

16 September 2020

Critical Infrastructure Centre  
Department of Home Affairs  
3-5 National Circuit  
BARTON ACT 2600

*Submitted via online form*

Dear Sir/Madam

### **Protecting Critical Infrastructure and Systems of National Significance**

The Customer Owned Banking Association (COBA) appreciates the opportunity to respond to the Department's August 2020 consultation paper *Protecting Critical Infrastructure and Systems of National Significance*.

COBA is the industry association for Australia's customer owned banking institutions (mutual banks, credit unions and building societies). Collectively, our sector has \$139 billion in assets, around 10 per cent of the household deposits market and more than 4 million customers. Customer owned banking institutions account for around three quarters of the total number of domestic banking institutions and deliver competition and market leading levels of customer satisfaction in the retail banking market.

COBA supports sensible measures to protect Australia's critical infrastructure and systems. The functioning of Australia's banking system is dependent on a secure cyber environment. Our members appreciate the risk posed by the evolving nature of cybercrime and responding to this risk is a high priority for our sector. Our members dedicate considerable resources towards maintaining and developing defences, and ensuring they are compliant with existing cyber security obligations under the various frameworks.

#### **Key points**

- 1. COBA members, like all Authorised Deposit-taking Institutions (ADIs), are subject to extensive prudential regulatory requirements, including legally-enforceable prudential standards that specifically address risk management, business continuity management and information security, including cyber attacks. This risk-management framework is administered and enforced by a powerful and well-resourced regulator, i.e. APRA, which is proactive and has strong oversight and intervention powers for the banking and financial services sector. This existing regime for ADIs already delivers the objectives of the proposed Positive Security Obligation, i.e. to identify and understand risk, to mitigate risk and prevent incidents, to minimise the impact of incidents and to promote effective governance.**
- 2. In addition to these legally-enforceable prudential standards, APRA has dedicated considerable strategic focus to the improvement of cyber resilience across the financial system.**
- 3. APRA enforces accountability obligations for ADIs and their senior executives and directors under the Banking Executive Accountability Regime (BEAR). These**

Suite 403, Level 4, 151 Castlereagh Street,  
Sydney NSW 2000

Suite 4C, 16 National Circuit,  
Barton ACT 2600

- obligations specifically cover risk controls and risk management of the ADI, and information management of the ADI, including information technology systems.**
- 4. COBA supports the approach of explicitly recognising existing regulatory regimes in new regulatory frameworks when the existing regime is achieving the same objectives. This approach is seen in the *Corporations Act 2001 (Cth)*, the *National Consumer Credit Protection Act 2009 (Cth)* and the Consumer Data Right framework.**
  - 5. The customer owned banking sector provides important competition and choice in the retail banking market but individual customer owned banking institutions are very small compared to major banks. The entire sector comprising 64 ADIs is considerably smaller than each of the major banks.**
  - 6. A major concern of COBA members and a key factor influencing the competitive capacity of small players in the banking market is the regulatory compliance burden. The fixed costs of complying with regulation fall more heavily on smaller firms. Regulation should be targeted, proportionate, risk-based and, where possible, graduated.**
  - 7. COBA understands that new regulatory obligations under this regime could commence in mid-2021. If new regulatory obligations are to apply to COBA members, this timeframe is inadequate. All banking institutions are currently focused on managing the challenges of the pandemic and economic downturn and the needs of customers in hardship. The development and implementation of any new regulatory obligations must take into account this environment and avoid diverting scarce resources away from acute customer needs.**

### **Importance of partnership approach**

We recognise the important role Government can take towards increasing cyber resilience with all Australians and we strongly support the theme that cyber security is a shared risk between government and the entire community of Australians.

COBA appreciates that the 2020 Cyber Security Strategy is the largest ever Australian Government financial commitment to cyber security and builds on the strong foundations from previous 2016 strategy.

At a time when more Australians are working from home than ever before we congratulate the Government on the commitment to invest \$1.67 billion to build new cyber security and law enforcement capabilities and protect the essential services upon which we all depend.

COBA and its members support the uplift of Australian Cybersecurity Centres and Joint Cyber Security Centres nationally of which we have been actively partnering with since rollout. In particular, we note increased funding for law enforcement to target and disrupt offshore cybercrime activity that affects all Australians.

Some key initiatives that have benefitted COBA members include:

- Introduction of a Cyber Security National Workforce Growth Program to actively assist businesses and academia to grow the cyber skilled workforce to benefit all Australians
- Strengthening law enforcement's counter-cybercrime capabilities with investment for law enforcement agencies to bolster their ability to actively target cyber criminals and their profits
- Direct funding of a new ACSC partner portal and threat-sharing platform
- The 24/7 cyber security hotline that will enable victims of cybercrime to call and receive advice
- Increased resources for ACSC and JCSC to support businesses of all sizes with improved threat intelligence

- The allocation of \$6.1 million in funding to support psychological services for victims of identity fraud through iDCare
- The Telstra Clean Pipes initiative work to see malware blocked at scale at the source
- Allocation of funding to support education and awareness campaigns for vulnerable persons and the elderly on Cybercrime to help protect themselves and raise the community's understanding of how to be secure online, and
- The recent introduction of a voluntary Internet of Things Code of Practice to help consumers make informed purchasing decisions.

COBA and its members will continue to work alongside the Government in reaching its cyber security objectives.

### **Proposed enhanced regulatory framework**

The Department has proposed an enhanced regulatory framework under the existing *Security of Critical Infrastructure Act (2018)* that will look to introduce:

1. A positive security obligation (PSO) for critical infrastructure entities, supported by sector-specific requirements
2. Enhanced cyber security obligations for those entities most important to the nation, and
3. Government assistance to entities in response to significant cyber attacks on Australian systems.

Under the PSO, critical infrastructure entities will be required to meet the following principles-based outcomes:

- Identify and understand risks
- Mitigate risks to prevent incidents
- Minimise the impact of realised incidents, and
- Effective governance.

We note the Department is seeking to establish a cohesive partnership between Government and industry, recognising that one size does not fit all across the various sectors it has deemed as critical. The proposed legislative amendments look to develop “proportionate requirements that strike a balance between uplifting security and ensuring businesses remain viable and services remain sustainable, accessible and affordable”.<sup>1</sup> The new requirements intend to build on and not duplicate existing regulatory frameworks.

The relevant existing regulatory framework for COBA members is APRA's prudential supervisory regime for ADIs. ADIs range from major banks to small credit unions. All COBA members are ADIs.

COBA members, like all ADIs, are subject to extensive prudential regulatory requirements, including legally-enforceable prudential standards that specifically address:

- Risk management
- Business continuity management, and

---

<sup>1</sup> <https://www.homeaffairs.gov.au/reports-and-pubs/files/protecting-critical-infrastructure-systems-consultation-paper.pdf>

- Information security, including cyber attacks.

This risk-management framework is administered and enforced by a powerful and well-resourced regulator, i.e. APRA, which is proactive and has strong oversight and intervention powers for the banking and financial services sector.

Leaving aside the question of which entities will be defined as critical infrastructure entities for the purposes of the enhanced regulatory framework, this existing regime for ADIs already delivers the objectives of the PSO, i.e. to identify and understand risk, to mitigate risk and prevent incidents, to minimise the impact of incidents and to promote effective governance.

### **Current regulatory framework for COBA members**

In the consultation paper, the Department recognises that the banking and financial services sector is already subject to rigorous regulatory frameworks that impose risk management, reporting and transparency obligations. It highlighted that regulators in the banking and financial services sector are already equipped to supervise entities, identify emerging threats, and assist regulated entities respond to those threats.<sup>2</sup>

As noted above, APRA is a proactive regulator with strong oversight and intervention powers for the banking and financial services sector.

A number of the prudential standards also impose personal liability on key personnel within the ADI organisations, ensuring that accountability and responsibility is upheld by the respective businesses.

APRA's existing regulatory framework covering cyber risk is rigorous, sophisticated and operating effectively for the banking and financial services sector.

In addition to setting legally-enforceable prudential standards, APRA has dedicated considerable strategic focus to the improvement of cyber resilience across the financial system. In its 2019-20 Corporate Plan, APRA provided a timeline for its work program on this priority, with the implementation of new supervision practices to assess cyber resilience set to come into place from late 2020 and in the first half of 2021. Prior to COVID-19, APRA set the goal of uplifting industry practice to manage cyber risk to be implemented in the first half of 2022.<sup>3</sup>

As part of the 2019-23 Corporate Plan, APRA highlighted plans to:

*“Using data driven insights to interrogate cyber resilience data to prioritise and tailor supervisory activities. In the longer term, this will inform baseline metrics against which APRA regulated institutions will be benchmarked and held to account for maintaining sound cyber defences.*

*“Collaborating with peer regulatory agencies for better cyber resilience outcomes, including by executing the work plan of the Council of Financial Regulators Cyber Security Working Group, and engaging with other agencies, international peers and industry experts”.*<sup>4</sup>

Despite shifting circumstances due to COVID-19, APRA renewed its focus on financial system resilience and improving cyber resilience across the financial system in its 2020-24 Corporate Plan.<sup>5</sup>

---

<sup>2</sup> <https://www.homeaffairs.gov.au/reports-and-pubs/files/protecting-critical-infrastructure-systems-consultation-paper.pdf>

<sup>3</sup> <https://www.apra.gov.au/news-and-publications/apra-releases-2019-2023-corporate-plan>

<sup>4</sup> <https://www.apra.gov.au/news-and-publications/apra-releases-2019-2023-corporate-plan>

<sup>5</sup> <https://www.apra.gov.au/sites/default/files/2020-08/APRA%27s%202020-24%20Corporate%20Plan.pdf>

## **APRA prudential standards relating to risk**

We list below the key prudential standards and prudential guides that ADIs must comply with that align with the objectives of the PSO.

### ***Risk Management (CPS 220)***

*Requires an APRA-regulated institution and a Head of a group to have systems for identifying, measuring, evaluating, monitoring, reporting, and controlling or mitigating material risks that may affect its ability, or the ability of the group it heads, to meet its obligations to depositors and/or policyholders. These systems, together with the structures, policies, processes and people supporting them, comprise an institution's or group's risk management framework.*

### ***Outsourcing (CPS 231)***

*Requires 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, approval and ongoing monitoring. All risks arising from outsourcing material business activities must be appropriately managed to ensure that the APRA-regulated institution, or the group it heads, is able to meet its financial and service obligations to its depositors and/or policyholders.*

### ***Business Continuity Management (CPS 232)***

*Requires each APRA-regulated institution and Head of a group to implement a whole-of-business approach to business continuity management that is appropriate to the nature and scale of the operations. Business continuity management increases resilience to business disruption arising from internal and external events and may reduce the impact on the institution's or group's business operations, reputation, profitability, depositors, policyholders and other stakeholders.*

### ***Pandemic Planning (CPG 233)***

*Guidance for regulated institutions in considering and prudentially managing the risks posed by a potential pandemic, supporting the institution's compliance with the Prudential Standard on Business Continuity Management (CPS 232).*

### ***Information Security (CPS 234)***

*Aims to ensure that an APRA-regulated entity takes measures to be resilient against information security incidents (including cyber-attacks) by maintaining an information security capability commensurate with information security vulnerabilities and threats.*

### ***Managing Data Risk (CPG 235)***

*Guidance for regulated entities in managing data risks, targeting senior management, risk management and technical specialists. This guidance targets areas where APRA continues to identify weaknesses as part of its ongoing supervisory activities.*

## **Executive accountability**

APRA also enforces accountability obligations for ADIs and their senior executives and directors under the Banking Executive Accountability Regime (BEAR).

Under BEAR, an individual is identified as an "accountable person" where serving as a member of the board of the ADI or holding senior executive responsibility for one of the listed particular responsibilities, including management of the overall business activities of the ADI, overall risk controls

and risk management of the ADI, and information management of the ADI, including information technology systems.

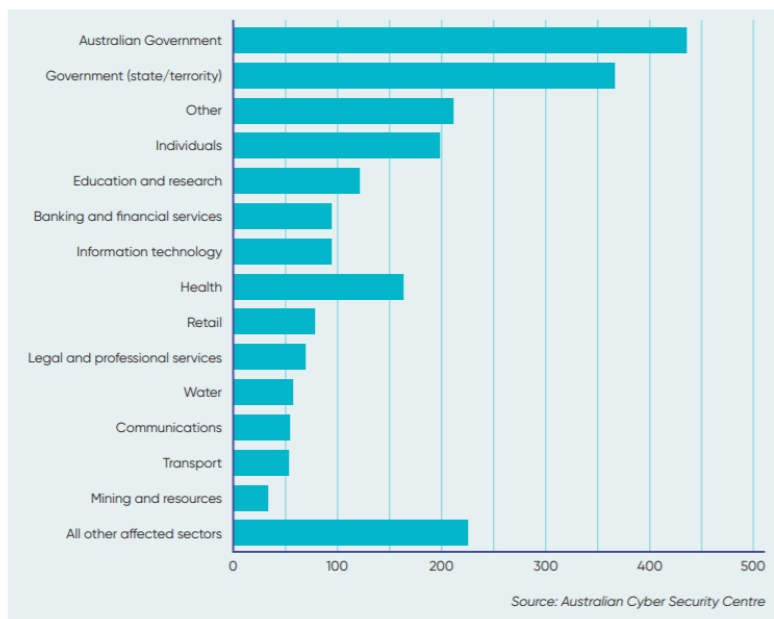
The existing BEAR measures are to be expanded to cover all APRA-regulated entities under a broader Financial Accountability Regime (FAR).<sup>6</sup> In addition to the existing responsibilities, FAR proposes to introduce a new obligation requiring accountable persons to take reasonable steps to ensure that entities comply with their licensing obligations. FAR will also see ASIC provide joint administration of the regime as the conduct regulator.

**Effectiveness of the current regulatory regime for banking and financial services sector**

Drawing on COBA and its member’s experience with the current regulatory framework and the downward trend in banking fraud rates, current measures are effectively responding to cyber risks and limiting the number of system disruptions.

Based on data from the Australian Cyber Security Centre, included in the Australia’s Cyber Security Strategy 2020,<sup>7</sup> the banking and financial services sector recorded less than 100 cyber security incidents from 1 July 2019 to 30 June 2020 (see Figure 1 below)The banking and financial services sector faced far fewer incidents than the Australian and state and territory governments, as well as other major sectors such as healthcare and education. This performance reflects the sustained efforts by the regulators and industry participants to identify, mitigate and manage cyber risk as part of their day-to-day operations.

Figure 1: Cyber security incidents, by sector (1 July 2019 to 30 June 2020)



**RBA focus on payments system resilience**

The Reserve Bank of Australia (RBA), as payments system regulator, noted in June<sup>8</sup> that during the COVID-19 period, the electronic payment system has had very few severe outages (despite the need for providers to quickly adopt different working arrangements).

<sup>6</sup> <https://treasury.gov.au/consultation/c2020-24974>

<sup>7</sup> <https://www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-strategy-2020.pdf>

<sup>8</sup> <https://www.rba.gov.au/speeches/2020/sp-ag-2020-06-03.html>

RBA Assistant Governor Michele Bullock welcome this outcome:

*“Given the reduced use of cash during this period, it could have been even more difficult for merchants were there to be disruptions to the electronic payment system. And in the circumstances a loss of access to funds could have caused harm to customers and dented confidence within the community. But this episode does highlight something we have been concerned about for some time – the importance of the resilience of the retail payments system.*

*“The Bank has already been working with the industry and APRA to develop a set of standard operational performance statistics to be disclosed by individual institutions. The proposed disclosures are intended to focus the minds of banks' executives and directors and ensure that appropriate attention is paid to the reliability of their retail payment services. They will also provide customers with transparency about the operational performance of different institutions.”*

This is another example of where risks to be targeted by the PSO are being managed in the banking sector by an existing regulator and, in this case, existing regulators working together.

COBA encourages the Department to factor this into its design of the critical infrastructure regime.

### **Recognising existing regulatory regimes**

COBA supports the mechanism of explicitly recognising existing regulatory regimes in new regulatory frameworks when the existing regime is achieving the same objectives.

This approach is seen in the *Corporations Act 2001 (Cth)*, the *National Consumer Credit Protection Act 2009 (Cth)* and the Consumer Data Right framework. These regimes recognise the status of ADIs and the requirements imposed by APRA and accepts these requirements rather than duplicating them for Australian Financial Services Licensees, Australian Credit Licensees and Accredited Data Recipients.

Under the s912A(1)(d) of the *Corporations Act*, AFS licensees are expected to have adequate financial, technology and human resources to provide the financial services covered by the license and to establish and maintain adequate risk management systems. These obligations do not apply to entities that are otherwise regulated by APRA,<sup>9</sup> effectively tailoring AFS licensee obligations to account for existing obligations for APRA regulated entities such as ADIs.

Similar treatment is given to ADIs under the *National Consumer Credit Protection Act*.

Under the ACCC's Consumer Data Right regime, banking sector participants are entitled to streamlined accreditation<sup>10</sup> as data recipients based on their existing authorisation from APRA as ADIs.

This approach would significantly reduce potential regulatory duplication for our members and acknowledge the existing regulatory regime overseen by APRA. In our view, it would also support the Department in reaching their positive security obligation objectives proposed as part of this consultation.

### **About the customer owned banking sector**

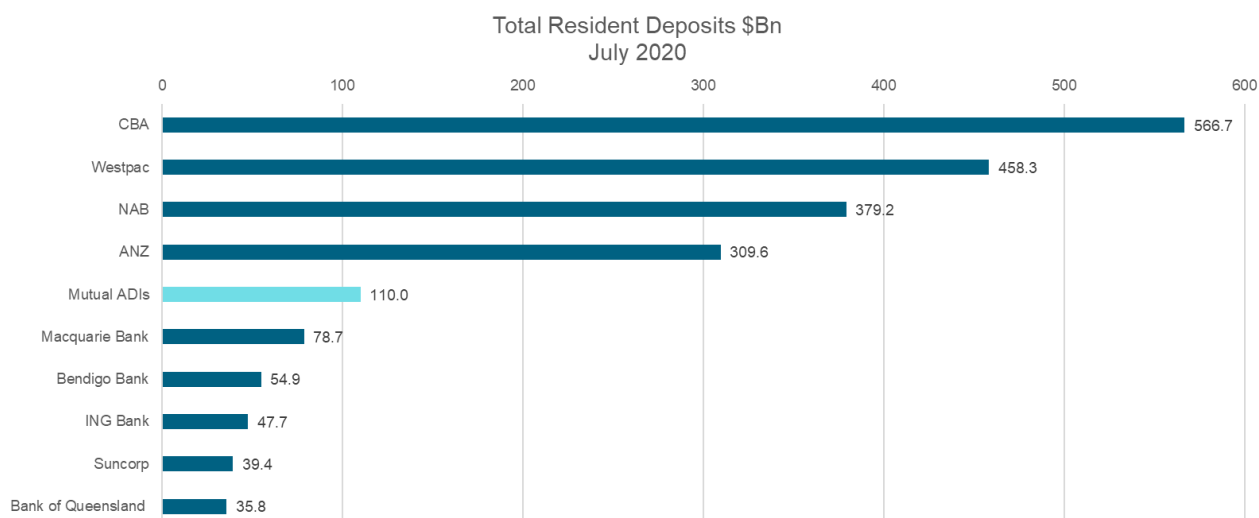
The customer owned banking sector provides important competition and choice in the retail banking market but individual customer owned banking institutions are very small compared to major banks. As

---

<sup>9</sup> <https://asic.gov.au/regulatory-resources/find-a-document/regulatory-guides/rg-104-licensing-meeting-the-general-obligations/>

<sup>10</sup> <https://www.accc.gov.au/system/files/CDR%20Rules%20Explanatory%20Statement%20-%206%20February%202020.pdf>

illustrated by the chart below, the entire mutual ADI sector comprising 64 ADIs is considerably smaller than each of the major banks.



(Source, APRA Monthly Banking Statistics July 2020)

This is an important observation in the context of defining a 'regulated critical infrastructure entity' and distinguishing between such entities and 'critical infrastructure entities'.

To obtain economies of scale, individual customer owned banking institutions rely on outsourcing of commercial services such as access to the payments system, core banking systems, data processing and other information technology requirements.

COBA members have recently undertaken significant efforts with their key suppliers in conjunction with APRA to comply with the new Information Security prudential standard, CPS 234. The objective of CPS 234 is to minimise the likelihood and impact of information security incidents on the confidentiality, integrity or availability of information assets, including information assets managed by related parties or third parties.

Under CPS 234, the Board of an ADI is ultimately responsible for ensuring that the entity maintains its information security. The key requirements of this prudential standard are that an APRA-regulated entity must:

- Clearly define the information security-related roles and responsibilities of the Board, senior management, governing bodies and individuals
- Maintain an information security capability commensurate with the size and extent of threats to its information assets, and which enables the continued sound operation of the entity
- Implement controls to protect its information assets commensurate with the criticality and sensitivity of those information assets, and undertake systematic testing and assurance regarding the effectiveness of those controls, and
- Notify APRA of material information security incidents.

### Proportionate regulation

A major concern of our members and a key factor influencing the competitive capacity of smaller challengers in the banking sector is the regulatory compliance burden. The fixed costs of complying with regulation fall more heavily on smaller firms.



The regulatory compliance burden provides yet another advantage to major banks because they can spread their costs over a vastly bigger revenue base. Regulation should be targeted, proportionate, risk-based and, where possible, graduated.

Decisions to impose new regulation should be co-ordinated and the cumulative impact should be assessed. Seen in isolation, a particular regulatory measure may appear relatively benign but the continual introduction of new measures can amount to death by a thousand cuts to smaller players in the market.

COBA supports the Department's intention to develop proportionate requirements that strike a balance between uplifting security and ensuring businesses remain viable and sustainable, accessible and affordable.

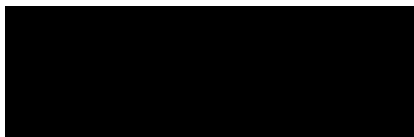
### **Cost of regulation and time constraints**

COBA understands that following this consultation, the Department is working towards the introduction of legislation into Parliament before the end of 2020, with the sector specific standards expected to be designed from later 2020 and into 2021. The obligations are expected to take effect in mid-2021.<sup>11</sup>

If new regulatory obligations are to apply to COBA members, this timeframe is inadequate. All banking institutions are currently focused on managing the challenges of the pandemic and economic downturn and the needs of customers in hardship. The development and implementation of any new regulatory obligations must take into account this environment and avoid diverting scarce resources away from acute customer needs.

COBA looks forward to working with the Department on the enhancement of cyber security and protecting critical infrastructure. Please do not hesitate to contact Luke Lawler, Director – Policy, on [REDACTED] if you wish to discuss any aspect of this submission.

Yours sincerely



**MICHAEL LAWRENCE**

**Chief Executive Officer**

---

<sup>11</sup> <https://www.homeaffairs.gov.au/reports-and-pubs/files/protecting-critical-infrastructure-systems-consultation-paper.pdf>