Australian Government
Australian Digital Health Agency

Cyber Legislation Reform Consultation Paper

23 February 2024

Approved for external use

Document ID: DOC24-003637

Australian Digital Health Agency ABN 84 425 496 912, Level 25, 175 Liverpool Street, Sydney, NSW 2000
Telephone 1300 901 001 or email help@digitalhealth.gov.au
www.digitalhealth.gov.au

Acknowledgements
The Australian Digital Health Agency is jointly funded by the Australian Government and all state and territory governments.

Disclaimer
The Australian Digital Health Agency ("the Agency") makes the information and other material ("Information") in this document available in good faith but without any representation or warranty as to its accuracy or completeness. The Agency cannot accept any responsibility for the consequences of any use of the Information. As the Information is of a general nature only, it is up to any person using or relying on the Information to ensure that it is accurate, complete and suitable for the circumstances of its use.

Document control
This document is maintained in electronic form and is uncontrolled in printed form. It is the responsibility of the user to verify that this copy is the latest revision.

OFFICIAL

Document information

Key information

Owner	Danielle Pentony	
Prepared by	James Meikle and Andrew Hacking	
Contact for enquiries	Australian Digital Health Agency Help Centre	
	Phone	1300 901 001
	Email	help@digitalhealth.gov.au

Draft version history

dv #	Date	Author	Comments
001	19/02/2024	James Meikle and Andrew Hacking	Initial draft sourced from DOC24-003637 Question for Review consultation sheet. Line inserted when the Agency has not chosen to/responded to a question and added sections for additional comments outside of questions – as stated by Home Affairs in the recent town hall not, all feedback has to align to question.
002	20/02/2024	James Meikle and Andrew Hacking	Added more feedback based on SME Industry research and experience, Home Affairs Town Hall attendance. Updated feedback using content provided by Agency Privacy and Policy SMEs. Aligned question numbers to the consultation paper numbers.
003	21/02/2024	James Meikle and Andrew Hacking	Added feedback from drop in legal SME discussion with Adam Flynn. Updated an answer from discussion with Cyber Operations (ransomware) added more content.
004	23/02/2024	James Meikle and Andrew Hacking	Updated with feedback from Director Cyber Solutions and Director Policy Assurance.

Product or document version history

Product or document version	Date	Release comments

Table of contents

1 Introduction

1.1 Purpose

The Australian Digital Health Agency (the Agency) are providing consultation to the Australian Cyber Security Legislative Reform work being led by the Department of Home Affairs (Home Affairs).

1.2 Intended audience

The audience for this document consists of Home Affairs - who are coordinating the consultation with commercial and public industry – and the Agency.

1.3 Scope

This document is limited to discussing cyber security legislative reforms, specifically Agency input into the consultation on proposed new cyber security legislation, and on changes to the *Security of Critical Infrastructure Act 2018*.

1.4 Overview

The following consultation feedback is provided by the Agency with internal consultation of the Cyber Security Branch including consultation with various subject matter experts across the Agency.

2 Part 1 - New cyber security legislation

2.1 **Measure 1** - Helping prevent cyber incidents Secure-by-design standards for Internet of Things devices

1. **Who in the smart device supply chain should be responsible for complying with a proposed mandatory cyber security standard?**

   Whilst this proposal may improve the quality of consumer Internet of Things (IoT) devices, the effectiveness of the control is dependent on devices being subject to robust deployment, patching and configuration practices by the device creator and the consumers using it. This may not be something that can be expected of or completed by all consumers, due to the variations in managing device settings, digital or technical literacy, and security maturity levels.

   The Agency notes the proposed scope and prioritisation of consumer IoT appears to be somewhat limited. The increasing use of many classes of IoT devices within a healthcare setting can pose a significant risk to life through interference of patient monitoring systems, disruption of clinical systems or a breach of patient confidentiality. There may be an opportunity for Home Affairs to consider expanding the scope and prioritisation of mandates for IoT security standards to consider the context of use where an IoT device is used, not only the class of the device.

   The Agency is keen to support and contribute to this re-consideration and requests that the threat and risk assessment that was used as input into this proposed reform be made available publicly. This would provide greater clarity around the use of IoT devices that may be covered within this reform and demonstrate that government has considered the significant impacts and potential misuse of IoT across the Australian landscape.

2. **Are the first three principles of the ETSI EN 303 645 standard[1] an appropriate minimum baseline for consumer-grade IoT devices sold in Australia?**

   The Agency supports the three principles and sees an opportunity for mandatory labelling of IoT based on the context of use. Higher risk environments including healthcare increasingly use consumer grade technologies which can pose a risk (Agency submission to question 1).

   Determination of a mandatory labelling requirement could be supported by industry specific codes of conduct and consistent risk assessment tools. Balancing the minimum baseline labelling requirements with existing investments in legacy systems may need to consider the presence of compensating controls in the absence of a compliance label, whilst mandating the labelling for new deployments.

3. **What alternative standards, if any, should the Government consider?**

   The Agency recommends exploring alternative standards appropriate to the context and tailoring of controls informed through detailed threat and risk assessment.

[1] The ETSI standard is a European standard for implementing Cyber Security for Consumer Internet of Things. Further information at this link: https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf

In respect of a medical or healthcare context, the Agency recommends consideration of the United States Design Controls for all Class II and Class III medical devices due to the associated risks.

Standards should include software supply chain security as a pre-requisite given secure by design is predicated on an accurate and detailed understanding of the composition of software.

This enables suppliers to provide patches and notify asset/device owners in response to vulnerabilities that occur deep within software dependencies. Currently there is a significant burden on asset owners as they do not have sufficient visibility of their supply chain or the necessary information to manage their risk and prioritise remediation activities.

The Australian government should look to United States (US) and other international standards efforts, such as those published or adopted by:

- National Telecommunications and Information Administration (NTIA)
- Cyber Security Industry Alliance (CSIA)
- National Institute of Standards and Technology (NIST)
- BSI Group.

The focus would be on standards that include a Software Bill of Materials (SBOMs) such as Software Package Data Exchange(SPDX) and CycloneDX, Software Identification (SWID), Vulnerability Exploitability Exchange (VEX), and Common Security Advisory Framework (CSAF). This would cover software identification, software ingredients, vulnerability attestations and security advisories in machine readable formats.

4. **Should a broad definition, subject to exceptions, be used to define the smart devices that are subject to an Australian mandatory standard? Should this be the same as the definition in the PTSI Act in the UK?**

   The Agency supports a reform that includes use of devices within a medical or healthcare context, and more broadly, where any device poses a significant threat based on context of use, with mandatory controls covering both secure by design standards *and* operational concerns.

   Control measures should include use of comprehensive controls including network segmentation, vulnerability and patch management, secure administration, system hardening and monitoring.

5. **What types of smart devices should not be covered by a mandatory cyber security standard**

   Contexts where the inherent risk is low or where existing alternative controls for the use of these devices can sufficiently manage the risk.

6. **What is an appropriate timeframe for industry to adjust to new cyber security requirements for smart devices?**

   The Agency recommends an implementation plan of one year for suppliers of in scope industries to meet mandatory requirements. Australia has the opportunity to inherent much of the work the US has already achieved in respect of secure by design and supply chain security.

   The US government set down one year for transparency over their suppliers, many of which currently supply to the Australian market and may be in a good position to be able to comply.

7. **Does the Regulatory Powers Act provide a suitable framework for monitoring compliance and enforcement of a mandatory cyber security standard for smart devices?**

   The *Regulatory Powers Act 2014* may be a suitable framework for monitoring and enforcing compliance with the mandated cyber security standard. It offers powers that are broad and far-reaching and would enable a regulatory authority to monitor and investigate electronic equipment. However, careful consideration needs to be given, and legal advice sought, on the specific requirements with the *Regulatory Powers Act 2014* that must be satisfied before certain powers can be exercised. For example, the provisions under section 18 of the *Regulatory Powers Act 2014*. The Attorney-General's Department, as the owner of this legislation may be best placed to advise Home Affairs on the suitability of this framework for the intended purposes.

   Additional feedback addressing measure 1

   The Agency welcomes the opportunity to be engaged in future consultations that are out of scope in the current reforms. Small businesses constitute many of the users of our systems (Healthcare Providers) and there is an increasing use of devices and mobile applications.

   The Agency assumes that as the Therapeutic Goods Administration (TGA) is responsible for regulating the supply, import, export, and manufacturing of medical devices, these are currently excluded from the proposed standard. It is worth noting that smart phones and personal fitness trackers often collect a range of health and wellness data, as well as other sensitive personal information. The line between medical and other devices with a role in digital health will become increasingly blurred. There may be opportunities to explore alignment with the TGA's regulatory approach to medical devices.

   Given the relative market size of Australia, the Agency supports alignment to international standards as far as is practicable. The Agency suggests that local standards be avoided, due to the effects of increased conformance costs that have the potential to impact the availability of mature and competitive solutions in the global market.

2.2 **Measure 2** - Further understanding cyber incidents

Ransomware reporting

While the healthcare sector is often targeted by ransomware, introducing another notification and reporting regime may be perceived as an additional administrative burden for healthcare providers. Noting the sector is subject to the Notifiable Data Breach (NBD) Scheme that is administered by the Office of the Australia Information Commission (OAIC) and involves reporting health data breaches.

The incidents that lead to a data breach may potentially also involve a ransomware attack. It will be important to provide clarity to healthcare providers that may be subject to both reporting regimes on the associated workflows, should both elements apply to an incident. The Agency understands the OAIC is working closely with Home Affairs to reduce any duplication and streamline the reporting regimes.

The Agency also works with the OAIC in its role as System Operator for the My Health Record system. Based on this experience, several suggested approaches are offered for consideration:

- Developing the necessary "limited use" powers for capture and sharing anonymous ransomware reporting data from regulators, such as the OIAC, Australian Health Practitioner Regulation Agency (AHPRA), to leverage and align with existing reporting regimes.

- Reviewing and amending where necessary the breach notification powers and secrecy provisions in the My Health Records Act to enable "limited use" sharing of ransomware reporting data.
- Develop "limited use" powers for capturing ransomware reporting data in circumstances where an entity is not already subject to existing notifiable breach powers.

8. What mandatory information should be reported if an entity has been subject to a ransomware or cyber extortion incident?

The Agency recommends "limited use" powers and that such information needs to be anonymised, prior to sharing via an existing regulator. Please refer to the response to question 11 and 16 for further details.

9. What additional mandatory information should be reported if a payment is made?

The Agency recommends "limited use" powers and that such information needs to be anonymised, prior to sharing via an existing regulator. Please refer to the response to question 11 and 16 for further details.

10. Which entities should be subject to the mandatory ransomware reporting obligation?

The Agency recommends "limited use" powers and that such information needs to be anonymised, prior to sharing via an existing regulator. Please refer to the response to question 11 and 16.

11. Should the scope of the ransomware reporting obligation be limited to larger businesses, such as those with an annual turnover of more than $10 million per year?

There is a potential risk in this approach that by using this threshold, it excludes smaller businesses within the Australian economy. This could result in entities that are not subject to reporting (due to their turnover) being seen as soft targets, and for such ransomware activity to go unmonitored.

The proposed turnover threshold needs to consider the severity of the impact on businesses of all sizes. Noting, the *Privacy Act 1988* is currently under review and the NDB scheme considers penalties based on the significance and value of the data breach, there may be opportunities to align the criteria with this existing legislations and regime to make it consistent and simpler for businesses to understand their obligations.

Home Affairs may be able to align with the existing NDB scheme and leverage other regulatory powers to capturing ransomware reporting data. This provides an opportunity for a more accurate and complete understanding, without introducing additional reporting burdens on entities. It also allows those regulators to gain the necessary insights and implement industry appropriate measures to combat ransomware attacks.

The Agency suggests Home Affairs explore the following options:

- Developing the necessary "limited use" powers for capture and sharing anonymous ransomware reporting data from regulators (not the entities themselves) who are already notifiable for data breaches (e.g. OIAC, AHPRA).
- Eschewing any powers that require entities to report ransomware breach notifications directly to Home Affairs.
- Obtaining "limited use" powers for the collection of anonymised data from existing regulators to avoid administrative or economic burdens on industry and streamline enforcement functions across government.

- For entities not covered by any mandatory breach notification powers, then reform should occur within the remit of the relevant regulator and include a review of mandatory breach reporting requirements based on the potential risk of harm.
- Specify the minimum reporting data requirements for regulators to implement.

12. What is an appropriate time period to require reports to be provided after an entity experiences a ransomware or cyber extortion attack, or after an entity makes a payment?

The Agency recommends a consistent approach be used and align with existing mandatory breach notification powers, such as the *Privacy Act 1988*, and other relevant legislation for the industry classifications. Home Affairs may need further consultation with the Department of Health and Aged Care to explore the best approach to leveraging existing legislation in relation to incident notification requirements, such as in the *My Health Records Act 2012.* Noting this would only capture healthcare businesses that participate in this system. The Department would be best placed to comment and advise on this matter, as the owner of the legislation and with a broader remit and view of the Commonwealth and jurisdictional health ecosystem and regulatory environments.

13. To what extent would the no-fault and no-liability principles provide more confidence for entities reporting a ransomware or cyber extortion incident to Government?

The Agency suggests, exploring different options to direct reporting to Home Affairs by entities and instead rely on mandatory breach reporting obligations in existing regulatory powers.

14. How can the Government ensure that the no-fault and no-liability principles balance public expectations that businesses should take accountability for their cyber security?

It is possible that public expectations may not be met with this approach. Evidence-based research suggests that accountability for cyber security responsibilities requires legislative compliance with minimum standards, which are enforced by regulations.

Discretionary risk management is insufficient to drive accountability, the existence of regulators supports this truth. Accountability for cyber security requires that compliance with minimum standards is ultimately enforced by regulations.

Licensing bodies within various industries could be used to mandate compliance to cyber security standards as a necessary basis of participation. This provides an opportunity for industry specific security practices, guidelines, and maturity roadmaps to be developed whilst providing a robust control against rogue or negligent operators.

The above measures are likely to obviate the need for direct punitive measures and the unintended consequence of breach monetisation by cybercriminals, as has occurred with the European General Data Protection Regulation (GDPR).

15. What is an appropriate enforcement mechanism for a ransomware reporting obligation?

The Agency suggest a whole-of-government approach to ransomware reporting and enforcement powers for Home Affairs. The mandatory breach reporting powers of existing regulators is the preferred approach.

16. What types of anonymised information about ransomware incidents would be most helpful for industry to receive? How frequently should reporting information be shared, with whom, and in what format?

The Agency suggests the following anonymised information be collected where it is available, noting that there are varied levels of maturity with respect to incident response handling:

- Australian Taxation Office (ATO) Business Industry Codes (BIC)
- Source of breach / attack method:
    - Malicious: cyber incident, social engineering, rogue employee/insider, theft of physical media/device/papers.
    - Accidental: human error, system fault.
    - Detail of the attack/kill-chain.
    - Was a professional forensic security specialist involved in analysing the breach?
- Key dates and times:
    - when the breach was first communicated/detected.
    - when the mandatory reporting authority was notified (e.g. OAIC, AHPRA, etc.), where applicable.
    - when the breach/attack actually occurred (if known).
    - when the ransom was received.
    - when the ransom was paid.
    - whether the malicious actor fulfilled or reneged on their end of the deal.
    - when system returned to normal operation.
- Ransom amount:
    - Original ransom amount requested.
    - Actual ransom amount paid.
    - Method of payment (including the specific crypto currency used).
    - Did the malicious actor fulfill or renege on their end of the deal?
    - Location of attackers (if known).
    - Was a negotiator or negotiation service used?
- Estimated cost of the breach **excluding** the ransom paid:
    - Lost staff hours and cost dealing with the breach.
    - Specialist services used, type of service, hours billed and cost.
    - Tools and equipment, licenses for breach investigations and restoration of services.
- Data involved in the breach:
    - element types included in the breach:
        - Credentials (e.g. username, password, myGov).
        - Contact information.
        - Identity information.
        - Financial details.
        - Health information.

        - Other sensitive information.
        - Tax file numbers.
    - Estimation of the quantity of each type of record.
- Actions taken to prevent/avoid future breaches.

2.3 **Measure 3** - Encouraging engagement during cyber incidents Limited use obligation on the Australian Signals Directorate and the National Cyber Security Coordinator

17. What should be included in the 'prescribed cyber security purposes' for a limited use obligation on cyber incident information shared with ASD and the Cyber Coordinator?

Purposes:

a. to minimise and contain cyber attacks;

b. Information gathering and techniques to identify perpetrators;

c. Forensic analysis and maintain chain of custody necessary to support prosecution and working with the Australian Signals Directorate (ASD) partner organisations in other jurisdictions;

d. Maintain anonymised repository of all attacks including payloads used, malware samples, Indicators of Compromise (IoC's);

e. Capture and report on the following anonymised information:

   i. ATO Business Industry Code (BIC)

   ii. Source of breach / attack method:

      1. Malicious: cyber incident, social engineering, rogue employee/insider, theft of physical media/device/papers.
      2. Accidental: human error, system fault.
      3. Detail of the attack/kill-chain. (e.g. MITRE ATT&CK, CVE's NVD's IOCs used in the attack).
      4. Was a professional forensic security specialist involved in analysing the breach?

   iii. Key dates and times:

      1. when the breach was first communicated/detected.
      2. when the mandatory reporting authority was notified (e.g. OIC, APRA, etc where applicable).
      3. when the breach/attack actually occurred (if known).
      4. when system returned to normal operation.
      5. for ransomware attacks:

         a. when a ransom was received.

         b. when a ransom (if any) was paid:

i. whether the malicious actor fulfilled or reneged on their end of the deal.

ii. Original ransom amount requested.

iii. Actual ransom amount paid.

iv. Method of payment (including the specific crypto currency used).

v. Did the malicious actor fulfill or renege on their end of the deal?

vi. Location of attackers (if known).

vii. Details of ransomware negotiator/service used (if any)

iv. Estimated cost of the breach **excluding** any ransom paid:

1. Lost staff hours and cost dealing with the breach.
2. Specialist services used, type of service, hours billed and cost.
3. Tools and equipment, licenses for breach investigations and restoration of services.

v. System information:

1. Business criticality (critical, essential, necessary, desirable)
2. System type (on prem, cloud IaaS/PaaS, SaaS, endpoint, edge/IoT/OT)

vi. Data involved in the breach:

1. element types included in the breach:
    a. Credentials (e.g. username, password, myGov).
    b. Contact information.
    c. Identity information.
    d. Financial details.
    e. Health information.
    f. Other sensitive information.
    g. Tax file numbers.
2. Estimation of the quantity of each type of record.

vii. Actions taken to prevent/avoid future breaches.

18. What restrictions, if any, should apply to the sharing of cyber incident information?

Information should be anonymised by default prior to sharing.

Information should not be shared outside of the “limited use” powers without the consent of the implicated entities that the incident pertains to.

19. What else can government do to promote and incentivise entities to share information and collaborate with ASD and the Cyber Coordinator in the aftermath of a cyber incident?

Government initiatives designed to improve supply chain transparency and sharing of vulnerability exploitability, security advisories using machine readable formats would support the rapid response to vulnerabilities and recovery from cyber incidents, whilst fostering a collaborative approach to preventing future incidents.

The relevant government cyber security agencies could also encourage entities in both the public Initiatives to improve supply chain transparency and sharing of vulnerability exploitability, security advisories using machine readable formats.

Promote entities in both the public and private sectors to publish security.txt so that entities can be contacted by the Cyber Coordinator, cyber security researchers and members of the public.

2.4 **Measure 4** - Learning lessons after cyber incidents A Cyber Incident Review Board

20. What should be the purpose and scope of the proposed Cyber Incident Review Board (CIRB)?

To improve the resiliency of systems to cyber-attack through the systematic review of significant events, knowledge sharing and providing recommendations for regulatory reform supported by data.

21. What limitations should be imposed on the CIRB to ensure that it does not interfere with law enforcement, national security, intelligence, and regulatory activities?

Limit the powers of the CIRB as a review function and after other law enforcement, national security, intelligence, and regulatory activities have concluded and/or approved the CIRB review.

22. How should the CIRB ensure that it adopts a 'no-fault' approach when reviewing cyber incidents?

Information voluntarily provided to CIRB must receive the same effective protection as legal privilege would, even though the information shared to CIRB is not a purpose where legal privilege could be claimed.

Ensure a culture where exemplary incident response is reviewed by the CIRB to squash any potential stigma that could result or be inferred by a CIRB review.

23. What factors would make a cyber incident worth reviewing by a CIRB?

Use of a novel or advanced attack method that is not well understood.

An exemplary incident response handling or measure, so that effective methods and techniques can be analysed and shared as much as ineffective ones.

Where the event is significant in scope or harm with impacts exceeding a defined threshold of cost, number of individuals or organisations impacted or the severity of the impact results in loss of life or had the potential to result in a direct loss of life (near miss).

Cyber incidents that impact the privacy and safety of Australian citizens, much like other significant products and services including construction/housing, children's toys, vehicle safety, food safety, electrical goods, aviation, transport.

24. Who should be a member of a CIRB? How should these members be appointed?

Similar model to that of the USA Government Charter CSRB equal standing positions from Public and Private sectors - e.g. appointed by ASD Secretary representatives from Defence, Australian Signals Directorate, ASIO, Australian Federal Police, and ACSC. Members must be

Australian citizens and hold security clearances. Private sector members are held to Australian Federal Government ethics and accountable as special members of the Australian Government while in the appointment.

25. What level of proven independent expertise should CIRB members bring to reviews? What domains of expertise would need to be represented on the board?

Government appointed office holders only.

26. How should the Government manage issues of personnel security and conflicts of interest?

Handled by existing government policy and processes for appointments.

Members should be required to obtain an Australian Government Security Vetting Agency (AGSVA) clearance, commensurate with the system classification and the nature of the event, with a Baseline security clearance as a minimum requirement. To provide further confidence in the membership, additional vetting such as Police Checks, could be conducted.

Investigations may reveal that an event has national security implications and as a result, the personnel requirements may evolve and change throughout the incident. The membership would need to be diverse and have the appropriate clearances and qualifications to leverage and access all investigation information.

27. Who should chair a CIRB?

Cyber Incident Response Commissioner appointed using the following:
Parliament of Australia – Commissioners' appointment, tenure, and remuneration

Further guidelines which could inform appointment:
Australian Government Attorney-General’s Department - Policy & Guidelines - Appointments to the Australian Human Rights Commission

28. Who should be responsible for initiating reviews to be undertaken by a CIRB?

The Agency suggests the Home Affairs Secretary, National Cyber Security Coordinator (Cyber Coordinator), is the most appropriate officer of the Commonwealth to initiate reviews undertaken by a CIRB. Noting, there are some instances where a cyber security incident may be at a scale that it is referred by other relevant authorities or government agencies such as the Australian National Audit Office, the Department of Prime Minister and Cabinet or the courts.

29. What powers should a CIRB be given to effectively perform its functions?

- Minimum required insofar as CIRB participation is either voluntary or compelled through powers to refer by another regulatory body.
- Minimum required so as to not interfere with other law enforcement, national security, or other regulatory activities.

30. To what extent should the CIRB be covered by a ‘limited use obligation’, similar to that proposed for ASD and the Cyber Coordinator?

Information voluntarily provided to CIRB must receive the same effective protection as legal privilege would, even though the information shared to CIRB is not a purpose where legal privilege could be claimed.

Information provided to CIRB where compelled by another regulatory body should be covered by usage and obligations set forth in the relevant regulation

31. **What enforcement mechanism(s) should apply if entities fail to comply with the information gathering powers of the CIRB?**

    There should be no powers, only what is volunteered or compelled by the powers conferred by another regulatory body.

32. **What design features are required to ensure that a CIRB remains impartial and maintains credibility when conducting reviews of cyber incidents?**

    Following existing Government policies and values with membership held by Government appointed officers.

33. **What design features are required to ensure a CIRB can maintain the integrity of and protection over sensitive information?**

    Handled by existing government policy and processes for appointments.

    AGSVA clearance commensurate with the system classification and the nature of the event, with Baseline as a minimum requirement.

Additional feedback addressing measure 4

It is anticipated that Home Affairs would be focused on ensuring transparency in any proposed processes to ensure trust within the industry. This would be supported by legislative and other mandatory obligations.

The penalties within existing legislation, where obligations are not met, appear to be sufficient. The impacts of cyber security incidents having commercial ramifications and brand reputational factors of disclosure.

One approach to ensuring transparency may be to include a public listing on government CIRB incident register and mandatory reporting of significant cyber incidents to the Australian Securities Investments Commission (ASIC). This would align with entities issuing press releases to inform customers and the general public of a significant cyber incident and the steps being undertaken to limit the impact on customers.

There may be an opportunity for the government and affected entities to collaborate on issuing press releases during and until investigations have concluded. This would allow for coordination with the necessary authorities to consider the timing and type of information that is disclosed to the media.

3 Part 2 - Amendments to the Security of Critical Infrastructure Act 2018

3.1 **Measure 5** - Protecting critical infrastructure Data storage systems and business critical data

34. How are you currently managing risks to your corporate networks and systems holding business critical data?

The Agency performs regular threat and risk assessments using subject matter experts to inform risk decision making and the prioritisation and selection of cost effective control measure for inclusion in the Agency workplan. The Agency is also subject to independent audits to ensure compliance obligations are being met and that risk is being appropriately managed.

35. How can the proposed amendments to the SOCI Act address the risk to data storage systems held by critical infrastructure while balancing regulatory burden?

While the "regulatory burden" is often reduced through market forces, it is important to take a balanced approach to managing risk through compliance regimes. Government measures that may achieve this balance include: supporting industry to be able to comply with effective standards, seeking security attestations / model security notices, and promoting transparency around the ways to reduce operational and supply chain risks.

The Agency sees an opportunity to elevate risk decisions to match the level of national interest in protecting key national infrastructure. There is a good foundation to leverage, based on the current work that government and industry are doing to enhance Risk Management Plans (RMPs) and other controls. A potential extension to this work is to find a mechanism to accurately assess the net consequences, born by all Australians, should a major incident or outage occur. This may lead to tightening of regulations and compliance obligations with minimum security standards, more quickly, for some parts of industry.

The public and media observations, in respect of recent national scale cyber breaches, have revealed that a "discretionary risk" approach may not be able to rapidly lower risk outcomes. The rate of change of the current threat environment requires a rapid shift of industry to safer systems.

The Agency recognises that regulating minimum standards and additional compliance requirements, may require sector-specific approaches. The compliance model needs to be developed in collaboration with industry and result in security maturity roadmaps that consider other elements, such as the size of different businesses. While larger Australian and global businesses have greater access to resources, Small and Medium Enterprises (SMEs) are often more limited by capacity and available resources to adapt to new regulations. It will be important to give industries and the different sectors and segments sufficient time to innovate and deliver cost effective solutions. This approach has the potential to lower the overall cost to those industries, as the larger may evolve their model to become service providers that offer cost-effective security and risk management solutions to SMEs.

36. What would be the financial and non-financial impacts of the proposed amendments?

A holistic risk assessment can be very effective if it results in regulations and compliance with standards. While government regulators are best placed to perform this comprehensive risk assessment on behalf of the relevant sector and set the standards of compliance, other self-assessment tools and guidance materials are needed to support the diversity of organisations and minimise the financial and non-financial impacts of the proposed amendments.

A significant opportunity exists to align with internationally recognised standards as this provides a larger selection of cyber security products and services than is available using domestic publications such as the Information Security Manual (ISM). There are also messaging around everyone having a role to play in the nation’s and their personal cyber security.

A good example of commoditisation when compliance standards are introduced can be observed with the payment card industry PCI compliance standard. All businesses across the globe now have cost effective payment solutions *because* of well-defined and robust standards which eliminated discretionary risk assessment in favour of compliance. Similarly, families that are “burdened” with compliance and the use of child seats in their vehicles which must comply with standards can now be purchased for a nominal sum. By enforcing compliance aligned with international standards the market continually demonstrates the ability to provide cost effective solutions which deliver net economic benefit and reduced harm.

To what extent would the proposed obligations impact the ability to effectively use data for business purposes?

Not applicable as the Agency is a government entity rather than a business.

3.2 **Measure 6** - Improving our national response to the consequences of significant incidents

Consequence management powers

37. How would a directions power assist you in taking action to address the consequences of an incident?

The Agency would welcome powers that assist in managing the consequences of a cyber security incident, in particular connected systems that pose a threat to the My Health Record system.

It will be important that such powers if used, will result in consistent outcomes and a holistic approach to security maturity .

38. What other legislation or policy frameworks (e.g., at a state and territory level) would interact with the proposed consequence management power and should be considered prior to its use?

The Agency does not have responsibility for any legislation and is limited to perspectives as the System Operator of the My Health Record system, as delegated by the Department of Health and Aged Care.

39. What principles, safeguards and oversight mechanisms should Government establish to manage the use of a consequence management power?

Not applicable, as above.

3.3 **Measure 7** - Simplifying how government and industry shares information in crisis situations Protected information provisions

40. How can the current information sharing regime under the SOCI Act be improved?

The establishment of agreed protocols for using secure communication channels between parties during a crisis, would further enable a nationally coordinated effort to addressing crisis situations.

41. How would a move towards a 'harm-based' threshold for information disclosure impact your decision-making? Would this change make it easier or more difficult to determine if information held by your asset should be disclosed?

Adopting an objective decision method for determining the impact of harm to be measured against a defined threshold would provide valuable additional certainty and efficiency to decision making.

Adopting a harm based threshold test based on subjective and ambiguous "reasonableness" terms that are written into law to be argued by lawyers would make it more difficult.

3.4 **Measure 8** - Enforcing critical infrastructure risk management obligations Review and remedy powers

42. How would the proposed review and remedy power impact your approach to preventative risk?

The Agency supports the proposed powers and adoption of minimum standards for benchmark/review and remedy. The Agency has recommended adoption of international standards in Measure 9 that can promote market efficiencies.

3.5 **Measure 9** - Consolidating telecommunication security requirements Telecommunications sector security under the SOCI Act

43. What security standards are most relevant for the development of an RMP?

The Agency understands that a balance between risk reduction through compliance and economic cost is an important consideration.

The Agency recommends:

- **the adoption of international standards where possible as a measure to drive economical cyber security outcomes**. Continued use of local security guides has hampered availability of tools and services that would otherwise be available if international standards were adopted. In particular security compliance reporting, security KPI assessment and reporting tools are anchored to NIST functional domains, and there is no official mapping of the local guidelines to NIST.
- **Endorse adoption and recognition of ISO/IEC 27001 and NIST in the PSPF as cyber security recommendations of Government.**
- **Retire the ACSC Information Security Manual (ISM) and IRAP**. Rationale:
  - the ISM is a set of subjective guidelines, not a standard.
  - the IRAP is not conducted as certification, and it does not have the quality of audit required of a certification standard.

- IRAP assessors are not readily available across the Australian continent, whilst ISO 27001 audit services are available in much higher supply.
- the ISM and IRAP has created a high-cost burden for implementation at the expense of more affordable and higher quality certification options such as ISO 27001 audits with controls from NIST standards.
- the ISM provides thin guidance. As a result, the ISM is ambiguous compared to ISO and NIST specifications, whilst at the same time the ISM refers to NIST in a non-normative fashion. This ambiguity results in higher cyber security implementation and assessment costs, as well as large variance in the standard of assessment.
- The ISM often lags the international community by several years, yet the cyber security threats faced by Australia is largely the same. Compare the publications, standards and regulations established by NIST, NTIA and CISA in the USA in respect of software supply chain security and AI, vs the lack of publications or standards by the Australian Government and it is clear we are falling further behind each year.
- with Australia falling further behind in respect of adopting security standards, it is likely to leave the nation as a soft target unless the current position changes.
- the NSW Government has adopted NIST cyber security standards.
- the ISM has significant churn each quarter because it lacks the quality, foresight, and investment present in mature international standards. This tinkering would be fine if the ISM demonstrably addressed current and emerging threats, but as evidenced by the current ISM there is a distinct lack of controls for addressing cyber security supply chain and AI threats. This exacerbates an already difficult situation of needing to meet compliance with a changing ISM and yet failing to address current threats.
- the ISM does not identify the threats that have given rise to the ISM controls and guidelines. This lack of transparency leaves organisations that must perform risk assessment in quite a bind. On one hand there is the expectation of compliance with ISM controls and on the other, unstated threats and no obvious way to assess the efficacy of the ISM control prescriptions as there is no relationship to any stated threat.
- The ISM has structural issues, as evidenced by the constant tinkering with the control wording. ISM controls conflate many different concerns, and often include many distinct control elements under a single control. This creates ambiguity for implementers and assessors. Controls use random identifiers rather than an organised standards like NIST, ISO 27002 or almost any comparable international standard.
- given there are very few products and services available for the latest edition of the ISM, organisations must procure international products and services which are aligned to robust international standards and then have the added cost of demonstrating compliance with the ISM.
- The domestic market is too small to support innovation by Australian businesses developing a local flavour of security products and services, whilst ignoring the much larger international market. The domestic cyber security

industry would be fostered by aligning to standards internationally and this would lead to additional competition and lower cost and increases in cyber security exports.

- Recommended standards alignment:
  - ISO 27001 Information Security Management Systems
  - ISO 27002 Information security, cybersecurity, and privacy protection
  - NIST CSF Cybersecurity Framework 2.0
  - NIST 800-53 Security and Privacy Controls for Information Systems and Organizations
  - NIST 800-30r1 Guide for Conducting Risk Assessments
  - NIST 800-39 Managing Information Security Risk: Organization, Mission, and Information System View
  - NIST 800-37 Risk Management Framework for Information Systems and Organizations
  - NIST SP 800-161 with updated guidance from EO 14028.
  - ISA99 Industrial Automation and Control Systems Security
  - ISA/IEC 62443 Security for industrial automation and control systems

44. How do other state, territory or Commonwealth requirements interact with the development of an RMP?

Within healthcare a number of existing powers and regulatory regimes may have the potential to interact with development of an RMP for Systems of National Significance, and Systems of Government Significance. The Agency recommends a consistent approach be used and align the *Privacy Act 1988*, and other relevant legislation to industry classifications. Home Affairs may need further consultation with the Department of Health and Aged Care to explore the best approach to leveraging existing legislation, such as the *My Health Records Act 2012*. Noting this would only capture healthcare businesses that participate in this system.

The Department of Health and Aged Care would be best placed to comment and advise on this matter, as the owner of the legislation and with a broader remit and view of the Commonwealth and jurisdictional health ecosystem and regulatory environments.

45. What are the main barriers to engaging with government through the notification process as it is currently enforced? How can the obligation to notify be clarified?

Implementing “limited use” powers to promote information sharing.

46. How do your procurement and network change management processes align with the existing and proposed notification arrangements? Can you suggest improvements to accommodate industry practice?

Procurement and change management can be improved by enforcing supply chain transparency similar to the US Executive Order 14028, and the NTIA, CISA and NIST standards.

NIST in SP 800-161 is being updated as a direct outcome of EO 14028 and should be monitored for adoption.

https://csrc.nist.gov/pubs/sp/800/161/r1/final

https://www.nist.gov/itl/executive-order-14028-improving-nations-cybersecurity

47. How can outlining material risks help you adopt a more uniform approach to the notification obligation?

To date, Home Affairs has not provided clearly articulated risks in a form with sufficient detail, including:

- applying a robust threat and risk assessment methodology that stands up to public scrutiny;
- threat scenarios clearly articulated with the chain of events that lead to an adverse event outlined. This is often referred to as the 'kill-chain' and assists with identification of appropriate and cost effective multi-layered controls; and
- assessment of the likelihood of the threat event occurring using relevant contextual factors to determine the inherent risk and the residual risk after implementing the controls.

The Agency supports reform and improvement of security posture across the health sector. This represents an opportunity to look for other ways to increase transparency and security maturity across the sector by sharing the threat modelling behind the legislative controls being proposed by Home Affairs.

It would be helpful if Home Affairs can publish the threat modelling and risk assessments that justify the proposed reforms (noting there may be some need to redact any sensitive information) for the following reasons:

- To assist organisations in understanding the threats and risks that have informed the regulatory obligations; and
- To promote transparency of the risk and threats, and assist organisations to assess their true inherent risk, tailor their controls, or assess their residual risk based on the maturity of their control implementations.

END OF RESPONSE.