ACT Government

Cyber Security Legislative Reforms – Consultation Paper

Australian Capital Territory Government Submission

February 2024

Contents

Summary 3

ACT Government Response to the Consultation Paper 4

Measure 1: Helping prevent cyber incidents – Secure-by-design standards for Internet of Things devices 4

Measure 2: Further understanding cyber incidents – Ransomware reporting for businesses 5

Measure 3: Encouraging engagement during cyber incidents – Limited use obligation on the Australian Signals Directorate and the National Cyber Security Coordinator 6

Measure 4: Learning lessons after cyber incidents – A Cyber Incident Review Board (CIRB) 6

Measure 5: Protecting critical infrastructure – Data storage systems and business critical data 6

Measure 6: Improving our national response to the consequences of significant incidents – Consequence management powers 7

Measure 7: Simplifying how government and industry shares information in crisis situations – Protected information provisions 8

Measure 8: Enforcing critical infrastructure risk management obligations – Review and remedy powers 9

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

Summary of consultation paper questions 10

Part 1 - New cyber security legislation 10

Part 2 – Amendments to the SOCI Act 14

Summary

The ACT Government welcomes the opportunity to provide this response to the *Australian Cyber Security Strategy: Cyber Security Legislative Reforms Consultation Paper* (the Consultation Paper).

The ACT Government (ACT) is in-principle supportive of the Australian Government's ambition to make Australia the world's most cyber secure nation by 2030. Cyber security is critical to realising the benefits of data and digital technologies that will continue to be an enabler for more effective, efficient, accessible and equitable service delivery. Within governments and across the business sector our data is a vital strategic asset. Similarly, our citizen identities are a precious possession that carries vital national significance.

Reforms of this scale require a balanced and sustainable whole-of-system approach that considers and assesses the regulatory and economic burden of ongoing legislative reforms that continue to be implemented, such as under the *Security of Critical Infrastructure Act 2018* (Cth), as well as the proposed new cyber security legislation. While the ACT is supportive of the intent of the proposed regulatory reforms, further consultation and development would ensure that new regulations are sustainable and capable of achieving stated objectives across industry and business sectors and that the cost of implementation will not be passed-on to consumers.

Protecting our most vulnerable citizens from the harms caused by cyber-attacks requires governments, businesses and industry to ensure that personal information and data is only retained under reasonable grounds. Too often in recent significant cyber incidents, personal information of citizens has been exposed as being retained long after it was necessary for service delivery and customer relations. This issue cannot be solved through enhanced cyber security but through a holistic lens of cyber, privacy, data and identity measures to manage information risks and enhance protections and mechanisms for enforcement when personal information is retained after it is no longer required. To create whole of economy change, we recommend that the Australian Government take a holistic approach that considers the foundations of how personal information is collected and stored, and how businesses and industry can be supported to build and use systems that enable data deletion as a control against the risk of a data breach and resulting harms to our communities. This in turn will ensure that the strong cyber defences delivered through the *2023-2030 Australian Cyber Security Strategy* are right-sized to protect the critical information, data and systems needed in our vibrant and growing economy.

By adopting the recommendations in this submission, the Commonwealth will be taking a national approach to implementing the *2023-2030 Australian Cyber Security Strategy* that recognises that making Australia the most cyber safe nation cannot be achieved without the support and influence of State/Territory governments who have a critical role in protecting government services, supporting industry and business sectors and protecting the community from the harm caused by cyber attacks.

ACT Government Response to the Consultation Paper

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

The ACT recognises the importance of security for Internet of Things (IoT) devices and the benefits of a national approach to protect consumers. We agree that legislating minimum standards for consumer grade devices supports national consistency and more secure devices in the market, however the impacts of this regulatory reform should be considered appropriately through further consultation once a model has been determined. This reform should be applied to parties that contribute to the development and manufacture of devices, as well as suppliers. For governments, infrastructure and business to adapt to these changes and address the significant scope of legacy devices, new legislation should not have retrospective application without significant additional consultation and an impact assessment to allow for new devices that meet the regulatory standards to enter the market or be developed. The ACT uses significant numbers of IoT devices to provide services to the community, such as smart light poles, electronic vehicle chargers and smart meters. The ACT also utilises a wide range of medical IoT devices subject to existing regulations and controls such as certification by the Therapeutic Goods Administration. Retrospective application of new legislation and mandatory standards would have a significant impact on the ACT in both the re-assessment and replacement of devices across the community. Further, non-retrospective application of new legislation would minimise any potential financial impact on consumers for the cost of replacement devices that may be passed on by the business sector. A three-year window to meet the new legislation for new devices would be an appropriate minimum timeframe to adjust to these reforms.

The consultation paper also seeks feedback on adopting the first three standards of the international ETSI EN 303 645 standard as mandatory for consumer grade devices in Australia under new cyber legislation, which provides an equivalent framework to international regulations. As an appropriate minimum baseline under the ETSI EN 303 645 standard to safeguard consumers, the ACT also supports incorporation of the following additional three standards:

- Standard 5: Communicate securely
- Standard 8: Ensure that personal data is secure
- Standard 11: Make it easy for users to delete user data.

Inclusion of these additional standards would align with the direction of reforms to the *Privacy Act 1988* (Cth) and provide enhancements to data security. It would also minimise potential loopholes that may be exploited by manufacturers under new legislation to the detriment of consumers, and reduce the likelihood of reactive regulations being introduced in coming years that compound the impact on governments, industry and business sectors.

The ACT supports consideration of similar provisions to United Kingdom (UK) legislation to exclude the following types of devices under new legislation on the basis that work is separately underway to develop tailored security requirements that will apply to these devices:

- Electric vehicles and charge points

- Smart meters
- Medical devices
- Computers.

Tailored security requirements for medical devices outside of these reforms should consider leveraging controls stipulated by the Therapeutic Goods Administration.

Once developed, a model for mandatory minimum standards under new legislation should be actively consulted with State/Territory governments, industry and business to ensure the impacts of the regulatory reform are fully costed and understood. This will be critical to sustainable economic growth, future business innovation by small-to-medium sized enterprises (SMEs) and minimising the cost to consumers.

Recommendations: That a new legislation providing mandatory minimum standards for IoT devices:

- apply to new devices entering the market and not have retrospective application
- apply to parties that contribute to the development and manufacture of devices, as well as suppliers
- have a minimum three-year grace window prior to being enforceable
- consider inclusion of an additional three ETSI EN 303 645 standards- 5, 8 and 11
- consider mirroring exclusions under UK legislation for devices that will be subject to separate regulations or standards to minimise duplicative reforms
- undergo additional consultation with State/Territory governments, industry and business sectors once a regulatory model has been determined to fully assess the cost of implementation.

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

The ACT acknowledges the limited national visibility on the prevalence of ransomware and cyber extortion and the value in understanding the collective threat picture to deliver effective and timely support services to the private sector and victims. The ACT does not condone the payment of a ransom to cybercriminals. Payment does not offer a guarantee that data encrypted in ransomware will be decrypted by the attacker and is likely to attract further attacks from cybercriminals seeing a soft target.

SMEs may struggle to meet the burden of ongoing regulatory reforms and reporting obligations under this reform. A range of existing regulatory obligations on businesses have been designed to effectively manage risks and ensure accountability, including cyber security risks, such as under the *Corporations Act 2001* (Cth) (*Australian Securities and Investments Commission v RI Advice Group Pty Ltd [2022] FCA 496*). While the proposal to limit the obligation to businesses with a revenue of $10 million or more per annum will impact on approximately 1.7 per cent of Australian businesses, consideration could also be given to alignment with linked forthcoming regulatory reforms, such as the review of the *Privacy Act 1988* (Cth). Aligning ransomware reporting obligations with businesses that may face enhanced privacy requirements, such as for Notifiable Data Breaches or high privacy risk activities, under a new Privacy Act would mean that the most sensitive information also carries response obligations to report ransomware and cyber extortion to the Australian Cyber Security Centre. This would remove the regulatory burden from businesses within the proposed threshold that do not store significant or sensitive data on clients and community members. While these businesses may continue to face the revenue and business impacts of ransomware and cyber extortion, the total regulatory burden would be streamlined and aligned to a greater extent across the current scope of Commonwealth regulatory reforms on privacy, data and identity security. This will support

the business sector to uplift protections and improve national visibility on the impacts and harms of this criminal activity.

Recommendation: That the Commonwealth consider aligning ransomware reporting obligations with concurrent and forthcoming regulatory reforms that will also have a significant impact on the business sector, including a new Privacy Act, to ensure that a national picture reflects ransomware activity that has the greatest potential for harm to the community.

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

The ACT supports engagement with the Australian Cyber Security Centre and National Cyber Security Coordinator during cyber incidents and works closely with national and inter-jurisdictional agencies on these matters.

Recommendations: Nil.

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

The ACT supports the establishment of a CIRB to facilitate lessons learned from major cyber incidents to assist governments, industry and business to implement mitigations and controls to avoid repeats of similar incidents in future. Giving the CIRB a risk-based focus will allow its findings to provide the greatest national benefit. Reporting by the CIRB should prioritise incidents where the release of risk-based findings and recommendations would assist impacted members of the community and future impacts to Australian entities.

The CIRB could also provide an aggregate view of cyber incidents across Australia that could help inform and focus risk mitigation strategies and the effective prioritisation of programs to address collective vulnerabilities and enhance public awareness and understanding of the impacts and occurrences of cyber incidents.

Recommendations: That the functions of the CIRB prioritise incidents that:

- would provide the greatest value and benefit to industry and business sectors in preventing significant disruption or economic loss
- result in a loss of control or access to sensitive and personal information and data relating to the community
- for the health sector, cause a significant disruption to the delivery of healthcare, which may include direct or indirect patient harm, or placing undue strain on other healthcare facilities.

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

The ACT understands the drivers behind this proposed regulatory extension for critical infrastructure assets under the *Security of Critical Infrastructure Act 2018* (Cth; SOCI Act) however increasing the burden on regulatory reforms that are yet to be fully implemented and evaluated may have negative consequences and impacts on governments, industry and business sectors. Achieving an appropriate balance between addressing issues and concerns identified through recent significant cyber incidents and further holistic

regulatory reform requires an assessment of any additional financial impacts and be subject to a further period of implementation to be sustainable.

The regulatory burden of recent reforms to the SOCI Act has yet to be assessed and evaluated to determine the successes and impediments to industry uplift and the consequential positive impacts to Australia from these critical infrastructure reforms. The ACT recommends that additional regulatory reform not occur until such an evaluation has taken place in consultation with State/Territory governments and critical infrastructure sectors.

While the proposed reforms seek to prescribe business critical data and data storage as part of a critical infrastructure asset within the meaning of 'relevant impact' under the SOCI Act and associated Critical Infrastructure Risk Management Program (CIRMP) obligations, there may be unintended challenges for government critical infrastructure in which the management and control of relevant data occurs across multiple business units. The proposed reforms may have potentially significant cost to government through extension of CIRMP requirements to business units operating separately to a government critical infrastructure asset, and decrease efficiencies and processes governing the use of this data through inclusion within the scope of a critical infrastructure asset, or multiple assets for the same dataset. As currently set out, this reform may be prohibitive for the ACT to implement without extension of current CIRMP regulatory timeframes.

The ACT agrees with the importance of ensuring that data sets are protected in a manner that reflects their importance to a critical infrastructure asset and the impact to citizens of misuse, theft, or compromise of personal data. The proposed reforms, while seeking enhancements on some of those data sets and systems, may provide inconsistent protections that leave open the potential for other comparable data not linked to a critical infrastructure asset to be compromised in a similar manner. As such, further regulation should be considered in the context of other initiatives under the *2023-2030 Australian Cyber Security Strategy* such as Systems of Government Significance and new Cyber Security Legislation which may provide additional mechanisms to achieve the objectives of the proposed reform.

Recommendations:

- Extension of regulation under the SOCI Act to data storage systems and business critical data should be informed by a review of the regulations that are still being implemented under this Act.
- A Regulatory Impact Assessment should be developed in close consultation with State/Territory governments, industry and business sectors.
- Consideration be given to the potential for inconsistent application on data sets and systems of national importance that could result in significant community, government or business disruption if compromised.
- An extended grace period should apply if these reforms are progressed.

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

The ACT supports a national approach to responding and recovering from our most significant critical infrastructure incidents led by the National Coordination Mechanism (NCM) and consultation with State/Territory governments directly or through that forum.

Recognising that the proposed consequence management powers are 'last resort' powers, care should be taken to ensure that this measure does not place undue further burden on an entity that is in a crisis response, and that secondary consequence handling does not interfere with addressing the primary

incident. This should occur through close consultation with all stakeholders throughout the exercise of these powers. The example of mandating that an entity takes certain actions, such as funding the replacement of identity documents, gives rise to potentially significant burdens on State/Territory governments who would have to fulfill this request, even if payments were to be borne by another entity. There are similarly supply chain and other considerations that may require phased roll-out or implementation, which reinforces the importance of consultation and dialogue in decision-making throughout these events. The NCM has previously proven to be a successful mechanism for these conversations provided that supplied points of contact are utilised.

The operation of consequence management powers has the potential to conflict with the exercise of ACT powers under the *Emergencies Act 2004* (ACT) and *ACT Emergency Plan* for concurrent significant incidents or emergencies to the Territory. Consideration should be given to how consultation with State/Territory governments to inform decision-making under these powers can minimise duplication in the exercise of regulatory powers or decision-making.

It will also be important for the Commonwealth to ensure there is good public awareness of consequence management powers and how and when they will be exercised to avoid confusion and pressure to announce consequence management measures while the response to the initial incident is still underway.

Recommendations: That the consequence management powers:

- be exercised in close consultation with State/Territory governments and decision-making informed by the outcomes of that consultation
- be accompanied by accessible public advice on how and when these powers will be enlivened.

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

The ACT supports simplifying the protected information provisions in the SOCI Act to ensure information can be shared within governments as required for government operations, risk monitoring and management, and incident and emergency responses.

The current protected information use and disclosure provisions restrict the ability for officers in non-regulatory but relevant roles in government departments, such as those responsible for community safety and emergency management, to support the ACT in managing risks, planning for or responding to an incident impacting a critical infrastructure asset. Similarly, the current provisions may limit the ability for the ACT to share protected information with ACT Policing where there is a need to know, unless under certain conditions. This may impede risk management activities for critical infrastructure assets within the Territory. Removal of these restrictions would provide consistency with established arrangements with industry for the establishment of plans and management of risks within the ACT.

Protected information provisions for State/Territory Ministers should also be extended to all Ministers regardless of portfolio responsibility.

The proposed harms-based approach supports sufficient information sharing to address the current impacts and inefficiencies caused by the current protected information sharing provisions. However, amendments to these provisions should also ensure information can be shared with State/Territory police agencies where there is a need to know.

Recommendations: That protected information provisions under the SOCI Act:

- remove current limits on disclosure and sharing of information to and between State/Territory departments
- remove current category limits on disclosure and sharing of information to and between State/Territory Ministers
- ensure protected information sharing provisions do not restrict State/Territory departments from sharing information with State/Territory police agencies where there is a need to know.

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

The proposed powers would not impact on preventing and managing risks within the ACT.

Recommendations: Nil.

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

Consolidating security requirements for the telecommunications sector under the SOCI Act will not have a consequential impact on ACT legislation and regulation of these assets.

Recommendations: Nil.

Summary of consultation paper questions

Part 1 - New cyber security legislation

#	Question	Our Response
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?	Page 4
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?	Page 4
3	What alternative standard, if any, should the Government consider?	No response.
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?	Page 4
5	What types of smart devices should not be covered by a mandatory cyber security standard?	Page 4
6	What is an appropriate timeframe for industry to adjust to new cyber security requirements for smart devices?	Page 4

#	Question	Our Response
7	Does the Regulatory Powers Act provide a suitable framework for monitoring compliance and enforcement of a mandatory cyber security standard for IoT devices?	No response.
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?	No response.
9	What additional mandatory information should be reported if a payment is made?	No response.
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?	Page 5
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?	Page 5-6
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?	Page 5

#	Question	Our Response
13	To what extent would the no-fault and no-liability principles provide more confidence for entities reporting a ransomware or cyber extortion incident?	No response
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?	No response
15	What is an appropriate enforcement mechanism for a ransomware reporting obligation?	No response
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?	No response
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?	No response
18	What restrictions, if any, should apply to the use or sharing of cyber incident information provided to ASD or the Cyber Coordinator?	Page 6

#	Question	Our Response
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?	No response.
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)?	Page 6
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?	No response.
22	How should a CIRB ensure that it adopts a 'no-fault' approach when reviewing cyber incidents?	No response.
23	What factors would make a cyber incident worth reviewing by a CIRB?	Page 6
24	Who should be a member of a CIRB? How should these members be appointed?	No response.
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?	No response.
26	How should the Government manage issues of personnel security and conflicts of interest?	No response.

#	Question	Our Response
27	Who should chair a CIRB?	No response.
28	Who should be responsible for initiating reviews to be undertaken by a CIRB?	Page 6
29	What powers should a CIRB be given to effectively perform its functions?	No response.
30	To what extent should the CIRB be covered by a 'limited use obligation', similar to that proposed for ASD and the Cyber Coordinator?	No response.
31	What enforcement mechanism(s) should apply for failure to comply with the information gathering powers of the CIRB?	No response.
32	What design features are required to ensure that a CIRB remains impartial and maintains credibility when conducting reviews of cyber incidents?	No response.
33	What design features are required to ensure a CIRB can maintain the integrity of and protection over sensitive information?	No response.

Part 2 – Amendments to the SOCI Act

#	Question	Our Response
Measure 5: Protecting critical infrastructure – Data storage systems and business critical data		

#	Question	Our Response
34	How are you currently managing risks to your corporate networks and systems holding business critical data?	Page 6
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?	Page 6
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?	Page 6
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?	Page 7
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?	Page 7
39	What principles, safeguards and oversight mechanisms should Government establish to manage the use of a consequence management power?	Page 7
Measure 7: Simplifying how government and industry shares information in crisis situations – Protected information provisions		

#	Question	Our Response
40	How can the current information sharing regime under the SOCI Act be improved?	Page 8
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?	Page 8
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?	Page 9
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 response.
44	How do other state, territory or Commonwealth requirements interact with the development of an RMP?	Page 9
45	How can outlining material risks help you adopt a more uniform approach to the notification obligation?	No response.
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 response.

#	Question	Our Response
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 response.