Australian Banking Association

14 April 2023

Department of Home Affairs

101 George Street

Paramatta NSW 2150

Submitted via Department of Home Affairs' webform page: https://www.homeaffairs.gov.au/reports-and-publications/submissions-and-discussion-papers/2023-2030-australian-cyber-security-strategy-discussion-paper/cyber-security-strategy-discussion-form

Also submitted via email: auscyberstrategy@homeaffairs.gov.au

**Submitted 14 April 2023**

# 2023 – 2030 AUSTRALIAN CYBER SECURITY STRATEGY

The Australian Banking Association (**ABA**) welcomes the opportunity to respond to the Department of Home Affairs' consultation on the development of the 2023-2030 Australian Cyber Security Strategy (**the Strategy**).

As the consultation paper notes, Australia faces an increasingly complex cybersecurity environment with new and more challenging cyber threats impacting government and businesses of all sizes alike. Meanwhile, the ongoing series of significant cyber incidents and data breaches provides irrefutable evidence that Australia's capacity to both prevent and respond to cyber events are not consistently effective.

ABA Member banks are supportive of the overall objectives of the proposed Strategy, in particular the emphasis upon a "Team Australia" approach where individual organisations are encouraged and supported to work closely together to strengthen Australia's cyber resilience and response capability.

A consistent focus throughout the 2023-2030 strategy period on cyber resilience capability building offers a clear pathway to achieving the goal of making Australia the most cyber secure nation in the world. A robust and widely available Digital Identity (**Digital ID**) capability could be the anchor for a new, secure-by-design approach to cyber resilience that provides a technological solution to issues such as privacy protection obligations and document retention. A smarter technological pathway should, over time, mitigate the need to collect and store personal and sensitive information about individuals, including government-issued identity documents. Legislative reform (including the Privacy Act) will nonetheless be required to simplify and update obligations covering decades of legacy data.

This medium-term focus must, of course, be balanced with the opportunity to prioritise short-term improvements in the regulatory environment to streamline compliance obligations and enable business stakeholders to direct scarce resources to actual cyber resilience capability. A two-way 'single door' approach to cyber incident reporting is likely to be the low-hanging fruit in the immediate term.

## Our Views

In addition to our response to the specific consultation questions, the ABA proposes the following key themes to guide the development of the Strategy.

1. Accelerated rollout of a robust and widely used Digital ID capability is the essential anchor of a fundamentally strong cyber security eco system. This capability should link both existing government and trusted private sector capabilities in a consistent and interoperable framework and remove any obligation for organisations to store highly sensitive ID information beyond initial ID verification. Focusing on the widespread adoption of a trusted Digital ID would bring Australia into line with leading jurisdictions including the European Union, which has mandated a 2024 start date for an EU wide digital identity wallet capability to every citizen who wants one, with

the objective of achieving 80% adoption by 2030. Five European countries, Canada and India already have between 30 per cent and over 90 per cent adoption of Digital ID.

2. Consolidation of cyber and data security incident reporting requirements through a 'single door' is an important step in easing the compliance burden on business and enabling a greater share of scarce resources to be directed toward strengthening actual cyber resilience capability. The 'single door' should operate in two directions to streamline both communications to regulators and requests for information from regulators and government departments.
3. A wider review of overlapping cyber security, privacy, and AML/CTF obligations should be undertaken with the objective of streamlining and consolidating the underlying compliance obligations. The trigger events, timeframes, and reporting requirements should be aligned.
4. The outcomes of the Privacy Act Review which is currently underway should be aligned with the Cyber Security Strategy. In general, this should be optimised toward creating confidence to delete personal information as quickly as possible, rather than creating penalties for storing that data (which may otherwise be in tension with record retention obligations). The review should examine opportunities to remove unintended impediments to co-ordinated action to help mitigate the impact of cyber security breaches on affected individuals. The complexity and inconsistency of document retention obligations in various legislation (e.g., AML/CTF Act) and the overriding requirements for deletion of personal information under the Privacy Act should be clarified and minimised. The proliferation of retained data may be driven as much (if not more) by numerous and far-reaching liability rules than the complexity and number of specific retention rules.
5. Strengthening the cyber resilience capabilities of small and medium businesses is essential to securing the overall data ecosystem. Any additional cyber security obligations impacting SME businesses should be carefully developed to minimise compliance burdens and should only be imposed upon SME businesses as a last step. Access to a secure Digital ID infrastructure supported by education and resources to build capability are likely to be more effective than regulation alone – and may, in certain circumstances, reduce the need for regulation. Consideration should be given to enhancing the capability and obligations of cloud computing service providers (including cloud hosting and cloud software service providers) as a more effective point for consistent capability uplift. In general, the Government should introduce measures aimed at increasing the cyber security capability of businesses that supply technology products and services to Australian businesses. This is preferable to Government placing additional regulatory responsibility for the security of these third-party products and services on Australian businesses.
6. Developing a voluntary cyber security accreditation regime that includes an ongoing audit process for small to medium size businesses will provide a clear pathway for such organisations to lift capability. It will allow them a single mechanism to demonstrate their cyber security risk management capability to larger organisations, such as banks when assessing their supply chain requirements under the Australian Prudential Regulation Authority's (**APRA's**) CPS234 Information Security (**CPS234**), when participating in procurement processes without the overhead of multiple due diligence requirements.
7. Appropriately designed safe harbour mechanisms should be implemented to facilitate and encourage businesses impacted by a cyber incident to seek prompt support from specialist government resources such as the Australian Cyber Security Centre (**ACSC**). There may be a reluctance to engage as openly and constructively as possible with the ACSC or other government agencies given the current level of focus on liability frameworks and follow-on regulatory and litigation risks. To address this, there should be a priority on removing barriers to swift collaboration, communication, and response. The model needs to be consistent with the 'single door' reporting approach.
8. The sustained effort on cyber capability building through to 2030 should be supplemented and given clear focus by identification of three implementation horizons. This will allow early delivery of short-term capability enhancements while ensuring appropriate focus is also given to medium- and longer-term opportunities.

## Responses to Consultation Questions

**1. What ideas would you like to see included in the Strategy to make Australia the most cyber secure nation in the world by 2030?**

ABA Member banks propose the following key ideas for inclusion in the Strategy:

- Design a fundamentally stronger cyber security ecosystem around a robust and widely used Digital ID model linking both government and trusted private sector capabilities in a consistent and interoperable framework.
- Consolidate data (including personal information) and cyber incident reporting obligations through a two-way 'single door'.
- Streamline existing cyber security obligations to provide consistency and clarity across multiple regulators.
- Remove Privacy Act constraints on sharing details of affected customers for co-ordinated action between government and across industry sectors to mitigate the impact of cyber security breaches on impacted customers.
- Enhance the capability of the Document Verification Service (**DVS**) to consider providing tokenised identity credentials post-verification, and act as a consolidated reference source of information for credentials compromised in a cyber or data incident. This should include a review of the DVS charging model.
- Strengthen the role and obligations of cloud computing service providers (including cloud hosting and cloud software service providers) as the most effective point of intervention to assist SME businesses to enhance their cyber security capabilities.
- Develop a voluntary cyber security accreditation regime for SME businesses to uplift capability and provide evidence of capability when participating in supply chain processes.
- Implement safe harbour mechanisms to facilitate and encourage businesses impacted by a cyber incident to reach out for support to specialist government resources such as the ACSC.
- Enhance and expand involvement of critical infrastructure entities in the Cyber Threat Intelligence Sharing program and ACSC National Intelligence Exchange. Models implemented by other Governments, particularly the UK and US, should also be considered (e.g., the UK NCSC's Industry 100 program).
- Support the essential expansion of the cyber security workforce through the streamlining of visa application processes to ensure Australia has the best chance in a global competition for securing and retaining talent.
- Implement broader skills, education, and training reforms including both tertiary education and micro-credentialling programs to support currently employed individuals to transition to new roles in cybersecurity, while attracting and retaining new talent to this sector.
- Encourage development and roll-out of machine learning and AI capabilities to enhance cyber detection and minimise the probable cyber skills gap.

**2. What legislative or regulatory reforms should Government pursue to enhance cyber resilience across the digital economy?**

**a. What is the appropriate mechanism for reforms to improve mandatory operational cyber security standards across the economy (e.g., legislation, regulation, or further regulatory guidance)?**

Many industry sectors already have industry-specific cyber security obligations with larger players also often subject to Security of Critical Infrastructure Act (**the Act**) requirements. Legislative or regulatory reform should initially at least focus on clarifying and harmonizing overlapping obligations.

Mandatory cyber security standards should only be rarely and judiciously deployed where there is clear evidence of a consistent capability deficiency that is not responding effectively to other interventions.

Mandatory standards run the risk of locking in a lowest common denominator approach rather than facilitating a flexible response capability in a fast-changing environment.

A principles-based approach rather than prescriptive standards is likely to prove more effective. This can be supported by an active program to continuously review and update regulatory guidance and best practice educational materials – linked to threat intelligence and data obtained from 'single door' incident and breach reporting.

**b. Is further reform to the Security of Critical Infrastructure Act required? Should this extend beyond the existing definitions of 'critical assets' so that customer data and 'systems' are included in this definition?**

It is difficult to identify a specific deficiency in the operation of the Act that would be cured by the extension of existing definitions of 'critical assets' to include customer data and 'systems'.

As far as banks are concerned, the concept of 'critical banking assets' is defined by reference to 'assets' that satisfy certain conditions in the Act. The Act defines 'assets' non-exhaustively to include 'computer data' (i.e., data held in a computer or storage device) and 'systems, and 'any other thing'. As we understand it, the concept of 'asset' in the Act already includes customer data and systems. It is not clear then, at least as far as banks are concerned, that any further amendments to the definition of asset are needed to include customer data and systems.

The core purpose of the Act is continuity of critical services. Extension of the scope of the Act to customer data and systems may be counterproductive and introduce further overlap and confusion particularly with Notifiable Data Breaches under the Privacy Act.

The ABA is aware of a suggestion that an extension in the scope of the Act would facilitate better co-ordination between industry and government to mitigate the impact of a data breach on affected consumers. Although this is a goal that we support, it is unclear why the extension of the scope of the Act is necessary to achieve this outcome. Without a clear purpose for the extension of the scope of the Act to customer data and systems, this change would appear to run the risk of increasing compliance burdens across our Members' people, processes, and systems, without contributing to enhanced cyber resilience.

We support reform to the Act to consolidate and align cyber security reporting requirements. A 'single door' for cyber security incident and breach reporting would be a significant step in streamlining reporting requirements. In practice, it may prove difficult to deliver without an alignment of the underlying reporting obligations distributed across multiple legislative and regulatory instruments.

For example, banks must currently navigate overlapping reporting requirements under, at least, the Act, the Privacy Act and CPS 234 along with the prospect of further requirements under CPS230. Additional reporting obligations to ASIC and the RBA may arise depending upon the particular circumstances of a cyber incident. The trigger events, timelines and required data as well as the reporting mechanism for these reporting requirements are inconsistent and risk diverting attention from managing a cyber incident to managing compliance reporting obligations.

The ABA also notes that the Act provides responsible entities protection from liability for damages arising from compliance with incident notification requirements, ministerial directions, and action directions. However, the Act provides no such protection for good faith compliance with other types of government directions and measures. This includes compliance with enhanced cyber security obligations (e.g., providing Government agencies with access to system information). The ABA submits that the immunities in the Act should also apply to other Government directions and measures, including the enhanced cyber security obligations. This reform would provide for regulatory consistency and afford appropriate protection to entities acting in good faith compliance with Government directions.

The 'protected information' regime in the Act imposes onerous, criminal penalties and restrictions on responsible entities' handling of their own internally generated records and information. While ABA Members acknowledge the Act does provide exceptions to these restrictions, the exceptions are narrow and ambiguous in their scope. This creates uncertainty as to the use of an entity's own operational information and its disclosure to third party partners (e.g., service providers, professional advisers) which may limit the ability of an organisation to respond effectively to a cyber incident.

**c. Should the obligations of company directors specifically address cyber security risks and consequences?**

No.

Cyber security is already one of many issues to which company directors must give due consideration in the conduct of their responsibilities. There seems to be little value in specifically enumerating cyber security as an area that company directors must address. On the one hand, legal precedent already confirms that this is an area of director's responsibilities (ASIC v RI Advice Group Pty Ltd), and on the other, such an approach begs the question why the many other areas of directors' responsibilities are not similarly enumerated. The current principles-based approach to defining directors' duties is far superior to initiating a process that inevitably leads to an ever-growing laundry list of detailed responsibilities.

A far more effective approach would be to further support director education and best-practice sharing mechanisms so that company directors can be as effective as possible in the carrying out the cyber security aspects of their responsibilities.

In addition, ASIC could be encouraged to provide further guidance to Australian Financial Services License (**AFSL**) holders on how to best ensure their cyber security systems and processes comply with their licensing obligations.

Recognising directors of financial institutions already have (under BEAR) or are soon to have (under FAR) additional accountability obligations that include cyber risk.

**d. Should Australia consider a Cyber Security Act, and what should this include?**

Amendment of existing legislation to provide greater clarity and alignment between legislative instruments is likely to be the fastest and most effective legislative reform. A new Cyber Security Act may assist in enhancing Australia's overall cyber security capability only if it consolidates and replaces cyber security obligations and oversight powers in a single instrument.

We note the various obligations that already apply to banks including:

- Security of Critical Infrastructure Act;
- Privacy Act and proposed reforms including regarding APPs 11 (data security) & 8 (cross-border disclosure of personal information), further promoting data minimisation and the Notifiable Data Breach reporting regime; and,
- CPS234 and the proposed CPS 230 (Operational Risk Management).
- AFSL holder obligations including the overarching requirements in s 912A of the Corporations Act (noting that the RI Advice case recognised that s 912A is concerned with cyber risk management).

The design of any new Cyber Security Act should align with or incorporate existing legislation as well as establishing a single regulatory framework that can be relied upon to meet obligations under other legislative and regulatory instruments including, but not limited to the Privacy Act and AML/CTF obligations.

Before considering the introduction of new legislation, we suggest completing a PIR on recent major incidents (e.g., Optus, Medibank, and Latitude) together with cross sector exercises to clearly understand where existing legislation is lacking and whether that should be addressed via amendments or new legislation.

For example, we understand one area that could benefit from legislative amendment is data sharing to help prevent fraud following a major data incident. This may be addressed via amendments to privacy legislation.

On the point of sectoral exercises, the ABA notes recently, that the Minister for Home Affairs and Cyber Security, announced simulated exercises ('War Games')[1] across critical infrastructure assets, including large banks. The ABA is in favour of these War Games and remains confident the outcomes from these exercises will assist the Government in better formulating its Strategy.

[1] *'Consider what damage could be caused': Government launches cyber 'war games' for major banks.* Sydney Morning Herald. Knott., M. 11 April 2023.

**e. How should Government seek to monitor the regulatory burden on businesses as a result of legal obligations to cyber security, and are there opportunities to streamline existing regulatory frameworks?**

Development of a 'single door' for cyber security and data incident and breach reporting is likely to reduce the existing incident management compliance burden (allowing resources to be directed toward actual cyber resilience rather than compliance management) and provide a single point for measurement of the volume and complexity of cyber incident reporting.

In practice, the development of a 'single door' approach is likely to highlight the overlapping and confusing reporting triggers, timelines, data requirements and procedures. This will provide the opportunity for a further alignment of the underlying requirements across multiple regulators. The 'single door' should operate in two directions to streamline both communications to regulators and government agencies and requests for information from regulators.

The newly created Cyber Security Coordinator role should be the central point of coordination across the government agencies during an incident so that the impacted organisation can focus on incident resolution.

**f. Should the Government prohibit the payment of ransoms and extortion demands by cyber criminals by:**

**a) victims of cybercrime; and/or**

**b) insurers? If so, under what circumstances?**

**i. What impact would a strict prohibition of payment of ransoms and extortion demands by cyber criminals have on victims of cybercrime, companies, and insurers?**

A prohibition on the payment of ransom and extortion demands may appear to be sound policy intended to undermine the business model for cyber extortionists (if no ransoms are paid, cyber attacks deliver no payoff for their instigators and should decline).

However, a ban on the payment of ransoms may have unintended consequences that undermine the objective of strengthening cyber resilience and response capability. These could include:

- creating a disincentive for businesses impacted by a cyber incident (especially SME businesses) to report the incident and seek specialist support from government resources to manage and mitigate the incident;
- encouraging cyber attackers to directly 'monetise' an incident by directly targeting consumers impacted by the incident with scam and fraud attempts and/or by selling compromised data to more sophisticated actors.

A ban on payment of ransoms would necessarily exclude such payments from the scope of cyber insurance policies.

Although payment of a ransom should be broadly discouraged, the decision to pay a ransom is a difficult one that should be made in light of all the circumstances of the individual case and a careful balancing of the risks.

In one prominent example, US firm Colonial Pipeline paid a ransom (after negotiation with the hacker) when their petroleum pipeline servicing 20 states in the eastern US was disabled in a cyber attack. The consequences of continued disruption to fuel delivery services, including risky fuel hoarding behaviour and disruption to distribution of food and essential goods was considered more significant than the costs of paying the ransom.

One mechanism to encourage careful analysis before a decision to pay a ransom could be an obligation to report a ransomware threat to the ACSC and demonstrate serious consideration of available alternatives. Cyber insurance policies (where available) could require that the cost of a ransom payment would only be covered where such a report has been made. Criminalising payments may unduly restrict the ability to act proportionately to cyber attacks.

This reporting obligation could allow tracking of the volume of ransom demands and proportion which are paid.

**g. Should Government clarify its position with respect to payment or non-payment of ransoms by companies, and the circumstances in which this may constitute a breach of Australian law?**

The Government's current position on ransom payments is quite clear. However, better guidance may assist companies to understand the existing legislative framework (including existing laws which may already prohibit payment). Ultimately, payment of a ransom is not a Government decision, and companies remain free to make lawful payments.

**3. How can Australia, working with our neighbours, build our regional cyber resilience and better respond to cyber incidents?**

Cyber security risks are a global challenge and require a global response. Collaboration with regional partners will help strengthen capability in the region as well as further enhance Australia's own cyber resilience.

Opportunities for collaboration include:

- cyber simulation exercises across borders – particularly among tightly integrated sectors such as finance – similar to the Quantum Dawn[2] exercises conducted in the US;
- standardised cyber incident reporting models as proposed by the Financial Stability Board[3];
- enhanced threat intelligence sharing mechanisms including tactical intelligence sharing at sectoral level (e.g., suspect account information);
- enhanced cross-bordering policing of cyber criminals including streamlined mechanisms to request police support across jurisdictions in managing a cyber incident; and,
- access to Australian Government educational resources and the proposed voluntary cyber resilience accreditation scheme.

**4. What opportunities exist for Australia to elevate its existing international bilateral and multilateral partnerships from a cyber security perspective?**

One area to explore where bilateral and multilateral cyber security collaboration could strengthen cyber resilience is the development of legal frameworks and processes to facilitate the timely sharing between financial institutions in different countries of both general threat intelligence as well as specific data sets that may support the detection and disruption of cyber attacks.

**5. How should Australia better contribute to international standards-setting processes in relation to cyber security, and shape laws, norms and standards that uphold responsible state behaviour in cyber space?**

The ABA supports efforts to develop greater consistency in definitions of cyber security incidents (taxonomy) and alignment of reporting requirements across borders together with a consistent hierarchy of incident response mechanisms.

**6. How can Commonwealth Government departments and agencies better demonstrate and deliver cyber security best practice and serve as a model for other entities?**

Commonwealth Government departments and agencies should be subject to at least the same cyber security obligations and reporting requirements as similar private sector entities. This should be extended to State and Local

[2] Financial Sector's Global Cybersecurity Readiness Exercised by Quantum Dawn VI - SIFMA - Financial Sector's Global Cybersecurity Readiness Exercised by Quantum Dawn VI - SIFMA
[3] Achieving Greater Convergence in Cyber Incident Reporting – Consultative document - Financial Stability Board (fsb.org)

Government and departments and agencies wherever possible as, in many instances, they will have a greater cyber footprint than Commonwealth counterparts.

Commonwealth Government departments and agencies should role-model best practice for other entities including:

- actively adopt and promote the use of Digital ID and verified credential models;
- maximising in-app communication with customers (where relevant) and limiting or eliminating the use of links in government SMS messages; and,
- sharing best practice and guides to support repeat execution.

**7. What can government do to improve information sharing with industry on cyber threats?**

The proposed 'single door' for inward cyber incident and breach reporting creates a platform for enhanced outward information sharing with industry on cyber threats managed through the Trusted Information Sharing Network. Appropriately designed reporting processes facilitated through a single gateway provide the opportunity for effective and timely dissemination of both general (aggregate) threat information as well as specific threat intelligence.

Rapidly sharing critical updates will better enable organisations to respond effectively within often very limited time windows. A review of government information declassification standards, particularly when related to incidents impacting third parties, may establish clearer and faster pathways for timely intelligence sharing.

Models should be developed for collaboration with and integration into industry level threat intelligence capabilities such as the Australian Financial Crimes Exchange (**AFCX**). In addition, the capability of the DVS can be extended to provide a single reference point for data on compromised identity credentials.

The Cyber Threat Intelligence Sharing (**CTIS**) platform, established by the ACSC in November 2021, currently has just 2 per cent of participating entities joining the platform. CTIS allows voluntary sharing of observable indicators of compromise bi-directionally, allowing other organisations to take early action for their organisations. The government can play an important role in enabling increased usage of this platform across industry, including extension of safe harbour provisions to ensure entities can freely and voluntarily share information without regulatory consequences.

**8. During a cyber incident, would an explicit obligation of confidentiality upon the Australian Signals Directorate (ASD) Australian Cyber Security Centre (ACSC) improve engagement with organisations that experience a cyber incident so as to allow information to be shared between the organisation and ASD/ACSC without the concern that this will be shared with regulators?**

Yes.

An appropriately designed safe harbour mechanism would ensure that interactions between businesses impacted by a cyber security incident and the ASD and ACSC are focussed solely upon timely and effective action to rectify the incident and mitigate any impacts. There may be a reluctance to engage as openly and constructively as possible with the ACSC or other government agencies given the current level of focus on liability frameworks and follow-on regulatory and litigation risks. To address this, there should be a priority on removing barriers to swift collaboration, communication, and response.

Design of such a safe harbour mechanism should consider:

- alignment with the proposed 'single door' reporting model;
- Freedom of Information implications; and
- potential good faith immunity for reporting entities seeking assistance in a timely and fulsome manner.

Any entity seeking ASD/ACSC support would remain subject to review, investigation, and potential penalty through existing regulatory structures after the immediate impacts of the incident have been addressed.

Priority should also be given to simplifying the process for accessing ASD/ACSC support which can be complex, particularly for smaller organisations.

**9. Would expanding the existing regime for notification of cyber security incidents (e.g., to require mandatory reporting of ransomware or extortion demands) improve the public understanding of the nature and scale of ransomware and extortion as a cybercrime type?**

Credible ransomware demands would already be reported by many regulated entities, for example under CPS 234 as a potentially material information security incident. Any broader reporting of ransomware attacks should be subject to appropriate materiality thresholds.

Simplification and streamlining of cyber incident reporting obligations provides the most straightforward opportunity to obtain and analyse consistent information (without confusing overlap and differing taxonomies) as to the nature and scale of all types of cyber incidents including ransomware and extortion. A single source of truth provides the platform for clear insight and an authoritative perspective to improve public understanding.

In time, if any gaps in the information collected are identified, then the 'single door' reporting capability can be expanded appropriately, however, priority should be given to making better use of information already collected before further expanding compliance reporting obligations.

**10. What best practice models are available for automated threat-blocking at scale?**

The AFCX is a prominent example of cross-industry capability to share tactical threat intelligence and diagnostic information to support automated cyber attack detection and intervention approaches. Government should ensure that appropriate regulatory frameworks exist to facilitate such intelligence sharing capability, link government threat intelligence and data, and encourage wider adoption of similar capability both within and across industry sectors.

In addition, Government could consider opportunities to facilitate collaboration between banks and telecommunications providers to bolster the security of digital banking. Measures soon to be introduced in Singapore include:

- removal of clickable links in text messages;
- transfer limits;
- notification of changed mobile numbers; and,
- registration of SMS sender identities to prevent SMS spoofing.

**11. Does Australia require a tailored approach to uplifting cyber skills beyond the Government's broader STEM agenda?**

Skilled cybersecurity talent is a critical resource for a strengthened cybersecurity capability. An estimated gap in the cybersecurity workforce of up to 30,000[4] roles by 2026 is likely to only worsen by 2030 without targeted intervention. Medium and smaller businesses, in particular, are likely to be left under-resourced and more vulnerable to cyber attacks due to an increasingly fierce competition for limited cyber talent.

Some targeted steps to increase the cyber security talent pool include:

- streamlining visa application processes to ensure rapid turn-around time when recruiting cyber talent.
- increased support for school curriculum and initiatives such as the Grok Schools Cyber Security Challenge.
- developing micro-credentialling approaches to facilitate practical, hands-on retraining and skills recognition for currently employed individuals.
- examine the opportunity to develop a co-ordinated national curriculum through the TAFE system modelled on Israel's National Centre for Cyber Education; and,
- increased funding for additional students to study formal cyber related qualifications at tertiary institutions.

Meanwhile, the productivity of the cyber workforce can be enhanced by a focus on encouraging adoption of AI and machine learning solutions to cyber security monitoring and interventions, as well as streamlining compliance

[4] *Cyber skills shortage 'to hit 30,000 in four years'*. Australian Financial Review. Mason., M. 13 September 2022.

obligations to ensure maximum resources are allocated to building cyber resilience capabilities rather than managing compliance obligations.

We note that *Australia's Cyber Security Sector Competitiveness Plan 2022* highlights that cyber research funding has decreased by 23 per cent since 2019[5]. The ABA takes this opportunity to call out the need for investment not only in cyber security talent, but in investment initiatives to develop technologies that contribute to make Australia more cyber resilient.

**12. What more can Government do to support Australia's cyber security workforce through education, immigration, and accreditation?**

Please see Q11 above.

**13. How should the government respond to major cyber incidents (beyond existing law enforcement and operational responses) to protect Australians?**

Regular cyber incident simulation and response exercises including participants from across Government and across industry can enhance preparedness for a cyber incident. Such simulations should cover communications protocols and an aligned prioritisation of response based upon a common assessment of incident severity. At least initially, such simulations will be of greatest value among SOCI regulated entities.

Enhanced mechanisms supported by the ACSC for anonymised data sharing (including with smaller organisations) can facilitate a faster and more effective protective response for customers impacted by a cyber breach. This should include an expanded role for the DVS as a reference for compromised credentials and integration of industry capability such as the AFCX to facilitate rapid and secure sharing of relevant information across industry.

**a. Should government consider a single reporting portal for all cyber incidents, harmonising existing requirements to report separately to multiple regulators?**

Yes.

As noted throughout our responses, the ABA strongly endorses the creation of a two-way 'single door' for cyber security incident reporting. This will streamline the reporting process, reduce confusion and complexity in managing multiple reporting obligations, consolidate requests for information from multiple regulators and facilitate faster access to specialist support resources when required.

In practice, the development of a 'single door' approach is likely to highlight the overlapping and confusing reporting triggers, timelines, and procedures. This will provide the opportunity for a further alignment of the underlying requirements across multiple regulators and government agencies.

We note that this approach has been recommended by the Productivity Commission in their *Reform Direction 14: Cyber security compliance arrangements to underpin a productive digital economy*[6]*:*

> *Recommendation 4.5. A single interface for cyber security reporting.*
>
> *The cost for businesses of complying with cyber security regulations should be reduced by streamlining incident reporting requirements,* ***with all reporting to occur via a single online interface. The operating system underlying this interface would then direct reports to the Australian Cyber Security Centre or other relevant government agency as required.*** *This could provide the platform for the government to work with cyber security software providers to build incident reporting functions into commonly used software, so that reports are automatically sent to relevant agencies if an incident occurs.*

[5] Australia's Cyber Security Sector Competitiveness Plan 2022.
[6] Productivity Commission's, 5-year Productivity inquiry: Advancing Prosperity (Report no. 100 – 7 February 2023), pg. 102.

**14. What would an effective post-incident review and consequence management model with industry involve?**

Post incident reviews should be just one component of an overall framework for design, assessment, review, and remediation of cyber security capability. Various frameworks for accreditation of cyber security capability that include this approach already exist and are the most effective mechanism to drive post-incident review and remediation activities. Sector specific regulators are likely best placed to ensure that these processes are carried out appropriately.

Where a business that has been impacted by a cyber incident has sought specialist support from the ASD or ACSC in the management and mitigation of the incident, a supplementary post-incident review process may be appropriate. These should be focussed on cyber incidents whose scale and/or unique characteristics provide an opportunity for wider learning and capability improvement and should be subject to appropriate safe harbour protections to ensure constructive review.

A simplified model for the sharing of information about credentials compromised in a data incident including an expanded role for the DVS as a reference source for compromised credential information and a streamlined ability for relevant entities to share information about an incident will allow more effective consequence management by facilitating greater protective action for customers impacted by an incident.

**15. How can government and industry work to improve cyber security best practice knowledge and behaviours, and support victims of cybercrime?**

**a. What assistance do small businesses need from government to manage their cyber security risks to keep their data and their customers' data safe?**

As a general rule, individual businesses are best placed to determine how to meet their cyber security obligations by selecting an appropriate mix of technology and business process controls to achieve the required outcomes. Specialist advice is available to help businesses make these decisions.

Nevertheless, small businesses, in particular, are likely to benefit from access to best-practice recommendations. This could be facilitated by consolidation of Government cyber education programs, linkage to aggregate level cyber threat intelligence and amplification by 'trusted voices' such as relevant industry associations to communicate directly with specific industry sectors. Education programs should be based on behavioural research.

A voluntary cyber security accreditation and auditing model, managed by the ACSC with potential participation of approved private sector suppliers, could allow smaller businesses an efficient way to demonstrate their cyber security maturity to customers as well as when participating in procurement processes with larger organisations.

Consideration should also be given to working with cloud computing service providers (including cloud hosting and cloud software service providers) to integrate both clearly identified baseline and enhanced cybersecurity capabilities in their product offerings to support smaller businesses in reaching appropriate levels of cyber capability.

Individual customers impacted by a cyber security breach would be best supported by a clear process for informing them that they have been subject to a cyber incident together with a mechanism for facilitating appropriate action to mitigate the impact. This is likely to include both an enhanced DVS capability to act as a central source of information on compromised credentials and integration with intelligence sharing capabilities such as the Australian Financial Crimes Exchange. Amendments to the Privacy Act may be required to facilitate such protective action.

**16. What opportunities are available for government to enhance Australia's cyber security technologies ecosystem and support the uptake of cyber security services and technologies in Australia?**

A clear focus on the development, rollout and active utilisation of a robust Digital ID framework including verified credentials will act as a strong catalyst for the enhancement of Australia's cyber security technology ecosystem. A clear policy signal from Government that an interoperable Digital ID capability will form the foundation of a fundamentally strengthened data ecosystem in Australia will provide businesses and innovators with the confidence to invest in building out cyber security capabilities anchored in a trusted credentials model.

Similarly, the development of a voluntary cyber resilience accreditation and audit model (see 15 above) will have the added benefit of making it easier for Australian businesses to demonstrate that their capabilities meet or exceed international alternatives.

**17. How should we approach future proofing for cyber security technologies out to 2030?**

It is impossible to anticipate the technological evolution of both cyber threats and cyber security responses over anything more than a short period of time. This implies that any regulation should remain technology neutral so as to provide maximum flexibility for businesses to respond to evolving cyber threats and make use of emerging cyber resilience capabilities.

Adoption of a robust Digital ID capability is, nonetheless, a significant step-change in the cyber resilience of the data economy and should be adopted as an anchor for a fundamentally stronger cyber ecosystem. This capability too can be deployed in a way that allows for technological evolution of both threats and response mechanisms.

In addition, a Zero Trust approach to cyber security resilience requiring all users, whether inside or outside an organisation's network to be authenticated, authorised, and continuously validated for security configuration and access rights, can be progressively rolled out with Government agencies implementing and setting the standards for other sectors.

To the extent that the strategy creates new security obligations/standards, consideration should be given to regulating the technology product or service providers rather than the consuming organisations wherever possible. This provides a simpler point of intervention for continuous capability uplift in the face of emerging cyber threats.

**18. Are there opportunities for government to better use procurement as a lever to support and encourage the Australian cyber security ecosystem and ensure that there is a viable path to market for Australian cyber security firms?**

Cyber security is a structurally crucial and intrinsically global domain that requires access to best-in-class solutions from wherever in the world they are available. Subject to that overarching criterion, government procurement can be a judiciously applied lever to ensure that Australian best-in-class capability is given appropriate recognition. Successful tenderers for government cyber security projects can be promoted to the private sector.

Such a judiciously applied lever could be considered to drive significantly increased inherent security across the technology products and services landscape. Requiring that products and services are more secure by default.

A voluntary cyber capability accreditation and auditing scheme (see 15 above) can support a more efficient due diligence process for both government and private sector procurement processes while making it easier for Australian businesses to demonstrate that their capabilities meet or exceed international alternatives.

**19. How should the Strategy evolve to address the cyber security of emerging technologies and promote security by design in new technologies?**

The Government could consider legislating security by design standards for emerging technologies including, for example, AI. Such standards should apply to the providers of technology products and services rather than consuming organisations. This approach appropriately shifts liability onto entities that fail to take reasonable precautions to secure the products or software services rather than forcing the end user to suffer the consequences of an insecure product or service. Thereby, security by design may also extend to third-party providers of products and services supplied to businesses, including banks, which may contribute to cyber incidents. Australia may wish to assess the approach currently being considered in the US[7].

**20. How should government measure its impact in uplifting national cyber resilience?**

Appropriately measuring the impact of efforts to uplift national cyber resilience is a difficult challenge.

[7] National-Cybersecurity-Strategy-2023.pdf (whitehouse.gov)

Reporting on input metrics runs the risk of creating an additional compliance burden without a clear linkage to enhanced cyber resilience. Any such metrics such as the number of cyber security graduates, director centred cyber training courses or number of accredited entities under the proposed voluntary cyber accreditation scheme should be carefully selected for relevance and ease of reporting. There is little value in creating an expanded cyber capability metrics framework.

Similarly, simply measuring the number of reported cyber incidents is unlikely to offer useful insight and is subject to many external factors such as the actions of state-based entities. The number of attempted cyber attacks is likely to continue to rise irrespective of any action to enhance cyber resilience.

The 'single door' reporting model provides the best opportunity to develop insightful metrics to assess the impact of government efforts to uplift national cyber resilience. Measures of the volume, scale, nature (categorisation) and crucially of the impact of cyber attacks will provide the most useful insight. Potential metrics could include:

- Number of incidents
- Number of (potentially) impacted customers
- Nature of incident (attack typology)
- Reporting time (from discovery)
- Response time (time to recover)
- Impact (resolution)

Importantly, this measurement process would be integrated with the cyber attack response process rather than an additional compliance obligation. This approach will require the development of a clear and simple taxonomy for the measurement of the impact of a cyber attack: at what point, if any, was the attack detected and remediated?

Where possible, international benchmarks should be included to provide an assessment of comparative effectiveness of Australia's cyber security resilience and remediation capability.

**21. What evaluation measures would support ongoing public transparency and input regarding the implementation of the Strategy?**

The ABA has no additional contribution to make on this question.

## In Closing

The rapid and ongoing evolution of the data economy is set to bring considerable productivity and customer experience benefits to all Australians. It also expands the threat perimeter for ever increasing cyber security attacks from both criminal enterprises and state actors.

Accordingly, the ABA welcomes the development of the 2023-2030 Australian Cyber Security Strategy and is delighted to have had the opportunity to contribute to its formulation.

Streamlining of cyber reporting obligations (initially through a two-way single door capability and then through rationalisation and alignment of underlying obligations) together with a focussed effort to deploy an interoperable Digital ID capability across the economy provide the two anchor opportunities to build a substantially enhanced cyber security capability for the nation.

If you have any further questions, please do not hesitate to contact us.

Yours sincerely,

Nicholas Giurietto
Head of Future Policy
Australian Banking Association
[redacted]

Christos Fragias
Policy Director
Australian Banking Association
[redacted]