COMMUNICATIONS ALLIANCE LTD

Communications Alliance Submission

to the Department of Home Affairs

2023–2030Australian Cyber Security Strategy: Legislative Reforms

Consultation Paper

1 March 2024

Contents

Communications Alliance

Communications Alliance is the primary communications industry body in Australia. Its membership is drawn from a wide cross-section of the communications industry, including carriers, carriage and internet service providers, content providers, platform providers, equipment vendors, IT companies, consultants and business groups.

Its vision is to be the most influential association in Australian communications, co-operatively initiating programs that promote sustainable industry development, innovation and growth, while generating positive outcomes for customers and society.

The prime mission of Communications Alliance is to create a co-operative stakeholder environment that allows the industry to take the lead on initiatives which grow the Australian communications industry, enhance the connectivity of all Australians and foster the highest standards of business behaviour.

For more details about Communications Alliance, see https://www.commsalliance.com.au .

Introduction

Communications Alliance welcomes the opportunity to make a submission to the Department of Home Affairs (Department) in response to the *2023-2030 Cyber Security Strategy: Legislative Package Consultation Paper*.

Communications Alliance and its members recognise the significance of focusing on and enhancing Australia's cyber security – a reality emphasised by recent and ongoing national cyber incidents. The rapid development in technology and its increased integration into our daily lives has exacerbated the need of effective cyber security measures. Our members take cyber security very seriously and are in close contact with all relevant stakeholders, to continuously enhance cyber defences, and they will continue to engage with cyber security initiatives that seek to counter existing and emerging risks. Industry has also taken proactive steps to develop and apply industry-wide cyber security standards and best practices.

We agree with the statement that a significant effective uplift of cyber security will require "*an integrated whole-of-nation endeavour*"[1] that necessitates the involvement of and close cooperation between Government, the business community (including small businesses) and individuals. Especially with respect to small businesses and the general Australian public, substantial funds for awareness, education and practical assistance measures will be required.

We also appreciate and agree with the stated intent not to increase regulatory burden for industry in what is already a complex regulatory environment.

We commend the Department of Home Affairs and other stakeholders for the collaborative approach that has been taken in the development of the strategy and the measures proposed for implementation of the strategy. We believe co-design of regulation – to the extent additional regulation is necessary – through leveraging combined industry and Government/agency expertise will offer the most effective pathway to the long-term goal of becoming a highly cyber secure nation.

Communications Alliance is also conscious of the broader reform agenda of the Australian Government which intersects with the ongoing sharpening around and reform efforts of regulation and legislation in the area of cyber security. In particular, we note the

- Government's commitment to co-design with industry a voluntary AI code;
- ongoing Privacy Act review;
- creation/roll-out of an Australia-wide Digital Identity Framework;
- intensive (co-)regulatory activity in relation to online safety; and
- industry and Government measures targeting the reduction of harms from scams.

[1] p.7, Australian Government Expert Advisory Board, 2023-2030 Australian Cyber Security Strategy Discussion Paper, Feb 2023, https://www.homeaffairs.gov.au/reports-and-pubs/files/2023-2030_australian_cyber_security_strategy_discussion_paper.pdf accessed on 23 Feb 2024

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

Existing approaches and standards

1.1. The Consultation Paper proposes the establishment of a mandatory cyber security standard for consumer-grade smart devices. It also highlights Government's commitment to the introduction of a voluntary labelling scheme (noting that such a scheme is out of scope for the purpose of the Consultation Paper).

1.2. In line with the feedback received to align with international approaches and standards, the Paper considers the adoption of the first three principles of *ETSI EN 303 645 CYBER; Cyber security for consumer Internet of Things: Baseline requirements*. Adoption of these principles would align with the approach taken by the UK through the *Product Safety and Telecommunications Infrastructure Act 2022* (PSTI Act) and by a number of other nations, including the nations of the European Union, Canada and China.

5.1. Importantly, the PSTI Act (though it's subordinate regulation) does not adopt the first three principles of *ETSI EN 303 645* in full but only specific parts thereof. We recommend following the same approach for consumer-grade devices. The three requirements adopted in the UK are:

1) banning universal default passwords (but excluding items 5.1-3 to 5.1-5 of ETSI EN 303 645)

2) implementing a means to manage reports of vulnerabilities (but excluding items 5.2-2 and 5.2-3 of ETSI EN 303 645)

3) providing transparency on for how long, at a minimum, the product will receive security updates (but excluding items 5.3-1 and 5.3-2 of ETSI EN 303 645)

1.3. However, we believe that the approach to the types of devices in scope for regulation ought to be reconsidered.

1.4. We highlight that, in November 2023, Standards Australia identically adopted *ETSI EN 303 645* (in its current version V2.1.1 (2020-06)) as *AS ETSI EN 303 645:2023 CYBER; Cyber security for consumer Internet of Things: Baseline requirements*. Therefore, an Australian Standard for cyber security of consumer grade IoT devices, which is identical to the key international standard, already exists in Australia. This standard ought to form the basis of any regulation or legislation.

Devices in scope

1.5. The UK PSTI Act takes an exception-based approach to devices, i.e. generally any "*internet-connectable product*" and "*network connectable product*" is in scope unless specifically exempted. [2]

1.6. Devices in scope of the PSTI Act include smart phones and tablets, alongside 'traditional' consumer-grade smart devices.

1.7. We believe the UK approach to scope ought not be applied in Australia for the following reasons:

[2] section 4, UK *Product Safety and Telecommunications Infrastructure Act 2022*, https://www.legislation.gov.uk/ukpga/2022/46/section/4/enacted, accessed on 23 Feb 2024.

1.8. Smart phones and tablets are already well regulated through existing mandatory standards and legislation in a global context.[3] Additional regulation appears unnecessary and has the potential to create inconsistencies and confusion. These devices ought not be in scope of the proposed new regulation.

1.9. We also understand that that the adoption of the first three principles does not appear to address a problem known to exist in a smart phone/tablet context.

1.10. The UK approach of a default inclusion of internet or network-connectable products with subsequent exception appears unnecessarily complex and may act to stymie innovation in IoT devices that are not intended to be the target of the regulation but are caught by default, leaving innovators and manufacturers/providers with the uncertainty as to whether such devices will need to comply or may be, in the future, exempted.

1.11. It is in our view unnecessary to include any industrial IoT devices or sensors, such as sensors in agriculture, seismic, climate or environmentally related sensors etc., and network components into the scope of the proposed standard.

1.12. Any imposition of mandatory requirements should only apply to devices that can place a user, system, network or data at risk and where the device is not already subject to cyber security regulation to the same effect. If the nature of the device and its function precludes any risk to any of the above, the mandatory obligation should not apply.

1.13. Consequently, any regulation should only be proposed to apply to devices

- with direct connectivity to the internet (i.e. not those that join via Bluetooth or LoraWan through access management software);
- with sufficient processing power to enable them to host a botnet attack and/or sufficient functionality to place the user at physical or financial risk;
- where those devices are not already covered by other security related mandatory requirements to the same effect; and
- that are truly consumer-grade devices, i.e. have the capacity to place a consumer at risk or cause harm to a consumer (but noting our feedback above to exclude smart phones/tablets).

The second point is of particular importance as widening the scope to 'dumb' smart devices (i.e. for the purposes of the debate, devices that generally do not provide many avenues to place the user at risk but may offer the capability, when hacked, to pose risks to networks) would complicate and delay the implementation of any standard and unnecessarily focus attention away from the desired objective, i.e. the protection of consumers from harm.

1.14. With the vast majority of internet or network-connected devices falling into a non-consumer-grade category, it is, in our view, inefficient to take an exemption-based approach to mandatory requirements for consumer-grade IoT devices. The definition of a clear list of devices in scope – which can be added to as the need arises – appears to provide a more useful and innovation-friendly approach to the issue.

[3] For example, the Australian Standard/Communications Alliance AS/CA S042 series of standards, which are called up under legislation and enforced by the ACMA in order to achieve the Regulatory Compliance Mark (RCM). Cellular IoT devices connect to a telecommunications network and, therefore, must also comply with the ACMA labelling requirement in order to use the RCM.

Voluntary labelling scheme

1.15. We note Government's commitment to introduce a voluntary labelling scheme and we agree that such a scheme ought to be interoperable with the standard underlying the proposed regulation.

1.16. Against this background, it is important to highlight that there is already an Australian-developed voluntary certification and labelling scheme that is interoperable with *ETSI EN 303 645* (and the corresponding Australian Standard), the European Union Agency For Network And Information Security (ENISA) *Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures* and the US National Institute of Standards and Technology (NIST) *IR 8259 Foundational Cybersecurity Activities for IoT Device Manufacturers*.

1.17. This IoT Security Trust Mark™ and the associated Cybersecurity Labelling Scheme for consumer products already operate in Australia, the UK, European Union and the US. We note that certification trademarks apply in those jurisdictions, thereby potentially limiting the scope for the introduction of further new schemes covered by intellectual property rights.

1.18. Consequently, Government ought to consider making use of already existing certification/labelling schemes prior to embarking on the creation of a new scheme.

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

2.1. The Consultation Paper proposes the introduction of a reporting obligation for ransomware and extortion incidents. It also proposes a second reporting obligation when entities make a ransomware or extortion payment.

2.2. The proposal does not foresee a ban on ransomware payments.

We support this approach, in light of the fact that in certain circumstances the payment of a ransom may be the preferred option to limit harm from the incident. Not introducing a ban also appears justified given ransom payments have been decreasing steadily over the past few years, with 76% making a payment after an attack in 2019 to 41% in 2022.[4]

2.3. We support the proposals in principle but offer the following considerations.

Definition of ransomware attack / extortion and ransom payments

2.4. The Consultation Paper does not provide further detail as to what would be considered a ransomware or extortion incident.

2.5. We believe that a clear definition of which incidents are in scope for the proposed obligations ought to be contained in the legislation (as opposed to any formal or informal guidance).

2.6. This definition should be linked to the consequence or significance of an incident, ideally through already existing concepts for significance as, for example, used in the cyber incident reporting requirements of the SoCI Act.

2.7. If a consequence or significance threshold is being applied to the definition of reportable incidents (where no ransom payment has been made), we propose that

[4] Chainanlysis, https://www.chainalysis.com/blog/crypto-ransomware-revenue-down-as-victims-refuse-to-pay/, 13 Jan 2023, accessed on 23 Feb 2024

incidents that have been successfully mitigated or that do not meet the threshold be excluded from the reporting requirement.

2.8. Importantly, it is our strong recommendation that any entity already covered by the cyber incident reporting requirements under the SoCI Act ought not be required to provide additional reports under the proposed ransomware incident reporting regime, to avoid duplication and, consequently, unnecessary regulatory burden.

2.9. The proposal also envisages a reporting requirement where a ransom or extortion payment has been made. However, it is conceivable that material extortions could be made that do not involve a payment but rather the doing or not doing an act that meets the demands of the extorting party. The reporting requirement ought to also capture the fulfilment of non-monetary demands in order to be comprehensive.

2.10. We also note that any cyber extortion covered under the proposed reporting regime ought to be clearly delineated from extortion concepts that fall within the remit of the *Online Safety Act 2021*.

Entities in scope

2.11. The Consultation Paper states that

> *"A clear threat picture requires up-to-date data about cyber incidents as they occur. This includes the number of ransomware and cyber extortion incidents impacting Australian organisations, the type of ransomware used, the vulnerabilities that are being exploited, the overall impact of an incident and whether a ransom or extortion payment was made by the victim."*[5]

2.12. Simultaneously, the Paper recognises the regulatory burden and the associated compliance difficulties that smaller entities may face if the ransom and extortion incident reporting requirements were to be imposed on those entities. As also highlighted in the Paper, around 98% of businesses in Australia have a turnover of less than $10M and the vast majority (93%) have a turnover of less than $2M.[6]

2.13. We agree with the verbally stated aim (Department of Home Affairs Town Hall meetings) of ensuring that the any new requirements targeted at providing and sharing information about a threat picture and resulting ability to combat such threats needs to increase proportionately with including more entities into the obligation.

2.14. However, the exclusion of the vast majority of businesses from the regime may not provide the breath of information that the regime intends to capture and, subsequently, share to enable improved cyber defences.

Not including these entities may also make them a preferred target for malicious actors.

2.15. Importantly, a blanket exclusion of small businesses does not take into account the supply chain dependencies of those organisations that would be subject to the proposed reporting regime. In many instances, a small business may provide products and services to an entity subject to the reporting requirement. It is unclear whether in this instance the 'large' business would be required to 'absorb' the reporting requirement or, instead, the small business ought to be captured by the reporting requirements. An exclusion of the small business in these circumstances appears contrary to the policy intent.

---

[5] p. 13, Department of Home Affairs, *2023-2030 Cyber Security Strategy: Legislative Package Consultation Paper*, Dec 2024

[6] Australian Small Business and Family Enterprise Ombudsman, *Number of small businesses in Australia*, Aug 2023, https://www.asbfeo.gov.au/sites/default/files/2023-10/Number%20of%20small%20businesses%20in%20Australia_Aug%202023_0.pdf as accessed on 23 Feb 2024

These supply chain interdependencies ought to be clearly addressed in the proposed legislation.

2.16. It may be an option to extend the regime to small businesses in a voluntary manner by means of incentives, awareness raising and education, and assistance with incidents where those target a small business. The voluntary Cyber Health Check Program and the Small Business Cyber Resilience Service could provide this education and assistance. Potentially, additional funding for a large-scale awareness campaign of cyber risks and the availability of these programs is required.

The publication of detailed case studies identifying the cause and possible means of prevention of particular instances of cyber security breaches may also be of assistance for small businesses.

2.17. Alternatively/additionally, different (lesser) penalties and/or a more lenient enforcement approach could be considered for small businesses.

2.18. Our members by and large do not fall into the small business category, and we recommend intensive consultation with this respective sector to gain a good understanding of the needs and capabilities of small businesses, e.g. through consultation with the Australian Small Business and Family Enterprise Ombudsman

2.19. We also urge the Department to consider the importance to harmonise incident reporting requirements with a revised *Privacy Act 1988* (removal of small business exemption).

Information provision, protection and use of information

2.20. The information envisaged to be provided under the new reporting regime is extensive. In line with feedback that we provided in relation to the 72-hour timeline to provide information during a cyber security incident, we re-iterate our concern that the timing of the reporting could be onerous and detract from the task at hand, i.e. the limitation of harm arising from the incident and associated investigation and remediation efforts.

Indeed, the Consultation Paper notes:

> *"In addition, ASD has experienced delays in entities providing technical information relevant to ongoing cyber security incidents."*[7]

We suggest that one reason for such delays may lie in the entity's focus of resources to remediate the incident and the limited availability of stable information within the stated timeframe.

2.21. With respect to the payment of a ransom or fulfilment of extortion demands, it appears, in many cases, unlikely that the decision over such action or indeed the payment itself would be made with a 72-hour timeframe.

2.22. The Consultation Paper is silent on which Government agencies are envisaged to receive the reported information and with which agencies this information can be shared.

2.23. Given the likely sensitive nature of the information and in order to incentivise (or deter) entities from reporting, we strongly recommend restricting the sharing of this information and taking a 'limited use' approach to the reported information. This is of particular importance if it is intended to also share information with regulators. (Also refer to our comments at section 3 below.)

2.24. It is worth noting that we continue to object to a public reporting regime. We hold real concerns that public notification of ransomware attacks and extorsion attempts may

[7] p. 18, Department of Home Affairs, *2023-2030 Cyber Security Strategy: Legislative Package Consultation Paper*, Dec 2024

lead to public concerns/panic and unhelpful media speculations without associated benefits of transparency as the notifying entity will not be in a position to divulge many details given the circumstances of a potentially still ongoing criminal attack or a crime that is still under investigation.

In addition, it is likely that confidential and highly sensitive information will be involved in most ransomware or extortion cases (that may rise to the level of threatening national security) and, consequently, if the information were to be released to the public, it would have to be highly redacted.

Therefore, any reporting of information ought to be published in aggregated anonymised form only, or where more detail is being provided (without suggesting that no anonymisation ought to occur in this instance), only be provided to entities that can derive clear use from the information.

No-fault, no-liability approach

2.25. The Consultation Paper proposes a no-fault, no-liability approach to the reporting of ransomware and extortion incidents and the potential payment of ransoms.

We support this approach in principle.

2.26. While wilful neglect by entities subject to the SoCI Act would be prevented (assuming compliance) by the requirements of that Act and enforced (where required) through the mechanisms of the SoCI Act, it is unclear how such behaviour would be prevented for entities subject to the new reporting regime, but which are not in scope of the SoCI Act.

Further consideration ought to be given to deterring entities from such behaviour while at the same time maintaining a no-fault, no liability approach.

2.27. Against this background it appears particularly important to ensure that the information provided is protected by an appropriately defined 'limited use' principle.

2.28. It also not clear from the Paper whether the no-liability principle would provide a defence against an entity breaching applicable sanctions or crime laws by making a ransom payment of fulfilling an extortion demand.

This ought to be clarified within the legislation.

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

3.1. The 2023-2030 Australian Cyber Security Strategy Discussion Paper[8] sought views on an 'explicit obligation of confidentiality' on the Australian Signals Directorate (ASD) and the Cyber Coordinator to promote the sharing of threat information during a cyber incident. This proposal was supported by a majority of stakeholders, including Communications Alliance.

3.2. However, as set out in the Consultation Paper, the proposed 'limited use' obligation on ASD and the Cyber Coordinator does not actually constitute an 'explicit obligation of confidentiality' on those two entities but rather seeks to limit the permitted uses of the

[8] Australian Government Expert Advisory Board, 2023-2030 Australian Cyber Security Strategy Discussion Paper, Feb 2023, https://www.homeaffairs.gov.au/reports-and-pubs/files/2023-2030_australian_cyber_security_strategy_discussion_paper.pdf accessed on 23 Feb 2024

information once it has been shared with other Government entities, including regulators.

3.3. Furthermore, the Paper provides a list of suggested 'prescribed cyber security purposes' for which the shared information can be used.

We believe that these purposes are substantially too broad and ought to be narrowed to actually limit the use cases required to achieve the policy intent.

For example, the purpose "*to assist the entity with preventing, responding to and mitigating the cyber security incident*"[9] arguably could, from the perspective of a regulator, also include enforcement action as a 'response' to the incident.

Similarly, the purpose "*to facilitate consequence management after a cyber incident*"[10] could be read to include almost anything that has a causal relationship to the incident. (Also refer to our feedback at section 6.)

3.4. As currently proposed, it is also hard to see how a limited use obligation would provide the required certainty to affected entities and, consequently, incentivise them to share information about incidents and threats when regulators gain knowledge of the information provided and can, in almost all instances, subsequently compel the very same information under their own investigative powers that they were prevented from using for regulatory enforcement under the 'limited use obligation.

3.5. Overall, it appears that the sharing of information with a more limited number of Government agencies (identified from the outset) ought to be considered as the current scope for sharing is very broad and less capable to truly guarantee confidentiality of information.

3.6. Importantly, voluntarily provided information ought not be discoverable through a Freedom of Information request. If Government wants to incentivise industry to voluntarily share information, entities affected by an incident ought to have certainty that the information shared cannot be used in civil proceedings and class actions.

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

4.1. Entities captured under the requirements of the SoCI Act already have a number of reporting requirements.

Equally, regulators have the requisite powers to request information for investigation and enforcement action.

Members report that, in the case of an incident, the resources required to comply with (often duplicative) investigatory requests are substantial, even many months or years after the incident in question. Such resources are focused away from activities that would aim to implement learnings from the incident or from other compliance and business activities that may provide a greater value to consumers and the general public.

4.2. Consequently, we are very concerned that any reviews by a CIRB would add an additional layer of investigation and reporting to an already burdensome regime.

Additionally, it is difficult to understand how a CIRB process would operate (and what standing/impact its review, findings and recommendations would have) in amongst

[9] p. 20, Department of Home Affairs, *2023-2030 Cyber Security Strategy: Legislative Package Consultation Paper*, Dec 2024
[10] ibid

potential parallel enforcement proceedings and other regulatory investigations which may be conducted by separate bodies in relation to the same incident. Whilst the paper suggests that the CIRB would operate on a 'no fault' principle and that its "*findings and recommendations would not prejudice law enforcement or judicial proceedings*"[11] it is difficult to see how that would work in practice.

As such, our members generally do not support the introduction of a CIRB.

Despite our members' views, we have nonetheless set out some comments below on the aspects of the CIRB upon which further feedback has been sought.

Scope of CIRB and its functions and powers

4.3. The Consultation Paper raises the question as to how CIRB reviews ought to be initiated and which considerations ought to be taken into account for the initiation of a review.

4.4. Against the background of the question, we believe it is key to ensure that the CIRB's powers (however they may be constructed) only relate to specific cyber incidents, rather than critical infrastructure per se or to network resiliency issues.

Unfortunately, a conflation of these areas is likely given the broad definition of critical infrastructure asset and the additionally proposed inclusion of 'business critical data storage systems' which appear to further extend the scope of critical infrastructure asset to assets that may actually not be critical for the operation of critical infrastructure. (Also refer to section 5 below.)

4.5. In any case, the criteria for incidents that may fall within the scope for review by the CIRB ought to be clearly defined in the legislation. In formulating the criteria care ought to be taken to avoid standardised criteria but, instead, focus the criteria on taking into account the specific context of the incident, e.g. the sector, its size, type of services provided by the affected entity, etc.

With view to limiting regulatory burden and creating consistent frameworks, it will be important to align a materiality threshold for incidents potentially in scope with other already existing thresholds for reportable incidents.

4.6. Following on from the above (focus on incidents rather than critical infrastructure/resilience), it is hard to see how the CIRB could be reviewing systemic issues. We recommend limiting the scope of the incidents able to be reviewed accordingly.

4.7. Given the proposed (and necessary) independence of the CIRB, it appears appropriate that the initiation of reviews also remains removed from any stakeholder influence – including political influence – to the largest extent possible.

Consequently, in case the CIRB was to be established through legislation, reviews ought to be initiated by the CIRB itself.

However, as we elaborate further below, we believe that a non-legislated option may be preferable and alternative initiation mechanisms may apply.

4.8. As indicated earlier (and as noted further below), we are sceptical as to how the CIRB would be enabled to make unbiased recommendations, especially in the public eye, that provide sufficient detail for affected entities. We are concerned that such recommendations would further add to an administrative or quasi-regulatory burden for entities under review.

[11] p. 28, Department of Home Affairs, *2023-2030 Cyber Security Strategy: Legislative Package Consultation Paper*, Dec 2024

Legislated vs non-legislated establishment of a CIRB

4.9. The Consultation Paper appears to assume that the CIRB would be established through legislation. However, in verbal discussions, the Department indicated that this is still an open question, with feedback being sought.

4.10. At this stage, we believe that a non-legislated CIRB would be preferable to an establishment under legislation.

We believe that existing mechanisms, such as Minister-appointed experts or the referral to Parliamentary Committees provide sufficient avenues to review an incident where required.

The establishment of a legislated CIRB appears overly bureaucratic and, potentially, costly, without substantially offsetting benefits. It is unclear in what respects a legislated CIRB would materially differ from existing investigatory mechanisms.

Membership of the CIRB

4.11. Members of the CIRB require sufficient expertise in order to effectively review a given incident. This includes sector-specific as well as cyber security-specific expertise. Depending on the incident, legal expertise may also be of importance.

4.12. We note that individuals with the requisite expertise are limited and may not be available for extensive reviews. They must also be impartial and not be conflicted in their interests.

In this context, it is important to understand that the Australian Transport Safety Bureau (ATSB) in today's form can draw on decades of expertise and research and evidence base. This may not necessarily be the case for a newly established CIRB.

4.13. While standing members of a CIRB may provide for greater consistency across reviews, this arrangement bears the risk that the selected members (for example, by virtue of their office) may not have the requisite expertise, or where such experts are successfully recruited as standing members, their employment may entail substantial costs.

4.14. On balance, we believe that a pool of experts that can be drawn upon by the Minister or a Parliamentary Committee or a mix of standing CIRB members and a pool of industry experts may provide for the most efficient and effective approach to the constitution of a CIRB.

All stakeholders ought to be consulted extensively prior to the appointment of any members or, in particular, the chair of the CIRB.

We note that we are uncertain as to why experts from academia ought to form part of the CIRB membership and would appreciate further detail in this respect.

Information provision, protection and use of information

4.15. Building on our feedback in relation to a limited use obligation, we also raise concerns with the confidentiality and appropriate protection of information provided (be it voluntarily or compelled) to the CIRB.

4.16. As with the voluntary information provided to agencies for the purpose of incident and threat sharing, any information provided to the CIRB ought to be exempt from the *Freedom of Information Act 1982* and not be available in civil proceedings or class actions.

4.17. The information provided to the CIRB ought not be shared with Government agencies or regulators. Instead the findings of the CIRB ought to be shared with Government through a report on a confidential basis.

4.18. In addition, the information ought to be subject to an appropriately formulated limited use obligation.

4.19. We are alarmed by the Consultation Paper's statement that

> *"Uphold[ing] public interest criteria to manage sensitive information considered in the scope of a post-incident review. This could include not publicly revealing vulnerabilities, personal information or non-personal information that may expose individuals and businesses to harm."*

is proposed as a consideration for the management of sensitive information. The language of this criterion appears overly broad and discretionary and would, so we believe, not provide entities participating in a review with sufficient confidence that sensitive information provided indeed remains confidential.

Root cause analysis and no-fault principles

4.20. The Consultation Paper proposes a no-fault and/or no-blame approach to reviews by the CIRB. The Paper also suggests as a function of the CIRB to gain an understanding of the root cause of an incident and, following conclusion of a review, the publication of

> *"findings and best practice learnings to enhance collective cyber security and help prevent similar incidents from occurring in the future"*

Without further detail, we find it difficult to understand how the publication of meaningful information that would assist entities to remediate similar exposures could be balanced with a no-fault approach to a review.

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

5.1. The Consultation Paper proposes an express inclusion of 'business critical data storage systems' into the definition of 'asset' in the SoCI Act.

5.2. As previously highlighted, we are concerned with the broadening of the scope of critical infrastructure assets.

5.3. It is unclear as to what would constitute 'business critical data storage systems'. The difficulties stem from an, in our view, overly broad definition of 'asset' under the SoCI Act. For example, would business network data and metadata be included in that definition?

Assume, for example, a telecommunications network provider encountered an incident in its systems that inhibited its ability to produce call detail records (CDRs) while the network still functions to connect calls as intended. Arguably, the impact of this incident is 'relevant' as it has an impact on the availability and/or the reliability of the 'asset'. However, the impact does not impact on the functioning of the infrastructure that is really critical to Australia's economy or the well-being of its people. That is, the impact is not material to the operation of the critical infrastructure.

5.4. In this context we highlight the definition of critical infrastructure as published in the *2023 Critical Infrastructure Resilience Strategy* as

> *"those physical facilities, supply chains, information technologies and communication networks, which if destroyed, degraded or rendered unavailable for an extended period, would significantly impact the social or economic*

wellbeing of the nation, or affect Australia's ability to conduct national defence and ensure national security."[12]

5.5. We argue that the proposed extension has the potential to capture a multitude of business critical data storage systems that are not critical to the operation of the underlying critical infrastructure and urge the Department to apply a clear and more limited definition to any data or systems that considers not already being in scope of the SoCI Act which aligns more closely with the policy intent of protecting infrastructure that "*if destroyed, degraded or rendered unavailable for an extended period, would significantly impact the social or economic wellbeing of the nation, or affect Australia's ability to conduct national defence and ensure national security*."[13]

5.6. We also reiterate our concerns with respect to a potential overlap of the existing (and/or revised) requirements of the *Privacy Act 1988* to appropriately protect personal information and report breaches under the Mandatory Notification of Data Breaches Scheme under that Act. We recommend awaiting the conclusion of the Privacy Act Review prior to implementing further changes to the SoCI Act that may target similar outcomes.

5.7. The Consultation Paper asserts that

"The current definitions of 'asset' and 'material risk' in the SOCI Act do not explicitly call out these data storage systems. As a result, many entities are not including these systems in their CIRMP or reporting significant data breaches when they affect these systems."[14]

We are curious as to the empirical basis for the assertion of a causal link between the SoCI Act not explicitly addressing business critical data storage systems and the (purported) lack of entities not including such systems in their critical infrastructure risk management program (CIRMP), or an entity not reporting significant data breaches when they affect such systems, in circumstances where a relevant impact would actually destroy, degrade or render unavailable such an asset for an extended period of time and where, in such circumstances, this impact would significantly affect the Australian economy.

Similarly, we would like to understand more as to which significant data breaches of business critical data storage systems that meet the definition of the *2023 Critical Infrastructure Resilience Strategy* have not been reported.

5.8. Irrespective of our objections above, we note that the proposal to obtain Board approval should only apply to entities that are required under the existing rules to prepare a CIRMP and that are already required to submit a Board-approved annual report to Government.

[12] p. 4, Department of Home Affairs, *Critical Infrastructure Resilience Strategy*, Feb 2023, https://www.cisc.gov.au/resources-subsite/Documents/critical-infrastructure-resilience-strategy-2023.pdf, accessed on 24 Feb 2024
[13] ibid
[14] p. 36, Department of Home Affairs, *2023-2030 Cyber Security Strategy: Legislative Package Consultation Paper*, Dec 2024

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

Breadth of powers

6.1. The Consultation Paper proposes to establish last resort powers that would seek to help critical infrastructure entities manage the consequences of significant incidents.

6.2. We understand that the need for some of these powers, such as the ability to authorise sharing of information, may have become apparent in recent cyber incidents.

6.3. We support the ability for Government to authorise sharing of information in certain circumstances but do not support a compulsion to do so.

6.4. However, without a clearer understanding of what is encompassed by the term 'consequence management', we are concerned with the breadth of the proposed powers, even as a last resort power.

6.5. The criterion for the consequence to have a "*causal link to an incident impacting a critical infrastructure asset*"[15] insufficiently limits consequences in scope as the common language definition of consequence itself provides that an (in)action has a 'result or effect'. It is, therefore, not clear how far down the cascading chain of causal events the ability to manage 'consequences' would extend.

6.6. The breadth of the proposed powers is also concerning as the powers appear to be intended to not only apply to the technical incident but also to an entity's engagement with its customers as the power to direct an affected entity to replace documents makes clear.

6.7. Against this background, we request that it be made clear in the legislation that the consequence management powers do not extend to powers to direct the payment of compensation or to provide information to third parties, including for the purposes of litigation.

We also believe that the incidents that could be subject (to more limited powers) ought to be subject to clearly defined, narrow criteria.

6.8. Furthermore, we are concerned with the proposed unfettered power to

> "*Gather information for the purpose of consequence management, if this does not interfere with or impede any other law enforcement action or regulatory action.*"[16]

This power could enable Government to take regulatory or other enforcement action against an entity as doing so would not necessarily "*interfere with or impede any other law enforcement action or regulatory action*".

It ought to be put beyond doubt that information obtained in this manner cannot be used for regulatory or enforcement action.

6.9. As with other powers under the SoCI Act, the proposed breadth of the powers is also concerning due to its application to critical infrastructure and the overly broad definition of 'asset' that we highlighted above. This implies that the powers can be exercised for assets that, as we argued above, do not have to potential to "*prejudice the socioeconomic stability, national security or defence of Australia*"[17].

[15] p. 44, ibid
[16] p. 43, Department of Home Affairs, *2023-2030 Cyber Security Strategy: Legislative Package Consultation Paper*, Dec 2024
[17] p. 42, ibid

Authorisation of powers

6.10. In addition to the issues raised in relation to the breadth of the powers, we are concerned with the authorisation process for the use of these powers. Given political pressures during or shortly after a cyber incident and the interests of the relevant portfolio agencies, it appears that authorisation through the Minister for Home Affairs may not provide for sufficient independence. Alternative authorisation arrangements ought to be considered.

6.11. The Consultation Paper proposes that

> *"In determining whether to exercise the power, the Minister must consider the public interest – for example, whether issuing the direction is in the interest of public health and safety and is proportionate to the risk of inaction."*[18]

Unfortunately, none of the proposed safeguards consider the legitimate interests of entities subject to a direction. We request that a 'balancing test' be included to ensure that business interests are balanced against public or other interests.

Cost of compliance with directions

6.12. The proposal of the Consultation Paper does not provide details as to how the costs of compliance with a direction would allocated. However, the sentence

> *"The Department seeks your views on the proposed scope of this directions power, and what costs would be incurred in complying with these powers."*[19]

appears to imply that costs ought to be borne by the entity required to comply. This is not necessarily appropriate where a third party has received a direction to comply with a consequence management direction.

We also note that it is impossible to provide a meaningful idea as to what costs would be incurred given the breadth of actions that can be required of an entity.

6.13. With respect to costs, it is also unclear whether the proposal would provide Government with powers to allocate liability or fault, and consequently direct the absorption of costs for compliance.

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

7.1. We lend in-principle support to the simplification and clarification as to when responsible entities can disclose protected information about their assets for the purposes of operating them or to manage risks related to them.

7.2. In addition to the proposed reforms, we recommend a review of the definition of 'protected information' itself as the current definition of protected information also includes information that is publicly available or where disclosure would have no negative impact on the entity or national security.

[18] p. 45, ibid
[19] p. 45, ibid

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

8.1. We support Measure 8 in principle and do not offer additional feedback at this stage.

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

9.1. Communications Alliance is a member of the Australian Telecommunications Security Reference Group (ATSRG) that is currently progressing the consolidation of the telecommunications security requirements under the *Telecommunications Act 1997* and relevant requirements of the SoCI Act.

9.2. We are providing feedback through this group and will not include further commentary in this submission.

9.3. We commend the Department and the Department of Infrastructure, Transport, Regional Development, Communications and the Arts (DITRDCA) for the manner with which the process for consolidation of the two regimes has so far been conducted. This co-design approach ought to form a baseline for further engagement processes of Government and industry where co-design or co-regulation is required.

10. Conclusion

Communications Alliance looks forward to continued engagement with the Department and all relevant stakeholders over efforts to continuously enhance Australia's cyber posture through measures that focus on secure operation of infrastructure that is critical to the effective functioning of Australia's economy and/or to the wellbeing of its people.

To that end, we share Government's desire to create a robust, effective and efficient cyber-security framework that appropriately allocates responsibilities across all actors involved, and that enables all Australians to adequately protect themselves against the risks that come with it while enjoying the enormous benefits that it affords to all of us.

For any questions relating to this submission please contact Christiane Gillespie-Jones on 02 9959 9111 or at c.gillespiejones@commsalliance.com.au

Published by:
COMMUNICATIONS
ALLIANCE LTD

Level 12
75 Miller Street
North Sydney
NSW 2060 Australia

Correspondence
PO Box 444
Milsons Point
NSW 1565

T 61 2 9959 9111
F 61 2 9954 6136
E
info@commsalliance.com.au
www.commsalliance.com.au
ABN 56 078 026 507