ENGINEERS
AUSTRALIA

2023-2030 Australian Cyber Security Strategy: Legislative Reforms

Engineers Australia's Submission

2023-2030 Australian Cyber Security Strategy: Legislative Reforms

Engineers Australia's Submission

Author: Louis Field

Engineers Australia
11 National Circuit, Barton ACT 2600
Tel: +61 2 6270 6555
Email: policy@engineersaustralia.org.au

engineersaustralia.org.au

Contents

Introduction

Engineers Australia commends the Australian Government for developing a strong *2023-2030 Australian Cyber Security Strategy* and *2023-2030 Australian Cyber Security Action Plan*, building upon the insights gained from its industry consultation in 2023. However, this process has underscored gaps in the *Security of Critical Infrastructure Act 2018* (SOCI Act) that require attention to enhance the security of the Australian cyberspace.

With the proliferation of consumer smart devices and increasingly interconnected homes, there is an immediate need to establish adequate regulatory requirements and standards to safeguard our communities. While creating new legislation targeting all internet of things (IoT) devices might be a potential solution to explore, there are potential complexities arising from the interaction of this new cybersecurity legislation and existing laws, creating a legal patchwork and potentially adding new layers of administrative burden.

Engineers Australia recognises the work done by the Department of Home Affairs (the Department) to seek new solutions to tackle a growing issue that could potentially impact us all. Addressing the intricate and continually evolving nature of cybersecurity requires a nimble and adaptive solution.

In this submission, Engineers Australia offers the view of its expert members on a few alternative approaches the Department could consider that may streamline the problem while still effectively addressing the issues.

About Engineers Australia

Engineering is the essential link between thinking and doing. Between idea, and implementation. It's our means for positive, sustainable change, with an influence on every aspect of modern society. Engineers are the enablers of productivity because they convert smart ideas into new products, processes and services.

As Australia's national body for engineering, we are the voice and champion of our 120,000-plus members. We provide them with the resources, connections, and growth they need to do ethical, competent and high-value work in our communities.

A mission-based, not-for-profit professional association, Engineers Australia is constituted by Royal Charter to advance the science and practice of engineering for the benefit of the community. We back today's problem-solvers, so they can shape a better tomorrow.

As Australia's signatory to the International Engineering Alliance, Engineers Australia maintains national professional standards, benchmarked against international norms. Under the Migration Regulations 1994, Engineers Australia is the designated assessing authority to perform assessment of potential migrant engineering professionals' skills, qualifications, and/or work experience to ensure they meet the occupational standards needed for employment in Australia.

Engineers Australia can apply expertise in Cyber Security, Systems Engineering and Standards Development, offering the Government a unique view and advice to strengthen the security of our communities both offline and online.

Contact

Engineers Australia welcomes the opportunity to engage further with the Department of Home Affairs. These are complex and contextual issues. Engineers Australia has significant expertise in our Learned Society Colleges and Technical Societies that can assist in addressing them. To discuss the points raised in this submission further, please contact policy@engineersaustralia.org.au.

Part 1 – New Cyber Security Legislation

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

Responsible entities

"*A chain is only as strong as its weakest link.*"[1] Protecting the supply chain of IoT devices in Australia will require the participation of manufacturers, subcontractors, software developers, importers, distributors and end-users. Cybersecurity is a collective responsibility, necessitating a collaborative environment to fully enhance system security.

Engineers Australia supports adopting an approach similar to consumer product safety, in line with the UK's Product Safety and Telecommunications Infrastructure (PSTI) Act, which mandates that vendors, suppliers, importers, and manufacturers adhere to a set standard. This ensures a heightened level of protection without excessively increasing financial burdens.

The idea of a labelling scheme for consumer-grade IoT devices, whether it be voluntary and industry-led or mandatory, is a useful concept for consumer product security. However, existing models in place could be followed, such as Electromagnetic Compatibility (EMC) compliance, administered by the Australian Communications and Media Authority (ACMA). Using an existing model with which suppliers of IoT devices must already comply would ease the burden on the manufacturers, suppliers and distributors.

Consideration should be given to avoiding new layers of additional red-tape. Better use should be made of the current compliance systems in place. Incorporating cyber security compliance within the Regulatory Compliance Mark, overseen by the ACMA, presents a viable solution for establishing local infrastructure and services dedicated to conformity assessment. This approach aims to facilitate labelling capabilities and prevent hindrances to the local industry.

Standards to be adopted in Australia

ETSI EN 303 645

Engineers Australia strongly recommends adopting ETSI EN 303 645 which is the European Standard for cyber security for consumer internet of things. Aligning with international standards is an important first step to providing greater security requirements on IoT devices.

Due to the range and variety of IoT devices and corresponding levels of cyber security threats, a one-size-fits-all approach would not be appropriate. The ETSI EN 303 645 standard offers multiple principles allowing for a more tailored approach to securing IoT devices. The Department's reference to the first three principles as a minimum standard is necessary however it may not be sufficient because not all IoT devices have user interfaces and many constrained devices are not software-upgradable. We recommend the adoption of all ETSI EN 303 645 cyber security provisions for consumer IoT.

A gradual approach of mandated measures could be adopted, based on a risk management approach for each IoT device, considering the following:

1. The device's operating environment, including the device's network connection(s)
2. The sensitivity and value of the device's data

[1] Thomas Reid, *Essays on the Intellectual Powers of Man*, Cornhill Magazine, 1868

3. The attractiveness of the device's function and data as a cyber-attack target
4. The potential threat posed by the target, including whether it could be used as a gateway or bot to facilitate further cyber-attacks
5. Practicality constraints, including processing power, memory and energy
6. Other aspects which impacts the device's risk profile.

Additional Standards

Risk mitigation is a prime engineering principle that should be considered in Australia's approach to cyber security. Should the Government wish to consider recognising multiple standards, Engineers Australia would also recommend IEC 62443 as an additional standard to add to ETSI EN 303 645, and especially its risk mitigation design approach defined under IEC 62443-4-2 Edition 1.0 2019-02 Security for industrial automation and control systems – Part 4-2: Technical security requirements for IACS components.

Smart devices to be regulated

Definition

Engineers Australia recommends adopting a broad definition for smart devices that are subject to an Australian mandatory standard. This would cater for a wider range of IoT devices that have yet to be invented or do not fit clearly in one category.

The UK's PTSI Act should be used for guidance to help Australia build its cyber security strategy. Its part 4 "Relevant connectable products" and part 5 "Types of products that may be relevant connectable products" would be particularly helpful. While this may provide guidance, Engineers Australia does not recommend the definition be adopted wholly, as there are some limitations, such as what it considers a hack. A broader approach to avoid such limitations should be considered for the Australian context.

There needs to be scope to exempt some smart devices from mandatory compliance where the level of risk would not be worth the additional cost required to protect them. An example of these devices is a low-risk device, connected to a secure local network behind a gateway (with the gateway being covered by ETSI TS 103 848). Or simple devices which gather non-critical data and represent a low-profile target.

Using a risk management approach and assessing models like EMC, as listed above, these smart devices could easily be exempted from regulation without increasing the level of risk. All other smart devices collecting critical information should be covered by a mandatory cyber security standard.

Introduction timeframes

Engineers Australia believes the timeframe should be reflective of new product life cycles for smart devices, which on average is 12 to 18 months. Therefore, 12 months should be a reasonable timeframe for industry to adjust to new cyber security requirements for smart devices.

However, grandfathering provisions may be necessary for existing designs that cannot be practically made compliant. Smart devices that cannot be updated or modified should be given a 24-month period after which they should be declared unsafe by default and not used anymore.

Engineers Australia recommends a phased introduction of these provisions, using a risk management approach to focus on high-risk devices first then cascading to lower levels. This would ease the burden on industry while providing a clear pathway.

Monitoring and enforcement

The *Regulatory Powers (Standard Provisions) Act 2014* (the Regulatory Powers Act) does not provide a suitable framework for monitoring compliance and enforcement of a mandatory cyber security standard for smart devices. This is because of existing market disparities concerning cybersecurity knowledge and technical capabilities. Large businesses have the resources, people and time to build a deeper understanding of the cybersecurity standards and environment requirements when small and medium enterprises (SMEs) generally do not. The Regulatory Powers Act does not cater for that difference in knowledge and capability.

This highlights the need for the Government to invest more on educating SMEs on cyber security to help businesses across Australia to become more proactive on low-cost assessments. Lack of knowledge is too often the key issue leading to a lack of security opening the door to cyber-attacks. Educating businesses on the need for updating systems regularly, implementing strong passwords and backup policies, as well as two factor verification processes is key to increasing Australia's cyber security. Engineers Australia strongly supports the Government initiative on establishing a voluntary cyber health-check program, recommending the introduction of penetration tests (aka bug bounty), as well as a Small Business Cyber Resilience Service.

Before new legislation is created covering consumer product cyber security, Engineers Australia recommends seeing how existing legislation such as the *Competition and Consumer Act 2010* could be enhanced to achieve the same results. This legislation already covers consumer product safety and could be extended to include cyber security, leading to improved outcomes through a modest adjustment within an established regulatory framework. Using existing and proven frameworks appears to be the optimal solution, aligning with the Government's objective of enhancing cybersecurity standards for smart devices while minimising supply chain impediment.

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

Scope of reporting obligations

Engineers Australia supports the Department's suggested list of potential information to be reported as the main goal is to define the scope of the attack, timeframe under which it happened, entry point, type of attack, and what data was targeted. This approach would allow responsible entities to run a risk assessment on this attack on the community as well as define whether this was due to a human or technical error. An understanding on the nature of the ransom demand and timeframe of the demand is then needed.

Some additional information is required should the ransom be paid as it could assist further investigation and future resilience. Understanding how the payment was made, the amount paid, who paid it (for example, company or insurance) and the results of payment, i.e. what guarantees were provided to ensure no trojan horse was returned sleeping or waiting to be used on another event.

Which entities are required to report

Finding an appropriate scope of ransomware reporting obligations to increase visibility of ransomware and cyber extortion threats, while minimising the regulatory burden on entities with less capacity to fulfil these obligations, is a delicate exercise. It would be best if all businesses that are victims of cyber extortion are obligated to report it.

The main issue here correlates to the amount of information required to report and the competence of the organisation to compile data and make that report. A two-tiered approach could be used, separating larger organisations with turnovers of over $10 million and SMEs. For large organisations, providing the

full suite of information needed would be appropriate. For SMEs, the Government should expect a simpler amount of information be shared. This still needs to be enough to identify the ransomware attack, with the Government then aiding with understanding the attack.

The Department could also explore the option to require insurers to report any incidents with which they have assisted their clients. This would provide further incentive for businesses to report any cyber incidents but also a safety net for the Government to get more accurate reporting.

Timeframes for reporting

Timely reporting is critical. Best practice would dictate that any incidents are to be reported before any payment is made, and within 24 hours for high level risk incidents to the community.

Engineers Australia recommends that SOCI timeframes be applied to any other legislation related to cyber security for consistency.

'No-fault' and 'no-liability' protection principles

Engineers Australia considers it likely that 'no-fault' and 'no-liability' protection principles would have a major impact on businesses' confidence to report ransomware or cyber extortion incidents. It would allow staff of victim companies to report quickly about any incidents without the need to protect their commercial and/or legal risks before reporting, fast-tracking the process considerably and maximising chances of identifying the perpetrators.

However, 'no-fault' and 'no-liability' protection principles should not act as a way to exempt businesses from being accountable for their cyber security and the community's data safety. In fact, the principles should support the public's expectation that businesses take responsibility for their cyber security through timely reporting of a ransomware or cyber extortion incident, demonstrating intent to work on how to recover from the incident, and putting measures in place to proactively manage future cyber risks.

Penalties for non-compliance

Enforcement mechanisms of any regulatory obligations need to have the right balance of incentives and consequences. On one hand, any negligence, non-compliance and/or refusal to report should be penalised to deter other entities. Using public reporting and/or imposing fines based on the impact to the community and degree of negligence are two recommended options. Fines could follow what has been implemented in countries such as Finland where fines are based on a percentage of companies' taxable income/revenue.

However, finite resources should prioritise detecting and policing cyber criminals, rather than policing businesses for not reporting. Therefore, greater focus should be on incentivising businesses to report ransomware or cyber extortion incidents. Engineers Australia supports the Government's initiative to provide a greater level of assistance to businesses to understand their level of cyber security and encourage the Government to invest more in developing risk mitigation programs and additional protection capabilities to help them protect critical data.

Sharing ransomware reporting information

Lessons everyone can learn from previous incidents are one of the most important incentives for the industry to share ransomware reporting information. Anonymised case studies and lessons learned reports would assist all businesses to understand the threat environment and the tactics, new techniques and procedures used by hackers. The type of information that should be shared in these anonymised reports and case studies about ransomware incidents should be:

- Method of infection/types of attack

- Defence arrangements that have failed/hackers' entry point
- Type of product/software that was targeted

These anonymised information reports on ransomware incidents will need to be classified into a range of categories to reflect the different industries affected and then shared within the same organisation sizes. What would affect a large organisation will not necessarily be relevant to a smaller one. We would also suggest separating reports into two sides: technical and governance. Technical reports would be particularly useful to cyber engineers and IT professionals, while company directors would greatly benefit from a better understanding of the threat environment to make more secure governance decisions.

A release of these reports on a quarterly basis would seem an appropriate timeframe to gather sufficient information and provide enough lessons for the industry to learn from.

Measure 3: Encouraging engagement during cyber incidents – Limited use obligation on the Australian Signals Directorate (ASD)

Limiting the use of cyber incident information

Engineers Australia strongly supports the limited use obligation on the Australian Signals Directorate (ASD) and National Cyber Security Coordinator (Cyber Coordinator). As explained in measure 2, the aim is to create a collaborative environment inviting all businesses to report any ransomware or cyber extortion incidents as early as possible to provide more vital data and information to identify and stop cyber criminals.

One major deterrent in sharing information for both businesses and individuals is how sensitive information, such as personal or commercially sensitive data, can be accessed and used afterwards. Therefore, this type of information should be included in the 'prescribed cyber security purposes' to limit the use of cyber incident information shared with both ASD and Cyber Coordinator.

Sharing cyber incident information

Clear restrictions should be set on public sharing of information gathered through ransomware reporting to encourage all to share on any types of incidents. All sensitive information should be anonymised to ensure identities are protected. The use of this information should be solely for the purpose of understanding the incident and any potential threats to other businesses and/or individuals, as well as helping businesses and Government to develop recovery options.

Government agencies should be allowed to share this information with each other under the 'need to know principle' for the purposes identified under the limited use obligation. However, any agencies with which the information can be shared should be clearly identified. Any unauthorised disclosure should be pursued, and appropriate sanctions applied to anyone releasing confidential information.

Incentives to engage with Government after a cyber incident

The most efficient way that the Government can promote and incentivise entities to share information and collaborate with ASD and the Cyber Coordinator in the aftermath of a cyber incident is to demonstrate how easy, effective, useful and confidential these ransomware report mechanisms are by:

- Simplifying the reporting mechanism and reporting portal - a 'one portal' approach to avoid any confusion.

- Providing the industry access to anonymised reports on reported cyber-attacks - a valuable source of useful information for businesses to better understand and mitigate risk on their own systems.
- Demonstrating how collected information was used to deliver on successful outcomes – showing how everyone is contributing to stop cyber-criminal activities.
- Securing any confidential and sensitive information from any publications – reassuring all that sharing any information will not be detrimental to their business activity and reputation.

Contributing to the fight against cyber-criminality should become part of any corporate social responsibility. Australian businesses should not fear sharing ransomware reports but rather be proud to assist the Government and industry in better understanding and ultimately protecting the Australian cyber space.

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

Designing a CIRB

Engineers Australia recommends that the Department follows the example of the Australian Transport Safety Bureau (ATSB) to design a CIRB. The purpose of a CIRB should be to understand the process by which the incident happened and issue advice to government and industry on how to avoid recurrence.

Functions of the CIRB

The scope of action of a CIRB should be to:

1. Deliver reviews on cyber incidents, understanding what happened, how it happened, the extent of the damages, remedial actions taken, and any other vulnerabilities discovered.
2. Oversee the distribution of lesson learned.

The Government could also consider whether the CIRB should have within its scope a broader role to monitor improvements in incident reporting and the effectiveness of recovery efforts, sharing common themes across lessons learned from multiple reviews.

It is essential for a CIRB to align with Australian Cyber Security Centre's (ACSC's) role and responsibilities to avoid redundant and conflicting operations and outcomes. Responsibilities should be maintained within the ACSC whenever the mandate already exists and is already operating effectively.

The CIRB should not interfere with law enforcement, national security, intelligence and regulatory activities. To ensure this, the CIRB should focus on distributing lessons learned in order to strengthen resilience and prevent future incidents. Similar to the ATSB approach, confidentiality agreements need to be put in place with each member of the CIRB.

'No-fault' principle

The CIRB should not be purposed nor scoped to lay blame. A 'no-fault' approach, similar to the ATSB, should be the cornerstone for the CIRB.

Engineers Australia supports the Department's proposed solution and agrees that the CIRB should not:

- Apportion blame or fault for cyber incidents
- Provide the means to determine the liability of an entity in respect of a cyber incident
- Assist in court proceedings between parties relating to a cyber incident
- Allow any adverse inference to be drawn from the fact that an entity was involved in a cyber incident.

Initiating a CIRB review

While not all cyber incidents would be worthy of a full CIRB review, ignoring smaller scale cyber-attacks could be a missed opportunity to prevent larger ones. As all cyber incidents are not of the same calibre, the CIRB could proceed with full comprehensive reviews on either recurring, significant, high community risk and damage incidents; while still proceeding with more light touch reviews for smaller, lower-risk types of incidents. This approach will maximise the impact of the CIRB.

The CIRB could also adopt a multi-tiered approach, with different standing CIRB members reviewing each category of cyber incidents based on size, risk-level, occurrence, impact on community etc. Although the US Cyber Safety Review Board's approach is sound, especially given the size of the US population and therefore number of cyber incidents happening every day, Australia's smaller scale could allow for review of all cyber incidents, bringing a greater level of security and safety.

CIRB membership

An appropriate mix of expertise would be required to create a relevant and capable CIRB. Each would provide different views and perspectives which will provide for more effective review and credible advice. However, a CIRB composed of standing members only cannot have expertise on all types and instances of cyber incidents. As such, the Department's third option of a blend between standing members and a pool of experts who can be appointed to facilitate a specific review seems the most practical. Expert panels could be created from the pool by category of cyber incident and assist standing CIRB members whenever relevant.

Engineers Australia suggests the following expertise is needed for the skills mix of standing CIRB members:

- Corporate governance/Company director
- Legal expertise in the relevant governing legislation
- IT, including IT systems, software coding and human interactions
- Cyber engineering, including IT and Operational Technology (OT) systems, hardware, firmware and software
- Academia/research, including knowledge of emerging technologies and current R&D
- Product manufacturing
- ACSC representative

At its establishment, some familiarity with the operation of the 'no-fault' ATSB model would be valuable to the CIRB. If this experience is not among the standing CIRB members, it would be useful to appoint an adviser with this expertise to the CIRB's secretariat.

It is not unreasonable for all CIRB standing members to be required to hold and maintain a minimum NV1 security clearance level. The CIRB's handling of classified and commercially sensitive information would then be handled in accordance with that framework. Similarly, conflicts of interest with respect to specific reviews should be disclosed and, as dictated by good governance, CIRB members would be excluded from participating in any reviews where there is a real or perceived conflict of interest.

For the wider pooler of experts, nominations or endorsements could be sought from industry bodies, universities and peak bodies. This would provide a minimum level of professional vetting, and then security clearances for individuals in the pool could be pursued on an as-needs basis.

Engineers Australia supports the CIRB chair being a new independent official appointed by the Government. We recommend that extensive Board governance experience be an essential selection criteria for the CIRB Chair.

Power to initiate a CIRB review

Engineers Australia notes the Department's options for stakeholders with the power to initiate a CIRB review:

- The Minister for Cyber Security
- CIRB itself
- The National Cyber Security Coordinator
- Agreement between the Minister for Cyber Security and relevant Minister, depending on the nature of the proposed review.

Engineers Australia considers that there is sufficient justification for all of these stakeholders to have the ability to, at a minimum, *propose* that a cyber incident be reviewed.

For administrative purposes, and to avoid duplication, it may be necessary for the actual power to initiate a CIRB review to reside with the Minister for Cyber Security, with the ability for the Minister to delegate this power to the CIRB itself or the National Cyber Security Coordinator for certain types of cyber incidents, as appropriate.

As a safeguard, should the Minister reject the advice of the CIRB, National Cyber Security Coordinator or the relevant Minister to initiate a CIRB review, the Minister should be required to document the reasons for the decision and provide this to information to all parties that have the power to propose that a cyber incident be reviewed.

Investigatory powers

Reviewing options proposed by the Department, Engineers Australia believes that it would be best to provide limited information gathering powers to the CIRB to gather information for incident reviews. The ATSB has proven the need for these types of limited powers to be granted to review boards to ensure proper levels of information are shared in a safe 'no-fault' environment.

Therefore, the CIRB should be granted sufficient powers to gather information efficiently. Where there is a blended option of standing CIRB members being supported by a pool of experts, only the standing members should be authorised to exercise information gathering powers. The chair should be the only issuer of the notice to produce and should use this power only when they reasonably believe the entity required to produce has control of the documents, information or knowledge that will assist the CIRB. The CIRB should always request information be provided voluntarily before using information gathering powers.

On the face of it, Engineers Australia considers that the CIRB should be covered by a 'limited use obligation', as per our recommendation above for the ASD and the Cyber Coordinator. This would provide consistency and also support business confidence in the protection of information. However, it is important that a limited use obligation would not unduly constrain the CIRB to the extent that information used to produce lessons learned from a particular review could not also be used by the CIRB to consider in its broader insights from multiple reviews. It will be critical that the CIRB can consider emerging themes, recurrent issues and persistent risks arising from multiple reviews as part of meeting its objective to strengthen Australia's collective cyber resilience.

As per the ATSB model, the CIRB should be equipped with enforcement mechanisms should an entity fail to produce requested evidence. We support these enforcement mechanisms to be proportionate and aligned with the 'no-fault' principle as described previously. Unlike the ATSB model, Engineers Australia considers that penalties should be proportionate with the nature of the cyber incident under investigation. A default penalty would seem inappropriate given the sheer variety of size, level of importance and community impact of businesses involved.

Impartiality

The CIRB's impartiality will be greatly dictated by its skills composition, and its governance arrangements for disclosure of interests, for outside employment (particularly where an appointment may be full-time, such as the Chair), and the Minister's powers in relation to appointments and the termination of appointments. Professional credentials also provide assurances on a professional abiding to a code of ethics (as is the case for membership of Engineers Australia), helping to ensure impartiality across the Board. Impartiality could also be further reinforced by establishing an enforceable code of conduct for all members with provisions on appropriate sanctions for non-compliance.

To build credibility, the CIRB will need to comprise the appropriate expertise across a wide range of sectors and industries. This is why Engineers Australia supports a specific set of expert members to be part of the standing CIRB 'core' group while drawing any specialist knowledge from the pool of experts whenever necessary.

Protecting sensitive information

Given the context that the CIRB will be operating in, it could be expected that sensitive information held by CIRB to itself become a target of cyber-criminals.

Safeguards similar to what are applied to Restricted Defence Work should be put in place to protect and secure all gathered information. This would include, but is not limited to, the use of:

- Local server
- Data encryption
- Written agreements
- Emails automatically deleted after a set amount of days
- Inability to download data

No CIRB members should be allowed to hold any form of information on personal devices or be in a capacity to share any of it outside the CIRB. Should the CIRB meet online, it should be done within Government secured network systems, using approved devices.

Part 2 – Amendments to the SOCI Act

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

Engineers Australia supports the Department's proposed amendments to the SOCI Act. Consideration should be given to aligning the wording of all proposed amendments to international standard IEC 62443, which was developed to secure industrial automation and control systems throughout their lifecycle. Aligning the wording would allow greater ease of use of international standards and strengthen any future international collaboration to protect Australian cyber space.

Although the proposed amendments would increase the level of protection of critical infrastructure and especially data storage systems that hold business critical data, there are concerns that these protective mechanisms should also apply to the software recording data. Recent cyber incidents have shown how, despite a greater level of encryption and protection of the data storage systems, business critical data was still accessed by cyber-criminals through the less protected software recording the data. Provisions in the SOCI Act should ensure that not only the data storage systems are protected but also the software used to record that data. This will secure business-critical data as well as the event log data.

This also prompts further debate on how long businesses need to keep critical data. Major cyber incidents have shown how businesses tend to maximise the amount of sensitive data stored, exposing themselves to major cyber incidents impacting millions of Australians. Much of the sensitive information stored, such as copies of passports or driver licences, was not critically required by the businesses affected by the cyber incident to operate. Once customers have been identified and their accounts setup, businesses should not be allowed to keep record of their critical identity information documents but rather be required to have them deleted as soon as possible.

Reducing the amount of critical data stored would be an easy way to both reduce the attractiveness of a business as a cyber target, and lower the impact should any cyber incidents happen. The SOCI Act should consider mandating the forced deletion of personal and/or sensitive information kept for more than a reasonable amount of time. Stripping sensitive data stored to only critically needed information would reduce the level of risk and impact on the community.

Engineers Australia hears anecdotally from our members that many businesses do not have the in-house expertise and capability to secure their data storage systems appropriately and are outsourcing to third-party specialists. Many of these third-party specialists provide regular training and refresher courses to their business customers to keep them abreast of the latest changes to cyber threats and cybersecurity requirements. Other members are pointing out how poor companies can be at managing the operational technology data they build.

It is recommended ISO/IEC 27001:2022, the world's best-known standard for information security management systems, be implemented across all critical infrastructure as a minimum, and regular information security management system audits be undertaken to ensure the safety of data storage systems. Standards are regularly introduced for IoT devices however, very few are mandated for critical infrastructure entities despite the latter storing a far greater level of critical data.

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

Engineers Australia supports the Department's proposed all-hazards power of last resort, should there be no existing power available to support a fast and effective response during significant incidents. The proposed scope of direction power is reasonable and should be an effective way to enhance consequence management.

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

Engineers Australia supports the Department's proposed revision of the 'protected information' definition, the adoption of a new harms-based approach, and the clarification of disclosure provisions for the purposes relevant to continued operation of or mitigation of risk to an asset. Engineers Australia understands that this shift aims to eliminate any potential confusion in interpretations, fostering a clear and consistent understanding and application of the protected information framework.

However, consideration should also be given to information sharing of 'near misses' by critical infrastructure entities. It is not clear whether the Department's proposed 'voluntary disclosures' would include near misses. This addition could elevate our comprehension of existing vulnerabilities that cyber-criminals might have overlooked. It would be essential, however, to strike a balance to ensure that such sharing maintains boundaries between information shared for transparency and that which must remain protected to prevent or mitigate harm.

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

Engineers Australia endorses the Department's proposed introduction of a formal, written directions power in Part 2A of the SOCI Act to address seriously deficient elements of a Critical Infrastructure Risk Management Program (CIRMP) under the circumstances proposed in the consultation paper.

Consideration should also be given to penetration test programs which could be enforced on critical infrastructure entities under critical infrastructure risk management obligations. This preventive measure would be both an educative and enforcement mechanism, testing critical infrastructure entities' IT and OT systems by bug bounty hunters seeking any vulnerabilities that could be exploited by cyber-criminals. Any findings would be then shared by the Government to the respective entities with clear directions to fix any deficiencies.

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

Engineers Australia agrees with the Department's proposed consolidation of the security regulation for the telecommunications sector and the introduction of a co-designed Telecommunications Security and Risk Management Program (TSRMP) under the SOCI Act.

The implementation of a TSRMP framework should drive all telecommunications companies, including low-cost telecommunications carriers, to incorporate additional safeguards and contingency plans, ensuring secure fallback options in the event of an incident. This should include recognition of the significance of quarantine updates and rollback capabilities.