To limit the potential for unintended consequences and resistance from suppliers of potentially impacted IT Services, there should be clearly defined and limited uses to which provided information can be put.
- Clear safeguards and restrictions on which government agencies can access the information.
- Clear limitations or rules about whether such information can be used by regulators in an investigation, or in a regulatory or enforcement action.
- Where possible clear provisions dealing with sharing and use of personal information relating to non-Australian citizens or persons whose information are covered by foreign data and/or privacy regulation, such as the GDPR. Sharing of personal information of foreign citizens is problematic and will be more so if there aren't significant constraints on such Government use which ensure it is limited to threat reduction and management and is proportionate to the threat(s).

29) In what extreme situations should Government be able to take direct action in the national interest? What actions should be permissible?

Circumstances for government direct action: Government response may need to be sector specific. The key concept of 'immediate and serious cyber threat' should be clarified for all or specific sectors.

The ABA consider banks have a high level of cyber capability, have a strong history of cooperating with the government on cyber matters, and banks can be large and complex businesses. As such in relation

to banks, the ABA consider the government should be able to take direct action where the bank:

- Has consented to the government doing so; or
- Is refusing to respond to queries or requests from the Government – this should be clearly distinguished from circumstances where a bank is taking action to address and resolve an incident but there may be a difference of opinion with DHA/ASD staff about what actions are necessary.

In considering whether a direction is appropriate, the decision-maker should consider how the issue of a direction may impact on providers of shared or outsourced infrastructure who may already resist existing regulatory obligations (such as APRA's audit rights of an outsourced service provider). Where a direction may be to cease using a third party supplier, the decision-maker should consult with affected entities about impacts and consequences – these could include an entity's obligation under a foreign jurisdiction to use the specified supplier, and the time it would take to transition away from equipment supplied by one third party to equipment supplier for another party.

The details of directions should also consider, and if possible address, the issues raised in question 28.

Permissible actions: this is likely to be sector specific, as well as dependent on the size and complexity of a business.

Banks can be large and complex businesses, and parts of the bank are taking action in a range of financial markets in real time. Taking action that interrupts these actions or takes parts of a business offline can have significant flow on consequences for the bank, and by extension its customers and the financial markets. Banks would have developed disaster recovery plans taking into account these complexities. As such the ABA consider government direct action should be limited to providing advice and intel that informs the bank's decisions about how to respond to a cyber incident.

Also refer to our proposal that regulations can be used to establish sector specific regimes for government direction and direct action, noting that the *Banking Act* and other prudential legislation sets out a comprehensive set of triggers for APRA to use its directions powers and step-in powers.

The ABA also suggest:

- When the government takes direct action, legislation should ensure the Government has the same rights, vis-à-vis an outsourced provider, as the entity has under its contract. The Government's power to, in effect, step into these contracts should be in legislation rather than requiring private sector entities to seek to renegotiate contracts with a large number of third parties who may have unequal bargaining power.
- The direction action regime should address the issues raised in question 28.

Cross sectoral coordination: this is critical if the government or the entity takes action. For example, if power is to be turned off, it would be important for other key sectors to be informed as soon as practicable.

30) Who do you think should have the power to declare such an emergency? In making this declaration, who should they receive advice from first?

The ABA refer to our interim submission and ask for flexibility under legislation, to give Government, regulators and industry more time to consider the appropriate regulatory and coordination arrangements. This would include the roles, responsibilities and coordination arrangements vis-à-vis APRA and the RBA.

31) Who should oversee the Government's use of these powers?

The ABA refer to our interim submission which proposes further consideration of the appropriate regulatory arrangements. Actions taken by APRA and other regulators are subject to merits review and

judicial review, and the ABA ask that merits review and judicial review also apply to the use of these powers.

32) If, in an exceptional circumstance, Government needs to disrupt the perpetrator to stop a cyber attack, do you think there should be different actions for attackers depending on their location?

N/A.

33) What sort of legal protections should officers (both industry and Government) undertaking emergency actions be afforded?

The ABA consider the following are important:

- Protection from civil and criminal action or any regulatory action, the fact of the bank taking action should not be able to be used in regulatory investigations.
- Protection from liability under contract.
- Protection from liability in relation to obligations to customers.
- Protection from class action, shareholder action.
- Whether protections are needed under corporate law and markets regulation, for example directors duties, continuous disclosure obligations.
- Protection from liability under competition law, to the extent sectoral or cross-sectoral coordination is required.

The ABA also highlight there would be implications for bank's insurance cover, and a range of legal and regulatory risk that cannot be addressed under Australian law: liability under overseas laws such as GDPR, potential breach of overseas regulatory obligations, overseas class action. Note APRA's directions powers and step-in powers have provisions dealing with some of these matters.

34) What safeguards and oversight measures would you expect to ensure the necessary level of accountability for these types of powers?

The ABA consider strong safeguards would be needed before these powers are exercised:

- Clear obligation to notify the entity and provide a meaningful period of time for entity to respond before a decision is taken.
- Clear obligation to request and consider advice from sector regulators such as APRA and RBA.

It will be important to have safeguards *before* a power is exercised, rather than review after the fact.

35) What are the risks to industry? What are the costs and how can we overcome them? Are there sovereign risks to investment that we should be aware of?

The ABA refer to our response to question 33 and question 13 about costs. The ABA also note there is a risk that certain IT providers with global scale may perceive particular Government powers (such as direct action) as creating an unacceptable risk and decline to provide services to critical infrastructure entities.

36) Does this mix of obligations and assistance reflect the roles and responsibilities of Government and industry in protecting critical infrastructure? How would private sector management of risk

change with the proposed increased role for Government?

The ABA considers that a greater role for the government under an enforceable regulatory regime is likely to cause private sector entities to have a greater focus on compliance with new regulatory and reporting obligations. It would be important for the government to encourage entities in all critical infrastructure industries to adopt industry best practice and improving outcomes, rather than focus on baseline regulatory compliance.

Building on response to question 29, many banks, and large entities in other critical infrastructure industries, are complex entities with highly interdependent networks and business models. It would be important for any government direct action to work with and strengthen the entities' own disaster recovery capabilities and planning wherever possible,

This also highlights the benefits of initially focusing on enhancing voluntary information sharing, before considering imposing any mandatory information sharing obligations. As described above, this approach has been successfully used in the United Kingdom to establish successful government-private sector coordination.