Australian Information Security Association

2023-2030 Australian Cyber Security Strategy Legislative Reforms Response Submission

Executive Summary

This is a response prepared by AISA on the Cyber Security Legislative Reforms, covering the two parts of the consultation paper across the 9 measures. This response was prepared using feedback collected from AISA's member base, community members and senior executive members of the Executive Advisory Board for Cyber (EABC).

Comprehensive feedback has been collected over the past two months through in-person town halls and roundtables organised across most Australian capital cities and through an online survey.

We appreciate the engagement provided by the Department of Home Affairs and the Cyber Security Minister's office. We commend the team for attending meetings and roundtables with AISA representatives to discuss various aspects of the consultation paper and provide context to the different measures. We welcome these efforts and encourage continued engagement on matters related to the cyber security strategy and its implementation.

Akash Mittal
Chair, AISA Board of Directors

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?

To streamline the compliance processes, it is recommended that it should be the responsibility of all parties involved in the supply chain to ensure that their products, parts for a product, and any components of a smart device that connects to a network or internet meets the required standards. This could include goods and parts importers, manufacturers, retailers and distributors. As components move through the supply chain, each acquirer can gain confidence from their supplier that the components meet the minimum mandatory cyber security standard. This is like managing third- and fourth-party risks within the supply chain. This approach can improve accountability and traceability within the industry and assist with managing issues related to vulnerability management. By making all parties work together with transparency and accountability, we can protect common consumers, who may have limited knowledge about cyber security. Otherwise, the implementation of mandatory minimum standards for smart devices could be challenging, and finger-pointing could create confusion within the industry.

As the physical and digital aspects of our lives become more linked, the government should consider the impact this could have on awareness needs in other sectors and industries. For example, licensing requirements for physical security companies and individuals may need to be updated to include awareness of cyber risks associated with the use of smart devices, such as CCTV cameras. This would help ensure that those responsible for physical security are also equipped to address potential cyber threats.

As the use of smart devices becomes more widespread, it is important to consider how to raise awareness of cyber security standards among different groups of people. For example, individuals with disabilities who use smart devices such as wheelchairs, people from low socio-economic backgrounds, and the elderly may need to be made aware of these standards when purchasing smart devices. This can help ensure that they can make informed decisions and protect themselves from ongoing potential cyber threats.

This is in alignment with other standards such as Electrical and Telecommunications to ensure compliance with any obligations as devices are imported.

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?

According to the feedback received by AISA, the three principles outlined in the ETSI EN 303 645 standard, which includes:

- **No universal default passwords;**
- **A means to manage vulnerability reports; and**
- **Keeping software updated**

These are foundational controls for implementing standard minimum requirements for IoT devices. This approach enables the adoption of an existing international standard without the need to create new requirements or standards specific to Australia. It also allows the industry to adopt principles that are already globally required and provides a less onerous approach to setting minimum standards, while offering good coverage for cyber security threats addressed by the three selected principles. These principles have the greatest impact on securing consumer devices and ensuring that they can be updated as security requirements change.

The two main pieces of feedback on this topic were:

- ✓ the need for a mechanism to make the general consumer aware of these principles and their responsibilities, and
- ✓ the need to simplify the software update process using a model like mobile phones (Apple iOS/Android)

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

Governments worldwide are beginning to regulate the standards for consumer-grade devices and technology. In addition to the EU, two other standards that could serve as baseline controls for consumer-grade IoT devices are those developed by ISO and NIST. These standards are comprehensive and are updated periodically to address changing threats to these devices.

The following two are the specific standards which should be considered as part of Australian Legislation:

- ISO/IEC 27402:2023: IoT security and privacy Device baseline requirements
- NIST IR 8425: Profile of the IoT Core Baseline for Consumer IoT Products

Based on the feedback received, aligning with existing international standards where possible would be supported, as it ensures that products produced globally meet international standards.

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 TSI Act in the UK?

Aligning the definition of smart devices subject to an Australian mandatory standard with that used in the UK's Product Safety and Telecommunications Infrastructure (PTSI) Act could be beneficial. The definition in the PTSI Act covers a wide range of consumer-grade IoT devices including:

- **Internet-connectable**
- **Network-connectable products**
- **A product that is not an 'exempt product'**

Exceptions could be made for specific legislation that supersedes the baseline requirements, such as IoT for cars. This would ensure that minimum baseline standards are applied consistently across the board.

The definition should be periodically reviewed to keep up with technological advancements.

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

According to the previous point, we support that no devices outside the definition of network-connected devices should be excluded. If a device connects to a network or the internet, it should be subject to the minimum standard requirements.

However, a more cautious approach should be taken when applying these minimum standard requirements to the following:

- **Medical devices, or where there is significant impact to human life**
- **Disability assistance devices**
- **Devices in sectors such as aviation, where existing security requirements are of a higher standard than the minimum standard requirements**

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

A phased approach, spanning from when the minimum standards become legislation to 36 months, will be necessary. The government should take two approaches to implement the standards and provide maximum coverage for existing and new devices during the transition/catch-up phase:

Approach 1 - Address existing devices in use or on the market for sale. Manufacturers and assemblers of smart devices released within the last 12 months should release a document instructing how to change default passwords, provide updates for known vulnerabilities, and report new vulnerabilities, including steps consumers should take to protect themselves.

Approach 2 - Address new smart devices by following the three principles for minimum standards, implementing a last patch date to educate consumers, and introducing a star rating concept similar to the Health Star rating, with three ticks for compliance with the three minimum principles.

The government should be aware that initial implementation may be slow due to resourcing availability of companies to make the necessary changes. Over time, companies will catch up, and a 3-year period should support them in resourcing to meet the new requirements. Frequent consultation and feedback between the industry and the government will be necessary to address challenges and changing requirements. The government should also support the industry in imposing these requirements on overseas suppliers of smart devices, particularly those from countries such as China and Russia.

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

It appears that there is no need for a separate enforcement mechanism for IoT legislation, and that the current Regulatory Power Act should provide a suitable framework for monitoring compliance and enforcement mechanism.

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 common feedback on the subject suggests that reporting should primarily focus on the following aspects:

- Any available threat intelligence at the time of reporting to help government agencies verify attack signatures and determine if the threat is unique, state-sponsored, or affecting multiple businesses
- While victim information should be discretionary, disclosing the sector or industry should be mandatory including if the business is small, medium or an enterprise
- Information about the ransom demanded or paid, including transaction details, with victim information being optional

There is also a demand for a phased reporting process, where a company can initiate a report at the early stages of a ransomware incident and continue to provide more information as the threat intelligence evolves. This would allow for different levels of mandatory information to be provided based on the information available at the time of reporting.

However, there is a general reluctance within the industry to report incidents or to disclose complete information. The industry supports the option to anonymously report a Ransomware or Extortion attempt initially. This would enable the victim to report their situation at the early stages of an incident without the fear of it being a false positive event. It is believed that if this option is not available, organisations may be hesitant to report until the issue is fully understood, making it difficult to comply with the 72-hour window as per Question 12.

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

In a situation where a ransom is paid, it is essential to report the incident and include details about the payment, such as:

- **the method of transaction**
- **the amount paid and the currency used**
- **the date of the transaction**
- **the attacker's account details**
- **any information about the attacker who carried out the ransomware attack should also be included**

There is support within the industry for recording and notifying these incidents to better understand the scope of the problem. However, it is important to protect the identity of the victim throughout the process and, if an organisation chooses to disclose their identity, they should be protected from any consequence management.

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

The scope of reporting ransom payments should include all entities and individuals, without any regulatory or legislative requirements. Reporting should be open to everyone, with the option for complete anonymity.

As mentioned in the previous answer to Question 9, a reporting entity or individual may choose to disclose their identity and seek government support when dealing with a ransomware or extortion threat. This will allow us to understand the scope of the problem and provide useful information to protect against the threat of ransomware.

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?

Right now in Australia, dealing with ransomware requires more collaboration and assistance, rather than an obligation. The industry needs support and understanding to handle threats like ransomware without the fear of regulatory burden.

Regarding the turnover threshold, companies with access to over $10 million per year have the resources to hire experts and engage consultancy firms to deal with cyber threats. Also, this threshold only includes a small number of companies.

Lowering the threshold to an annual turnover of more than $3 million would include a larger group of companies and provide a more significant data sample to better understand the problem. Lowering the threshold would also provide better visibility to government and industry stakeholders. Also, the government could provide support to smaller organisations as part of the reporting process by offering clear advice based on their stage in the attack process, as part of the Ransomware playbooks being developed by the government.

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?

We believe that given an appropriate scope and triggers for notification of an incident, aligning the timing with the 72 hours specified as part of the SOCI Act would make sense. We agree with the existing sentiment that alignment of obligations would make compliance easier. This is contingent on where the mandatory component lies. As noted in Question 8, the 72-hour window becomes difficult where an incident is unfolding and not all information is to hand.

In cases where a ransom has already been paid, it could be mandated to report the incident within a 24-hour period. The first 24 hours after a ransom payment can be crucial in understanding the motives, scale, and nature of the attacker. Again, this reporting should be allowed with full anonymity choice from the victim.

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

In our opinion, the no-fault and no-liability principles are a positive development for the industry and could increase confidence for entities reporting a ransomware or cyber extortion incident. However, additional measures are also necessary to promote openness within the industry, such as:

- The option for anonymity when reporting a ransomware incident
- If a reporting entity chooses to share identifiable information, the details

of the report will only be used by the relevant government agency and will not be shared with any legislative or regulatory bodies

- Engagement should be driven by incentives and offers of help and support. A program based on assistance and incentives can help build confidence and bridge the gap between personnel who are most impacted and want to collaborate (such as CISOs, Cyber Teams, and Risk Teams) and personnel who may be more resistant (such as CEOs, CFOs, and Legal Teams)

It is certainly a positive step in the right direction, but it needs to include elements of collaboration and no consequence management. As one of our well-known Executive Advisory Board Committee members said, "The government needs to woo the industry to start a courtship."

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?

In our view, this marks the beginning of a new relationship between industry and government, one that should be based on collaboration, assistance, and a change in the way industry perceives the government.

This collaboration and openness will drive a fundamental shift in the industry's accountability, maturity, and overall cyber resilience.

The goal of the no-fault and no-liability principles should be to bring the industry and government together to work towards making Australia the world's most cyber-secure country by 2030.

Legislative reforms and regulatory bodies should serve as oversight tools for managing accountability and consequence management. This new initiative should focus on promoting the right behaviours for a fundamental shift in how the industry, government, and public become more cyber-resilient through collaboration.

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

The industry needs support and the right assistance when dealing with an issue like ransomware. It is important to understand that this is an unprecedented situation with little information available in most cases at the start of the incident. In such circumstances, entities need help and a partner to work with in confidence to deal with the crisis and protect the best interests of their customers. The government and its agencies have the capabilities to offer assistance in such circumstances. The government should advertise these capabilities, share use case stories where the government has assisted companies in dealing with ransomware attacks, and socialise the resources available for entities.

Questions from our membership have also covered the question of how this would be administered, particularly the identification of unreported incidents to the government. Would this only apply to incidents that made it to the general media? The definition of the point at which an incident is reportable will also be important in framing the enforcement mechanisms.

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?

In general, the Cyber Security community would benefit from key information such as

- **the type of attack being attempted**
- **attack techniques and initial access points**
- **any IOCs related to the incident**
- **the industry or sector that was attacked**
- **details about the attacker such as whether they were state-sponsored**

Feedback from our consultations suggests that the government may have access to intelligence greater than what organisations and third parties have access to through commercial arrangements. It is felt that if higher-level anonymised intelligence is available, this will improve the overall Cyber Security capability of the country

We believe that an improved version of the CTIS would be an appropriate mechanism for delivering ongoing incident information. If a broader audience is required, the ACSC alerts page is also appropriate. The data released should be timely and ongoing to enable organisations to ensure that their control measures and detection capabilities can respond to evolving threats.

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?

In our opinion a broad-blanket obligation (legislation) approach is unlikely to encourage industry participation. The industry is concerned that although the obligation limits the use of information, it does not prevent the sharing of information. This means that ASD can still share information with the Cyber Coordinator and other agencies, including law enforcement, national security, intelligence agencies, and regulators. This raises the question of whether the shared information could end up with a regulator and be used for consequence management, such as a regulatory investigation.

We do recognise that such a requirement will be necessary for:

1. **critical infrastructure, organisations where SOCI is relevant, and**
2. **in scenarios where serious harm is a concern.**

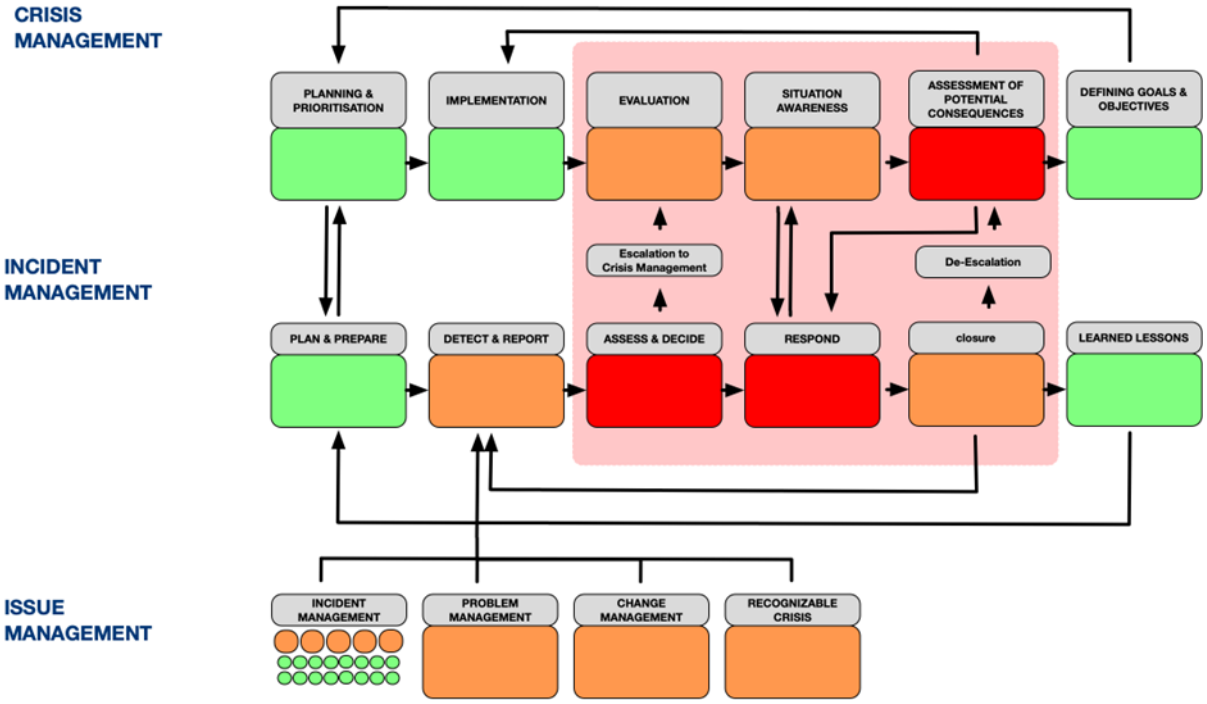
It is concerning for the industry that the government's focus is on engagement during cyber incidents. The reality is that no entity will think of reporting or engaging with the government during a cyber security incident. Their primary focus will be to restore services and protect the best interests of the organisation. Unfortunately, the industry-government relationship is not there yet.

Cyber resilience is a journey that starts early on, from threat intelligence all the way to crisis management. We believe that government efforts need to be across these stages and build strong relationships at the threat intelligence/ issue management phase, rather than coming in during a cyber incident. This approach will ensure:

- early engagement between the industry and government
- threat intel sharing and learning on how to combat potential cyber incidents
- organic government involvement if a threat is executed against a particular entity
- government involvement all the way through crisis management

The common feedback from members of AISA's Executive Advisory Board for Cyber (EABC) is that the industry needs a Centre of Excellence that would allow for stronger two-way sharing and collaboration. If the government is looking to improve cyber incident reporting, the best way to do this is to facilitate a bridge between not just the government, but also other industry players.

The government should also publicise more framework guidance on security issue management, and how it collaborates with cyber incident response/management, and further how this escalates to crisis management. In the words of a prominent EABC industry CISO, "To use an analogy of irrigation, the government is asking a farmer to allow it to turn on the taps, but not explaining how/when/where that water flow is going to work. In other words, the industry needs a commitment from the government to document and provide frameworks for incident response." An image has been created to illustrate the relationship between issues, incidents, and crisis, using best practices like ISO27035:2023 and ISO22361:2019 for incident management and crisis management.



Credit: Nigel Hedges

It is also noted that Cyber Threat Intelligence Shared (CTIS) platform is not being expanded to assist with threat intelligence gathering. CTIS allows for one way and two-way communication and sharing of incident information between ACSC (ASD) and network partners. This could be mutually beneficial for both the industry and the Government and provide an opportunity to collaborate proactively even before an incident occurs.

Part 2 – Amendments to the SOCI Act

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

In general, the industry is eager for help and support when dealing with cyber security-related risks and welcomes collaboration opportunities from both within the industry and from the government. However, there is an overarching fear about how information shared for the purpose of awareness about a cyber incident could be used for consequence management. Anything that could lead to legal liability will concern organisations, so it's not so much about what information is shared, but rather the:

- purpose
- intent, and
- long-term view of how the information will be used

The government, agencies, or regulators should clarify what they will do with the information, work independently of regulatory bodies, and provide assurance that the information will be protected and its purpose will not change with changes in governments or legislation. In other words, there should be a "safe harbor" for the information shared as part of the cyber incident reporting process.

1. Legal liability concerns of sharing rapidly changing information and definition of sensitive information. How these reporting organisations will be protected against future lawsuits or from being publicly mentioned.

2. The second concern is around how other agencies, ministers, and regulators will utilise the information and what will be shared in the public domain. There is currently ambiguity around the roles and responsibilities of ASD and Home Affairs when it comes to incident reporting. It is also unclear how and what type of information is shared between them (or can't be shared without the approval of the reporting organisation).

The organisations feel that they need to be protected when collaborating with Government agencies and provided with a Safe Harbour approach. A good example to learn from could be the Microsoft's Bug Bounty Program, Legal Safe Harbor policy prescribes that individuals who responsibly disclose security vulnerabilities through their bug bounty programs should not have fear of legal consequences because of their good faith attempts to comply with the bug bounty policy. The Government should encourage reporting through support and transparency, and address concerns around consequence management that may arise as a result of reporting an incident to the agencies. This would help foster a culture of openness and collaboration between the government and the industry.

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?

As covered in responses to questions 17 and 18, the industry seeks support, collaboration, and joint efforts to improve the management of cyber risks
Cyber resilience is a journey that starts early on, from threat intelligence all the way to crisis management. We believe that government efforts need to be across these stages and build strong relationships at the threat intelligence/ issue management phase, rather than coming in during a cyber incident.

The approach will ensure

- **early engagement between the industry and government,**
- **threat intel sharing and learning on how to combat potential cyber incidents,**
- **organic government involvement if a threat is executed against a particular entity, and**
- **government involvement all the way through crisis management.**

The common feedback from members of AISA's Executive Advisory Board for Cyber (EABC) is that the industry needs a Centre of Excellence that would allow for stronger two-way sharing and collaboration.

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)?

There is agreement that the proposed CIRB purpose of leading a fact based, no-fault based review of incidents that are of National Significance or Importance are reviewed as per the proposed functions.

The CIRB should strive to ensure that the Public is well apprised of the cause and any recommendations that can be taken by all stakeholders in the community, including ensuring the public can protect itself.

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 should operate as per the ATSB model of operating in harmony with any Government bodies such as Law Enforcement, National Security, Intelligence and Regulators.

It should be noted that there is a concern with the timeliness of information provided by the CIRB to technical groups if the review takes place well after the Cyber Event has occurred. This should be considered as part of the implementation, as a key value proposition in the learnings or intelligence shared with other organisations.

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

We are supportive of the 'no-fault' approach and view this as key to the success of the CIRB. Specifically the CIRB should adopt the ATSB principles listed in the consultation paper to provide participants with the best possible ability to provide information and engage with the review board in a constructive fashion.

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

There is agreement with the proposed factors for reviewing an incident through the CIRB. In particular, events that are in the public interest are those that we feel would be the most impactful to the national security and cyber resilience capability.

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

The CIRB should be made up of a blend of Government appointed subject matter experts and also industry and/or academic experts who will be able to provide the real world context required in a review of an incident. It is noted that Expertise, Security and Conflicts of Interest will need to be considered when appointing members to the board.

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?

It is expected that there would be a broad range of expertise held collectively by the CIRB members across the disciplines of Technology, Cyber Security, Legal and Regulatory in conjunction with Government representation. This will ensure that all considerations of the information provided to the board and the recommendations provided are of interest and value to all stakeholders. The Chair and non-Government members would need a level of independence from the government processes to ensure impartiality in these reviews.

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

As part of the CIRB processes and makeup, there should be a group of members that have the ability to declare a conflict of interest and excuse themselves from any review that they may have a conflict with. All members should hold the appropriate clearances to review information provided by the CIRB

27. Who should chair a CIRB?

The feedback we have received is that there should be a new role appointed, with an independent and qualified individual to drive the review process in conjunction with the other board members.

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

There is agreement that the proposed members for instigating a review are appropriate. It has been suggested that there should be an appropriate channel for organisations or the community to lobby these parties for a review to be initiated.

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

There is a preference to use limited information gathering powers for the use of the CIRB. It is felt that this will strike the balance between compelling organisations to provide information but is not as light as a voluntary option.

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 should gather and use information only for the express purpose of conducting a review. It is felt that this is very important so that participants are likely to provide meaningful engagement to the review board. If there is not a limited use obligation then organisations may not be able to fully inform the board, which in turn will result in CIRB findings not being as comprehensive or insightful as they should be. This would work against the intent and purpose of the CIRB. Additionally if there is not a limited use obligation, then there is a preference to move to a voluntary model.

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

On the basis that limited information gathering powers are used by the CIRB, there should be appropriate powers to compel an organisation to provide appropriate information to the panel. If this is not done, then it is reasonable to expect there will be Civil Penalties, similar to the Mandatory Reporting that would be available to use.

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

A key reason for the recommendation to appoint non-government and independent industry based experts to the panel is that it inherently provides credibility and impartiality to the process. If the CIRB is made up of only Government members then it is felt that there will be queries as to the impartiality of the findings with the biases that could be inferred.

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

Critical to the intent and functioning of the CIRB is that all information provided as part of an investigation is confidential and that any findings do not adversely affect any parties in a negative manner, being through law enforcement activities, regulatory action, judicial proceedings or reputational damage for the affected organisation(s). It is envisaged that any outcomes from a CIRB investigation would result in a confidential government report and then a public report which provides information required to explain the root cause and any recommendations for other organisations to learn from.

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?

Through engagement with our members that have SOCI experience, the IT and OT Cyber Security requirements are separated in terms of security programs and investment by an organisation. Most of the security controls applied are considered on a risk-based basis and as such, key assets such as data storage systems and business critical data have tended to have good levels of controls – as any impact to these would interrupt an organisation's ability to deliver or support delivery of key functions.

Most organisations have also gone to great lengths to separate their IT and OT environments, thus reducing the risk of contagion from an attack in either environment. This should be considered as a key defence for any Critical Infrastructure organisation.

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?

To address risk and reduce regulatory burden, consolidation of the obligations into a single set of rules and regulations that organisations can follow - which is commensurate with the risks being managed - is key. There are too many different obligations at a Federal, State and Industry level that make it difficult and costly to meet these requirements. Any changes that consolidate the obligations of Critical Infrastructure organisations is needed to ensure that regulatory burden does not become a key driver of costs and complexity. We also welcome any efforts to increase ongoing consistency in the application of standards and regulation as this leads to better outcomes for organisations through the same metrics as reduced cost of compliance and not having to build or implement security practices for different regulations and legislation.

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?

Where organisations have not considered the risk of securing business critical data and supporting data storage systems, they are at risk of having to increase their investment significantly to meet the new requirements being imposed by the changes in obligations. This might include upgrading physical security controls on data storage systems held by the environment but not under the same level of security control as the OT environments.

Additionally, there would be requirements for the risk management teams to consider the larger scope of security risks being faced by IT environments as the threat and risk profile differs significantly (for example IT environments have end user and external interactions, whereas OT environments are separated logically and not exposed to internal and external users).

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?

It is agreed that in certain situations, where an impacted critical infrastructure asset has consequences that is out of an organisation's direct control (for example, triaging supplies for impacted services) then having the ability for the Government to step in would be welcome. This would enable the impacted organisation to focus on restoring their operations, whilst the Government is able to assist with the downstream impacts.

These capabilities or measures are preferred through other processes or legislation which is not as imposing as the last resort powers. Thus efforts such as the changes to the Privacy Act to resolve some of the challenges of dealing with the consequences of a cyber incident are seen as more practical.

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?

As noted in the discussion paper, there are different legislation, policy frameworks or regulations at different levels of government that interact with the last resort power. As such, it would be expected that as part of the change to the legislation, there is an effort to provide clear direction as to the order and precedence of steps that would be taken to get to an invocation of the last resort power. This is critical to ensuring that organisations and the public have confidence in how and when the last resort powers would be used.

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

The proposed safeguards and oversight mechanisms appear to be comprehensive in ensuring that the last resort powers cannot be invoked easily and without due cause. As per Question 38, it is expected that all of the oversight controls are clear and able to be understood by the security community.

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 support the government's efforts to define protected information and have a consistent approach across all obligations, not just within the SOCI Act. It is agreed that sharing of information, in particular Cyber Security events involving or affecting Critical Infrastructure operators is imperative in continuing to improve the ability to detect and respond to Cyber Security Events.

It is recommended that a specific, Critical Infrastructure based threat intelligence network is created so that the lines of communication between the Government and Critical Infrastructure operators are able to be managed. This would also enable timely and potentially sensitive information to be able to be shared to an appropriate audience (like the non-disclosure deeds employed by the ACSC).

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 feedback we have received is that moving to a harm-based model would make it easier to determine if information should or could be disclosed in the event of a Cyber Security Incident. The concern we have received is that it is not always clear where information could have the potential to cause harm, which does not provide a definitive position for organisations to take. The scenario posed to us is where an assessment was made by an organisation that there was no harm in the disclosure of information, however it was found later that there was unintended harm that was not considered. There is no guidance as to how a situation like this would be handled as part of the legislation and there will continue to remain a disincentive to disclose information.

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 proposed review and remedy power would result in a review of the risks related to SOCI compliance inside an organisation and to re-rate those risks based on the increase in regulatory risk to the organisation where it has not previously existed.

Based on feedback we received, there is positive support for this measure - but most responses were keen to understand exactly how the oversight of these powers would work and particularly how the process would be enacted. It is the overall view that organisations that are responsible for Critical Infrastructure should take these obligations seriously.

Measure 9: Consolidating telecommunication security requirements – Telecommunications sector security under the SOCI Act

Regarding Measure 9, we have not engaged any parties that are able to provide commentary regarding the Telecommunications Sector changes. We do, however, support the changes to simplify and build consistency for any sectors as part of the changes to the SOCI Act. The understanding of the changes proposed appear to achieve this.

Response documented by:

AISA Board Director: Michael Burchell

Chair, AISA Board of Directors: Akash Mittal

AISA Member Town Halls

NSW Branch: Facilitated by Amit Chaubey, David Gerber and Reece Corbett-Wilkins

VIC Branch: Facilitated Richard Magalad and David Dowling

QLD Branch: Facilitated Carrie Gurr and Bruce Large

SA Branch: Facilitated by Emily Wingard and Michael Long

ACT Branch: Facilitated by John Karabin

Advisors

Members of the AISA Executive Advisory Board for Cyber

Industry representatives

Documented Prepared by

General Manager, AISA: Megan Spielvogel

Community and Advocacy Manager, AISA: Kathryn Barres

Australian Information Security Association

Australian Information Security Association (AISA)
ABN 181 719 35 959
Level 8, 65 York Street, Sydney NSW 2000
(02) 8076 6012
info@aisa.org.au | www.aisa.org.au