VeroGuard Systems

1 March 2024

Department of Home Affairs and Cyber Security
PO BOX 25
Belconnen ACT 2616

Dear Sir/Madam

Cyber Security Legislative Reforms

Thank you for the opportunity to participate in the consultation on proposed new cyber security legislation and on changes to the Security of Critical Infrastructure Act 2018.

We are delighted to provide our responses to the Consultation Paper.

We welcome any questions or clarification requests about this submission.

Please contact myself for any further information.

Yours faithfully

[redacted]

Nicholas Nuske
Director and CEO
VeroGuard Systems Pty Ltd

[redacted]

Responses to Consultation Paper

Part 1 – New cyber security legislation

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?

The manufacturer or distributor of the product needs to be responsible. As most consumer goods are manufactured outside of Australia the standard needs to cover both. Only the manufacturer can integrate into the product and the distributor needs to ensure that what they are selling complies with the standard.

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

Whilst it is important for Australia to align with global best practice standards to ensure that manufacturers have consistent standards to work to, the Cyber Security for Consumer Internet of Things (CSCIoT) standard, called ETSI EN 303 645, is designed to set a baseline for consumer goods, but falls far short of the professional IoT standard called IEC 62443. This raises several important questions.

a. **Is the protection of a consumers enviornment less important than the protection of a business or government to that consumer?**

b. **It can be argued that a consumer needs more protection than a business or government customer who has better resources to protect devices from cyber incidents.**

c. **Do the goods built as consumer products never get used in a business or government environment?**

d. **Could the gradation method of IEC 62443 extend down to consumers?**

Australia wants to be a leader in cyber security by 2030. Adopting compromised standards with ineffective gradation is leaving consumer products and consumers (and by extension many small businesses) unnecessarily exposed when a stronger common standard could and should be adopted up front.

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

- **International Electrotechnical Commission (IEC) 62443.**
- **Recommendations from IoT Security Foundation could be assessed and applied to ETSI EN303 645 with improvements such as gradation.**

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?

Consistency is critical across the globe for standards to be effective. It is more likely that global manufacturers will comply if the standards are consistent and broadly adopted by multiple countries or markets. The definitions in PSTI act are a good starting point however these would need practical implementation and ongoing improvement.

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

The less exceptions the better. Any connected device should be covered.

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

Australia should adopt timeframes that are consistent with other countries, such as the United Kingdom. Timelines should be as aggressive as possible as each passing year sees a significant number of smart devices enter the market with potential vulnerabilities exposing consumers to cyber criminals.

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

Even if the Regulatory Powers Act provides a suitable framework for monitoring compliance and enforcement of a standard, the Government and industry will need to have effective programs for catching non-compliance prior to the discovery of breaches which are most likely to manifest themselves in largescale cybercrime breaches.

Measure 2: *Further understanding cyber incidents – Ransomware reporting for businesses*

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

- The organisation and the industry it operates in.
- The date and time the incident was identified and the duration of the incident.
- The incident type (known or unknown).
- Details of adversary demands.
- The organisations response:
    - Technical (remediation).
    - Public communications.
    - Operational (continuity and remediation).
    - To criminal.
- The effect (impact) on:
    - the organisation.
    - customers; and
    - its partners (ecosystem).

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

- Any negotiation process that has occurred and the result of that process including the amount demanded and the amount paid.
- What data was recovered (if stolen) and what percentage of total data of the organisation does that represent.
- Were systems restored and percentage.
- Does the organisation believe that the threat has been entirely removed and when.

10 What is the appropriate scope of a ransomware reporting obligation to increase visibility of ransomware and cyber extortion threats, whilst minimising the regulatory burden on entities with less capacity to fulfil these obligations?

All organisations must report. If this does not happen, the scale of the problem and solutions to the problem will not be effective. (If it's not reported it can't be measured). Smaller organisations should have a minimum reporting obligation. Organisations with over 500 employees should be required to provide detailed and ongoing information.

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?

No – please view answers to question 10 above.

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?

As soon as an incident occurs there should be a basic level of detail reported (case opened):

- Organisation and industry.
- Date, time incident was identified and duration of incident.
- Incident type (known or unknown).
- Estimated number of impacted customers.
- Systems impacted.
- Number and potential number of records/people impacted.

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

Clearly an organisation is more likely to report if there are no punitive consequences to reporting. However organisations and directors should be held accountable to customers, shareholders and their partners on their obligations to maintain an appropriate level of cyber security to protect the continuity of their services, PII and other sensitive information.

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

Whilst the Government should not fine an organisation for paying a ransom or for experiencing a breach, it must hand down punitive measures for breaches of PII, leaks of classified information or where an organisation has experienced an avoidable breach impacting the availability of critical infrastructure.

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

Fines for failure to report an incident. The longer it takes to report, the higher the fine. Consideration should be given to establishing a 'name and shame' register.

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

For the type of information, please see answers to questions 8 and 9.

Ideally information should be available in real time to enable cyber security professionals and boards to be provided with relevant data.

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?**

Please view detailed information associated with answers 8 and 9.

18 **What restrictions, if any, should apply to the use or sharing of cyber incident information provided to ASD or the Cyber Coordinator?**

To be determined on a case by case basis by the National Co-ordinator but communicated to the effected entity prior to release.

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?**

Organisations are already incentivised to avoid incidents (business impact, cost of a breach, reputation damage).

The Government should:

- Set and enforce strong standards.
- Help remediate and advise when an incident if it occurs.
- Communicate information to others to prevent like incidents.
- Take punitive measures for breaches of standards.
- Require minimum standards of organisations working with Government, and ensure they are enforced.

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)?**

- Assess ongoing threats and actions taken by Government.
- Report on common issues and make recommendations to:
  - Provide the information to Government to give it insights on current and emerging threats.
  - Work with ASD to issue directives for Government agencies and critical infrastructure suppliers (e.g.: CISA directives in the US).
  - Provide bulletins and information to industry for education/awareness.
  - Advise on proposed updates to:
    - Government guidelines (e.g.: the Essential Eight).
    - Standards.

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

The CIRB's role should be limited to making recommendations and communicating with organisations specifically about the information it has available to it, for the sole purpose of helping these established functions and, ultimately, interested organisations better understand how to avoid breaches.

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

A CIRB team, independent of the data collection team, should assess the facts of the incident. It should also monitor the organisation's response against the Government guidelines to provide ongoing aggregated reporting on learnings and further guidance. This would be conducted without necessarily knowing the details of the organisation until after the review has been completed. This exercise should not be an assessment of compliance.

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

The overriding factors should be whether:

- The breach had any impact on continuity of operations by a critical infrastructure industry.
- Or there were any leaks of any PII, payment data (eg: credit card) or classified data.

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

A broad cross representation from the cyber security industry, (local and international companies and associations), legal, academic and business. This mix should attempt to avoid having limited perspectives on the problem, the solution, and cyber strategy (for example, representation purely from critical infrastructure companies will have a conflict of interest, as would represtation purely from organisations that focus on detection and remediation services).

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?

Please view our answer to question 24 and:

- Risk management and actuarial (eg insurance).
- Cross domain cyber security experience (hardware, software, services, identity, detection and remediation) - identity is core to any cyber security strategy/solution.
- Regulatory experience
- Legal (cyber, privacy, etc).
- Communications.
- Data sciences.

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

Similar governance to any board.

27 Who should chair a CIRB?

An effective leader/communicator who can navigate politics, government and business.

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

Set rules and refer based on the rules. If in doubt, allow the Country cyber security co-ordinator to apply discretion where required.

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

Unfettered access to breach information.

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

The CIRB needs to also have ‘limited use obligation’. The CIRB should always be under that restriction. However, significant process could be followed by a third party through established mechanisms to step outside that process. For example, where it is in the national interest, an enquiry or court process may be established to access and/or release the information.

31 What enforcement mechanism(s) should apply for failure to comply with the information gathering powers of the CIRB?

- Fines.
- Impacts on licences (where they exist).

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

- Independence and broad make up of board.
- Vetting and clearances of members.
- Independent assessment of quality of information and recommendations by the CIRB.
- Power to access all relevant information.
- Access by board members to ASD and ACSC expertise.
- Regular independent review of impartiality of board members.

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

Please view our answer to question 32 and:

- Strongest cyber security practices itself.
- Adopt sovereign capability and technology to be independent of foreign influence.

Part 2 – Amendments to the SOCI Act

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?

- Complying to Essential Eight.
- Certifying systems.
- Applying stronger authentication to all systems, networks and data, not just critical or classified systems (criminals are breaching non-sensitive systems as an entry point to ellevate privileges).
- Getting third party assessments of architecture.
- Penetration testing.
- Keeping up to date with latest threats.
- Maintaining robust continuity and back up capability.

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?

The Government must take action and hold critical infrastructure suppliers accountable for what they can control. Standards must not be watered down. Leaders are already aware of the problem. Allianz Insurance recently published their Risk Barometer for 2024, shedding light on the top global business risks. According to this comprehensive study, cyber incidents have emerged as the foremost concern for companies worldwide. These include data breaches, attacks on critical infrastructure, and ransomware attacks. They now occupy the top spot, accounting for 36% of overall responses. Notably, this is the third consecutive year that cyber incidents have claimed this position, and for the first time, they lead by a clear margin of 5% points. In countries like Australia, France, Germany, India, Japan, the United Kingdom, and the United States of America, cyber risk is particularly pronounced.

By making the standards clear, companies will adjust.

- It is important not to change the standards too often or too radically once they are set.
- The standards must be consistent with standards being implemented in other parts of the world because, for companies to operate in these other parts of the world, the companies will often have to comply with those regualtions anyway.
- The cost of a breach will significantly outweigh any cost of complying with reasonable requirements.
- There are technologies available that add value to digital environments without compromising security.

36 What would be the financial and non-financial impacts of the proposed amendments? To what extent would the proposed obligations impact the ability to effectively use data for business purposes?

There are technologies available that not only meet the highest of protection needs, but also lift cyber posture and capability without restricting the use of data for business purposes. Do not water down the standards.

Measure 6: ***Improving our national response to the consequences of significant incidents – Consequence management powers***

37 How would the proposed directions power assist you in taking action to address the consequences of an incident, such as a major cyber attack on your critical infrastructure asset?

Generally, the proposed directions power is beneficial as it would provide particpants with access to experience and expertise on how to minimise an indicent’s impact, deal with an adversary, remediate the problem and communicate with stakeholders on the breach in a timely and effective way.

Specifically:

(a) **Directions when no existing power to support a fast and effective response**:

The effectiveness of a direction will be predicated on the availability of information to the Minister to enable the direction to be sufficiently relevant and targeted to the immediate issue. Problems will arise if the direction is too broard or does not address the critical immediate or percieved consequent issue(s). Timely consultation with the effected organisation to ensure that a direction is approrpiate will be critical, but the power will also need to provide flexibility to the government to impose actions that the organisation may not agree to where the entity does not itself, for whatever reason, agree to work with the Minister but the criticality of the overriding public interest in addressing the issue requires action. Where a direction is given, the organisation must then have no liability for following the direction, even if the act of following breaches some other law of the Commonwealth or a state or territory.

(b) **Document replacement**: Agree.

(c) **Disclosure of protected information**: Agree.

(d) **Information gathering**: Agree.

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?

Privacy Act 1988 (Cth).

National Data Breaches Scheme.

Consumer and Competition Act 2010 (Cth).

Division 400 of the Criminal Code 1995 (Cth).

Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth).

Corporations Act 2010 (Cth).

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

We agree with the list set out on pages 44 to 45 of the Consultation paper.

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?

We have no suggestions.

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?

The severity and impact should be assessed independently and then thresholds/rules applied.

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?

Increase focus to avoid issues and improve internal governance/risk management.

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?

No comment.

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

No comment.

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

No comment.

46 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?

No comment.

47 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?

No comment.