VICTORIA State Government | Government Services

2023-2030 Australian Cyber Security Strategy: Legislative Reforms Consultation Paper

Victorian Government Submission

March 2024

Introduction

Governments across Australia rely on digital technology for the delivery of services that Australians depend on every day. The continuity and reliability of digital services is a priority of the Victorian Government. This includes the protection of government systems against cyber-attacks, as well as supporting businesses and the community to be resilient to the challenges of the digital world.

Victoria welcomes the opportunity to contribute to the development of cyber security legislative reforms that will support Australia to prevent, protect and respond to cyber incidents. Victoria requests the Commonwealth continue to work closely with states and territories as cyber security reforms need to be considered across industry, community and state and territory governments.

Victoria's position: Part 1: New cyber security legislation

Victoria is generally supportive of the legislative options detailed in Part 1 of the consultation paper to address gaps in current regulatory frameworks as detailed in the 2023-2030 Australian Cyber Security Strategy (the Strategy) and associated 2023-2030 Australian Cyber Security Action Plan (the Action Plan).

In developing the legislative reforms, the Commonwealth Government should consider existing reporting obligations and industry standards to mitigate the risk of adding undue administrative burden across government and industry.

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

The Victorian Government supports in-principle mandating a security standard for consumer-grade Internet of Things (IoT) technology to incorporate basic security features by design and help prevent cyber-attacks on Australian consumers.

As most devices are manufactured overseas, responsibility would fall to the manufacturer to ensure the devices are built in line with hardened patterns. This is

particularly relevant to systems that are deployed and not patched or reconfigured in the future which makes them highly susceptible to regular attacks. Regulation and compliance may need to ensure obligations are imposed not only on manufacturers, who are generally overseas, but also importers and retailers.

As a starting point, Victoria supports the adoption of the internationally recognised standards, such as the European Telecommunications Standard Institute (ETSI). Aligning with international standards should lead Australian suppliers and consumers to be more cyber secure (particularly if devices that will fall under the regulatory remit have been manufactured in jurisdictions that have the standards in place). Additionally, setting a reasonable benchmark is important to ensure that the devices meet community and industry needs and therefore do not inhibit the economy.

This measure supports primary prevention of cyber-attacks by way of robust, embedded standards for the design of IoT devices. It is important that any regulated security standard that is put in place consider existing security measures locally and/or internationally to ensure interoperability and avoid inconsistency. Victoria also requests the Commonwealth Government consider the implementation and administrative complexities using lessons learned from the implementation of the SOCI Act to reduce the likelihood of them occurring again.

The implementation of Measure 1 may support better informed purchasing decisions not only for consumers but also for governments. This could also assist in building better cyber security into state and territory governments.

Design and implementation of secure by design standard for consumer-grade IoT devices

As part of developing the legislative reforms, the Commonwealth may wish to consider the full range of IoT devices and assess whether the device is already heavily regulated and the timeframes required for implementation.

The consultation paper outlines that a 12-month transition period may be an appropriate time period after legislation has passed. The operationalisation of the SOCI Act is still being realised three years on, which suggests that a longer transition timeframe may be necessary.

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

The Victorian Government supports in-principle new ransomware reporting obligations where they support the development of a national threat picture, and do not create duplication, excessive administration or make findings of fault or liability.

Positive cyber reporting obligations currently exist within the SOCI Act and it is suggested that these additional ransomware reporting obligations be integrated with pre-existing reporting obligations for critical infrastructure entities (e.g., through Report Cyber and in line with the current reporting timeline requirements). It is not necessary to create a new process.

Rather than civil penalties for non-reporting, the Commonwealth Government could consider other levers to support the reporting of cyber incidents. These levers could include but are not limited to: an education campaign that provides information on

the no-fault reporting protection principles or aligning access to insurance claims with proof of cyber incident reporting being undertaken similar to claiming losses after a theft.

If the Commonwealth Government was to pursue penalties, this should only apply for repeated and continued failures and not in any first instance. This would align more closely to the 'no-fault' and 'no-liability' protection principles, which are about encouraging and removing the barriers to reporting rather than strict penalties for non-compliance.

As information regarding a ransomware attack or cyber extortion demand is vital for Government to enhance the national threat picture, reporting obligations could include, where possible, sufficient technical information to determine method of entry and Techniques, Tactics and Protocols (TTP). The Commonwealth may also wish to consider requesting the disclosure of additional information that ensures the full impact is understood. This may include a copy of the ransom note, and the volume and details of data stolen, if known.

Additionally, through the mandatory reporting function, the Commonwealth Government should provide authority to extend limited use sharing of cyber incidents to central government cyber units in states and territories to enable:

- enquiries to ensure the integrity and security of government networks (network integrations)
- Victoria to lead and manage consequences more generally to cyber incidents
- timely action to reduce the risk of follow up attacks using the same vectors or TTP.

Timeframes and requirements to report

It is important to strike an appropriate balance between maximising the visibility of the ransomware threat and minimising the regulatory burden imposed by a new reporting obligation.

The consultation paper proposes to limit the scope of the ransomware reporting obligation to businesses with an annual turnover of more than $10 million per year. It notes that this threshold, which is consistent with the small business threshold used by the Australian Tax Office, would capture approximately 42,000 businesses or 1.7% of all Australian businesses and would exempt small businesses from this new reporting obligation.

Victoria notes that defining a small business based on annual turnover (as opposed to an defining it as an employer of a limited number of people, e.g., under 15 employees as stated in the *Fair Work Act 2009*) excludes some small to medium enterprises (SMEs). This may increase the likelihood of sophisticated attackers targeting these types of businesses.

It would be valuable to understand what existing data suggests relating to the types of business currently being targeted by ransomware attacks. If data indicated that SMEs are more likely to be targeted, it may be necessary to consider including them (noting the additional administrative burden this may bring and the impact on the availability and affordability of cyber insurance).

Monitoring of the types of businesses impacted by ransomware once the reporting obligations are introduced should continue. If data indicates that some SMEs are

more likely to be targeted, it may be necessary to consider including specific sectors in line with requirements for certain organisations in the Commonwealth's Notifiable Data Breach scheme.

Further clarification is also needed on the size of third-party contractors that would fall into a 'small business category'.

Victoria supports in principle the new ransomware reporting obligation which reflects the capability of the organisation. Ransomware attacks can span an extended period. As such, reporting obligations need to consider response activities to address possible impacts to the industry or wider consumers as well as the ensuring the creation of real-time, nationwide intelligence which can be acted upon to prevent or identify similar or linked incidents.

Sharing ransomware reporting information

Victoria notes that providing industry with trends in ransomware attack and associate threat vectors will aid industry in countering attacks where possible. Further, continual engagement with industry will help reinforce the importance of security and reiterate the deployment of controls in this space.

Consideration should be given to providing anonymised information about ransomware incidents to law enforcement agencies as valuable intelligence that may aid in operational activities.

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

The Victorian Government supports in-principle a legislated, limited use obligation for Australian Signals Directorate (ASD) and the National Cyber Security Coordinator to encourage industry engagement with the Commonwealth Government following a cyber incident.

Timely incident reporting is vital for ASD and the National Cyber Security Coordinator to perform their functions and help manage the consequences of a cyber-attack. It is equally important for the Commonwealth Government to share timely cyber incident details with state and territory governments to better enable them to acquit their responsibilities to the public, help address state-specific consequences and acquit any specific regulatory requirements.

The proposed model of a 'limited use' obligation would restrict the use of cyber incident information, but not the sharing of this information. This should be expanded to include the efficient sharing of incident information with relevant state and territory government/s.

Incentives to engage with Government after a cyber incident

It is likely that the limited use obligations (which aim to specify that information shared with ASD or the National Cyber Security Coordinator cannot be used for compliance action against entities) will incentivise engagement with government.

There is also opportunity to incentivise organisations by creating more streamlined reporting. Currently, impacted entities are being requested to report multiple times,

once to the Commonwealth Government and again to each relevant state and territory government.

It is likely that impacted entities are more likely to engage with all relevant governments, have better visibility of what is reported, and benefit from a reduction of administrative burden if the impacted entity is empowered to submit one report which is then reliably shared in a timely manner with the Commonwealth and relevant state/territory governments. In this instance, Victoria and other states and territories would be able to disestablish their separate and duplicating reporting requirements for impacted entities.

Measure 4: Learning lessons after cyber incidents – A Cyber Incident Review Board

The Victorian Government supports in-principle the establishment of a CIRB. In Victoria's view the CIRB should include representation from each state and territory government. This should be an appropriate cyber leader, such as the State Government or Territory Chief Information Security Officer'. Victoria cannot support this measure in full until membership is confirmed.

At present, the national picture of cyber incidents and the emerging threat landscape is fragmented. It is important that when a major incident occurs, government understands the root cause and tactics, techniques and procedures that led to the attack and pass on lessons learned, including the impacts arising from the incident to industry, government and community to improve Australia's cyber resilience.

The establishment of a national body to review cyber incidents will support a shared understanding on emerging issues and risks and provide recommendations to strengthen Australia's collective processes and procedure to enhance cyber resilience.

Victoria supports the no-fault principle detailed within the consultation paper which will assist in the promotion of positive reporting. Victoria also supports in principle that the board could have the power to compel information to support its respective reviews.

The consequence of a cyber incident would be an important factor to consider when deciding whether to initiate a CIRB review. A classification standard for cyber incidents that can be used across Australia should be developed to inform what types of incidents should be considered by the CIRB.

Similar to the Australian Transport Safety Bureau (ATSB), the CIRB should prioritise reviews that have the potential to deliver the greatest public benefit. Additionally, similar to the ATSB investigations, the CIRB should not apportion blame but rather focus on factors that led to the incident so that lessons can be learned, and cyber security improved in the future.

Due to the connection between cyber incidents and emergency management, Victoria suggests alignment in methodology for learning from these events. The emergency management sector across Australian jurisdictions, including the National Emergency Management Agency (NEMA), follow the methodology for learning and continuous improvement as laid out in the Australian Institute for Disaster Resilience Lessons Management Handbook.

Establishment of the CIRB

In regard to membership of the CIRB, Victoria considers that the Australian Cyber Security Centre (ACSC) chair the CIRB and that the Chief Information Security Officer from each state and territory is appointed as a member. In some circumstances it might be beneficial to enable flexibility in the membership of the CIRB dependent on the incident. Additionally, information relating to potential industry participation in the establishment of the CIRB would be valuable.

Victoria seeks further clarification on implementation, including on how the CIRB would be intended to interact with Victorian Government entities. Clarification is also sought on the roles and responsibilities associated with review participation and publication to avoid duplicative processes, avoidable costs and to enable Victorian governance processes to be active and enabled during reviews. This information could be provided through the dissemination of a draft Terms of Reference for the CIRB to all Australian jurisdictions.

Victoria's Position: Part 2: Amendments to the *Security of Critical Infrastructure Act 2018*

The SOCI Act seeks to uplift the security and resilience of Australia's critical infrastructure by introducing positive security obligations for critical infrastructure and government assistance measures. However, the regulatory environment and administrative requirements under the SOCI Act can be complex for industry and government agencies to navigate. Several high profile and high impact cyber attacks have highlighted the need to address gaps within the SOCI Act to better support organisations to prevent, prepare and responds to cyber incidents.

The Victorian Government supports in principle amendments to the SOCI Act and welcomes the intention to ease the administrative burden on organisations and clarify identified complexities and gaps. Victoria requests close cooperation with states and territories when developing amendments to the SOCI Act and encourages the Commonwealth to continue exploring additional SOCI Act reforms to simplify complexities and further reduce administrative burden.

A continued focus on information sharing and collaboration will be key to addressing the concerns outlined above, especially as the Commonwealth Government moves closer to delivering their recommendations.

Further, Victoria encourages the Commonwealth to consider how Australian cyber security businesses can be leveraged and prioritised as the SOCI Act reforms progress. Using Australian-based capacity and capability to establish appropriate safeguards for critical infrastructure and incident response will present a significant opportunity for the local cybersecurity industry to develop.

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

The Victorian Government supports in-principle making amendments to the SOCI Act to protect critical infrastructure data storage systems that hold business critical data.

Amendment to the definition of 'Asset' and 'Material risk' in the SOCI Act

Victoria supports expanding the definition of asset and material risk. Clarification is needed on the physical/cloud-based boundaries, and how the intersection of each asset would be defined. The interaction with other SOCI provisions (such as trusted insiders and supply chains) in relation to newly covered assets would require consultation ahead of implementation. As this is an additional reporting obligation on responsible entities, consultation on the new definitions should include the anticipated benefits to the Critical Infrastructure Risk Management Plans (CIRMP) reporting system.

Administrative

The proposed amendments have the potential to increase the regulatory burden on critical infrastructure (e.g. hospitals). Increased regulatory burden will likely have financial and non-financial flow on impacts which may result in the need for increased resources. Victoria proposes that the Commonwealth works closely with state and territory governments to reduce potential regulatory and financial impact across sectors. Further, the Commonwealth should explore options to support these sectors to acquit new requirements including through financial incentives such as grants.

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

Victoria supports in-principle establishing last resort powers for consequence management as long as the appropriate safeguards and oversight mechanisms are in place and the powers complement existing arrangements. This includes ensuring engagement with the relevant state government and departments prior to initiating engagement with an entity. Further, to ensure the proposed powers achieve their intention, Victoria recommends that the scope of consequence management is clearly defined.

The Commonwealth Government should recognise existing legislative responsibilities. For example, the Victorian Emergency Management Commissioner (EMC) has consequence management legislative responsibilities under s.45 of the *Emergency Management Act 2013* (Vic). Any new directions powers would need to ensure there is no direct conflict with the EMC's powers.

It is also recommended that the Commonwealth consider the proposed consequence management powers alongside the *National Emergency Declaration Act 2020* and how it may be used to support emergency prevention, response and recovery.

Victoria notes that one of the direction powers details that an organisation may be directed 'to replace documents of individuals or businesses impacted by the incident.' Victoria seeks further clarification on whether the organisation would be refunded the costs associated with the replacement.

Interaction with other policy frameworks

Victoria's critical infrastructure resilience arrangements include both legislation and policy that together provide a framework for collaboration, information sharing, and building sector or organisational resilience across all hazards. The proposed

consequence management power would need to consider its interaction with the existing framework and undertake clear stakeholder engagement.

Additionally, the Australian Government Crisis Management Framework (AGCMF) outlines the national approach to preparing for, responding to and recovering from crises. The AGCMF agrees that state and territories lead consequence management for their respective jurisdiction.

Victoria notes that work is underway to provide the Department of Home Affairs a summary of relevant sections within Victorian legislation to inform implementation of Measure 6.

Principles, safeguards and oversight mechanisms

The Commonwealth Government should consider whether the last resort powers could be tailored to particular emergencies rather than being too general. This will ensure that the powers are exercised only when necessary.

The Commonwealth Government should consider mechanisms to ensure that improper release of information does not occur, and that the use of the information obtained as a result of the 'last resort powers' is appropriately constrained. While the proposal notes the use of any powers will be subject to Privacy Act requirements, the extension of powers to the sharing of information to third parties will need to be carefully drafted with clear definitions.

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

The Victorian Government supports the approach to simplify how government and industry shares information through the revision of the 'protected information' definition. Simplifying the protected information definition will support a clearer decision making and information sharing processes.

Victoria also agrees with the intention to provide greater clarity on the 'harms-based approach'. More defined boundaries will support government and industry in navigating their requirements when considering protecting and sharing information of major incidents. It is recommended that the revised definitions explicitly outline that the harms-based approach to information disclosure considers states and territories.

Victoria agrees with the Commonwealth position that protected information provisions in the SOCI Act should not limit or impede the sharing of information with government (at any level) or with regulators.

Victoria supports that the disclosure of protected information should be granted to all Commonwealth, state and territory government entities, including emergency management agencies, as this will support the performance of relevant, duties, functions or the exercise of powers.

Victoria suggests that federated data sharing models, through mutually beneficial data sharing agreements, could support better and more consistent access to common information.

Automation considerations

The automation of information flows and establishment of a common operating picture and risk management plans, led by the Commonwealth Government and shared with jurisdictions at all levels of government has potential to enable better preparation for and coordination when significant incidents and emergency events occur.

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

Victoria supports in-principle the proposal to introduce a formal, written directions power in Part 2A of the SOCI Act. It is noted that the directions power will be limited to deficiencies in the CIRMP that carries a material risk to the socioeconomic stability, defence, or national security of Australia or where there is a severe and credible threat to national security.

Victoria suggests that the Commonwealth Government should include a consideration of direct engagement with jurisdictions where risk management obligations already exist. This should include Part 7A of Victoria's *Emergency Management Act 2013* which provides the relevant portfolio Minister with the capacity to request additional information on a responsible entity's risk management plan.

Further clarity will be required on the cross-over with existing directions powers (for example, the Victorian water sector) that are available under current state legislation. The issue of overlapping directions power may be managed by consultation with the State when written notice is issued under the SOCI Act.

Victoria suggests that states and territories should have a mechanism that allows them to raise issues directly with the Cyber and Infrastructure Security Centre (CISC). This will encourage stronger lines of communication and greater transparency.

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

The Victorian Government supports the proposal to consolidate telecommunication security requirements of the Telecommunications sector under the SOCI Act.

The SOCI Act is the primary Australian Government framework for regulation and protection of Australia's critical infrastructure. The stronger consideration of telecommunications as critical infrastructure under the SOCI Act is important in the context of ever-increasing interconnectedness of critical infrastructure and interdependencies on telecommunications.

Telecommunications assets are an integral and interconnected component of the broader critical infrastructure ecosystem, and it is important to ensure that there is a consistent regulatory framework for these critical assets. The proposed reforms are intended to provide more consistent treatment of telecommunications as critical infrastructure. This should improve the transparency and risk management arrangements for the sector which should support greater continuity of telecommunications services, particularly when significant incidents occur.

Victoria agrees that reforms to the SOCI Act need to enable an agile, industry-led response to incidents with appropriate support from government when necessary.

It is also recommended that the co-design process includes the water sector as the water sector continues to operate internal telecommunications in specific operating environments.

Conclusion

Victoria welcomes the opportunity to contribute to the development of new cyber security legislative reforms and amendments to the SOCI Act. It is important that a new cyber legislation considers lessons learnt from the development and implementation of the SOCI Act.

Any new regulation and reporting requirements should complement existing arrangements and promote safe and ethical information sharing practices where practicable. No-fault and no liability principles are a positive mechanism to enhance voluntary reporting in an increasingly evolving threat landscape.

Victoria is broadly supportive of the proposed amendments to the SOCI Act and their intention to clarify current complexities, ease the administrative burden on organisations and address gaps that have been identified following recent major cyber security incidents. However, engagement with states and territories will be essential in ensuring the proposed amendments align with existing legislation and obligations.

Victoria strongly urges the Commonwealth Government to continue to work closely with industry and states and territories on all the proposed measures as cyber security reforms must be considered across both industry and state and territory governments to ensure fit for purpose and meaningful changes are created.