Australian Banking Association

Interim submission: Protection of critical infrastructure and systems of national significance

Summary

The Australian Banking Association (**ABA**) supports the Government having the capability to provide direct assistance to private sector entities on critical cyber matters.

We also strongly support the Government's desire to avoid duplication of regulation. A harmonised approach, where a single regulator has a clear mandate and a transparent system in place for regulatory co-ordination, is critical to the success of any direct assistance regime.

We would like to highlight that the Australian Prudential Regulation Authority (**APRA**) has comprehensive prudential regulation dealing with operational resilience, cyber resilience and managing risks including outsourcing and supply chain risks. These regulations are supervised and enforced by APRA's powers to issue directions and take direct action.

We propose the *Security of Critical Infrastructure Act 2018* (**SOCI Act**) give Government the ability to create tailored direct assistance regimes. This will enable Government and industry to undertake a gap analysis to determine the respective roles of the Australian Signals Directorate (**ASD**) and APRA, provide clarity of mandates and avoid regulatory duplication.

This can be done by adding a regulations-making power in the SOCI Act that allows for tailored provisions governing the direct assistance regime to be established for specific sectors as necessary.

Explanation

APRA prudential regulation

APRA has issued prudential regulations that address the proposed positive security obligations. Many of these apply to all APRA-regulated entities. Prudential standards include:

- CPS 220 risk management
- CPS 231 outsourcing
- CPS 232 business continuity management
- CPS 234 information security

Prudential guidance include 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.

In particular, under the banking sector accountability regime (**BEAR**), a bank is required to register executives who have accountability for specified areas. These include overall risk controls and risk management, and information management including information technology systems.

APRA enforcement and directions powers

APRA's prudential regulation is enforced by a comprehensive set of supervision, enforcement and resolution powers. APRA has stated that it 'seeks to identify prudential risks proactively and take action to prevent harm before it occurs', but it will 'act quickly and forcefully' to address risks including risks 'due to a lack of cooperation from an entity or individual.'

These powers can be exercised in anticipation of an event rather than after the fact.

- APRA can compulsorily require information and data from a bank.
- APRA can disqualify an accountable person under the BEAR, and can apply to the Federal

Court to disqualify other persons in the bank.

- APRA has a comprehensive directions power, and failure to comply with an APRA direction is an offence and can be a continuing offence. The *Banking Act 1959* (**Banking Act**) prevents another party closing out or refusing to perform under a contract merely because a direction has been issued. APRA can direct entities to take or cease particular actions if APRA is satisfied of broad triggers including:
    - the body corporate has contravened a prudential requirement regulation or standard
    - the direction is necessary in the interests of the depositors of the bank
    - there is, or there might be, a material risk to the security of the body corporate's assets
    - the failure to issue a direction would materially prejudice the interests of the depositors of the bank
    - the body corporate is conducting its affairs in a way that may cause or promote instability in the Australian financial system
- APRA has an ongoing supervision program ensuring that these prudential standards are being implemented and operated appropriately, and can impose additional capital charges when further risks are identified.
- APRA has broad powers to take control of a bank's business, or to appoint a statutory manager to do so. The statutory manager can require information from a person and it is an offence to refuse to comply. The Banking Act prevents another party from closing out or refusing to perform under a contract merely because APRA has taken control or a statutory manager has been appointed. Once appointed, a statutory manager has powers and functions of the members of the board of directors of the bank (collectively and individually).

Regulatory coordination

The Council of Financial Regulators (**CFR**, consisting of Treasury, APRA, RBA and ASIC) have existing partnerships with the Department of Home Affairs and the Australian Cyber Security Centre (**ACSC**), including but not limited to the CFR cyber security working group. Cybersecurity preparatory exercises is already proposed by the CFR under the Cyber Operational Resilience Intel-led Exercises (**CORIE**) framework.

During a cyber incident, a bank would already work closely and consult with APRA to address, isolate and resolve the incident. This would usually involve a close partner engagement with the local Joint Cyber Security Centres (**JCSC**) and/or the ACSC to support effective incident resolution.

These examples highlight the need to do a gap analysis and provide clarity on regulatory mandates.

Proposal: tailored regime that ensures clear mandate and regulatory coordination

The ABA proposes that Government create a regulation-making power in the SOCI Act enabling enhanced cyber security obligations and direct assistance obligations to be tailored in such a way that avoids duplication with existing regulatory obligations that apply to a particular sector. This would give Government and industry time to conduct a gap analysis of when and the types of direct action that may be taken, and what sectoral regulators can already do 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 the process and responsibility for coordination between regulatory agencies.

We reiterate that, when there is a serious cyber incident, it will be critical to have one regulator with a clear mandate and capability to take the actions necessary. Coordinating actions in the event of a serious cyber event would be critical to a rapid response. It is also critical to connect banks with the right government support – this requires capability and an understanding of the broader financial

system.

If there were two regulators taking action on an incident, operationally this significantly increases the risk of inconsistent advice or directions, delay in taking action due to differences of opinion between regulators, or even conflicting requirements being imposed on a bank.

The flexibility to create a tailored regime can also be used to allow a bank to proactively accept assistance from Government. It would also give industry more clarity on consequential questions like insurance, liability under contracts, impact on other regulatory obligations, continuous disclosure (details to be provided in full ABA submission).