Australian Government
Department of Home Affairs

Department of Home Affairs submission to the Review of the Cyber Security Legislative Package

Parliamentary Joint Committee on Intelligence and Security

25 October 2024

Table of Contents

Introduction

1. The Department of Home Affairs (the Department) welcomes the opportunity to make a submission to the Parliamentary Joint Committee on Intelligence and Security's (PJCIS) review of the Cyber Security Legislative Package. This Package comprises the Cyber Security Bill 2024, the Intelligence Services and Other Legislation Amendment (Cyber Security) Bill 2024 (ISA Bill), the Security of Critical Infrastructure and Other Legislation Amendment (Enhanced Response and Prevention) Bill 2024 (ERP Bill) and associated explanatory memoranda for the three Bills.

2. This submission provides an overview of the Package, including the extensive consultation and engagement undertaken by the Department to inform the development of the Bills. This submission outlines the purpose of the measures in the Package, and how they have been shaped in line with stakeholder feedback.

Public-private partnerships

3. The Department works collaboratively with all levels of government and industry to jointly uplift critical infrastructure security and resilience through engagement, information sharing, exercises, guidance and co-design of policy. As a regulatory authority, the Department also takes a partnership approach through compliance and enforcement seeking to prioritise security outcomes in the national interest.

4. Following previous reforms to the *Security of Critical Infrastructure Act 2018* (SOCI Act), through the *Security Legislation Amendment (Critical Infrastructure) Act 2021* (SLACI Act) and the *Security Legislation Amendment (Critical Infrastructure Protection) Act 2022* (SLACIP Act), the Department has partnered with the critical infrastructure community to ensure it achieves the intended regulatory outcomes for both Government and industry.

5. In February 2023, the former Minister for Home Affairs, the Hon Clare O'Neil MP, released the Critical Infrastructure Resilience (CIR) Strategy and Plan. The CIR Strategy and Plan outlines regulatory and non-regulatory initiatives to uplift the security and resilience of Australia's critical infrastructure.

6. The Australian Government's primary platform for partnering with the Australian critical infrastructure community is the Trusted Information Sharing Network (TISN). As at October 2024, the TISN is comprised of over 2,000 members from industry and all levels of government. Members of the TISN collaborate to identify and manage risks to critical infrastructure, address security gaps within sectors and implement mitigation strategies and inform future policy and programs to further support critical infrastructure resilience. The Department hosts online webinars, site visits, web forums and in-person workshops and roundtables with TISN members, including cross-sector meetings, to facilitate discussions and collaboration on:

   - understanding and management of risks to critical infrastructure,
   - increasing awareness and understanding of the flow-on impacts of disruptions to any critical infrastructure sector,
   - enhancing communication channels and networks between industry and all levels of government,
   - identifying gaps and implementing appropriate strategies to reduce risk within each sector,
   - informing future policies and programs to support critical infrastructure resilience.

7. The Critical Infrastructure Advisory Council (CIAC) is a joint government and industry advisory body that meets three times a year. It supports collaboration and provides leadership and strategic direction for the TISN.

8. The TISN is also supported by the Resilience Expert Advisory Group (REAG). The REAG is an expert advisory body which promotes organisational resilience in support of Australian critical infrastructure owners and operations. REAG does so by providing strategic advice, guidance and tools to mature security and resilience approaches. For example, in March 2024, over 70 TISN members, state and territory representatives and Government stakeholders participated in an activity day facilitated by the REAG. The activities were aimed at information-sharing and building awareness of interdependencies across sectors as well as event scenario discussions. The REAG also released a refreshed Organisational Resilience HealthCheck Tool and Good Practice Guide.

9. In addition to the TISN, the Department engages with industry through town halls, webinars, podcasts, exercises, workshops and conferences. In 2024, the Department has hosted the Critical Infrastructure Security Excellence Workshops in each capital city in Australia, which has included presentations from industry and government representatives on the latest information and practical advice relating to the protection of Australia's critical infrastructure through panel discussions and collaborative activities.

10. To assist critical infrastructure owners and operators to meet their obligations, Department has also released a range of guidance material, risk advisories and toolkits. This has included comprehensive guidance on a number of SOCI Act obligations, an Overview of Cyber Security Obligations for Corporate Leaders and the inaugural Critical Infrastructure Annual Risk Review.

11. The Department has been undertaking regular reporting to the PJCIS, as required by section 60AAA of the SOCI Act. Section 60AAA was inserted at the recommendation of the PJCIS, and requires the Department to provide reports on conduct, progress and outcomes of consultation relating to the SLACI Act and SLACIP Act to the Minister for Home Affairs, for provision to the PJCIS. As consultation on the SLACI Act and SLACIP Act is now completed, the Department welcomes PJCIS consideration of the utility and value of this ongoing reporting requirement.

12. Equally, the Department seeks the PJCIS' views on the utility of the review requirements under sections 60A and 60B of the SOCI Act.

Co-design process for the Cyber Security Legislative Reforms

13. In April 2023, the Minister for Cyber Security's Expert Advisory Board released the 2023 – 2030 Australian Cyber Security Strategy Discussion Paper (Discussion Paper). The Discussion Paper identified opportunities to enhance and harmonise regulatory frameworks including both consideration of a new Cyber Security Act and potential amendments to the SOCI Act. The Department received over 150 public submissions in response to the Discussion Paper, with most stakeholders noting support for new regulation, where necessary, to rectify gaps in current cyber security legislative frameworks.

14. In May 2023, the Government established the Australian Telecommunications Security Reference Group (ATSRG), as recommended by the PJCIS in its review of the Telecommunications Sector Security Reforms (TSSR), also known as the *Telecommunications and Other Legislation Amendment Act 2017*. The ATSRG is chaired by the Department of Infrastructure, Transport, Regional Development, Communications and the Arts, in close collaboration with the Department of Home Affairs. It is attended by representatives from

telecommunications industry including major carriers, industry groups and consumer representative groups.

15. The ATSRG has met 14 times since its establishment. The first phase of the ATSRG established a preference amongst industry partners to consolidate security regulation under the SOCI Act. The ATSRG has co-designed the detail of legislative amendments to the SOCI Act to integrate telecommunications security regulation and the details of subordinate legislation.
16. On 22 November 2023, the Government launched the *2023-2030 Australian Cyber Security Strategy* (the Strategy) setting out Australia's vision to become a world leader in cyber security by 2030. The Strategy outlined the Government's commitment to co-design legislative reform with industry, reflecting feedback received to the Discussion Paper that a comprehensive, clear legislative framework was needed. In addition to legislative change, the Strategy outlines a number of other initiatives designed to enhance our existing program of engagement with industry, including the development of incident response playbooks and the national cyber exercise program.
17. On 19 December 2023, the Department of Home Affairs released the *2023–2030 Australian Cyber Security Strategy: Legislative Reforms Consultation Paper* (the Consultation Paper) outlining two areas of proposed legislative reform: new legislated initiatives to address gaps in existing regulatory frameworks, and amendments to the SOCI Act to strengthen protection of Australia's critical infrastructure.
18. The Department received over 130 submissions in response to the Consultation Paper. The majority of submissions expressed support in principle for all measures with specific feedback focusing on ensuring appropriate scope and guardrails for powers, and that clear guidance is provided during implementation. During the consultation period, the Department held over 50 public town hall and deep dive sessions, over 30 roundtables with peak bodies and industry groups, engaged with industry through the TISN and provided written clarification to interested parties on the proposed reforms as needed.
19. The co-design process between industry and government provided valuable feedback to inform the design of the Cyber Security Bill and amendments to the SOCI Act. All public submissions from the consultation process are available on the Department's website.
20. In September 2024, the Department undertook targeted consultation on an Exposure Draft Package with industry and government stakeholders. Targeted stakeholders included peak bodies, TISN, State and Territory Governments, and others who engaged in the consultation process. To support consultation on the Exposure Draft Package, the Department hosted two town hall sessions attracting over 200 industry and government attendees each.
21. The Department received 61 confidential submissions in response to the Exposure Draft Package. Submissions highlighted continued support for the measures in the Bills. Many stakeholders welcomed how previous feedback had been addressed. Minor changes were reflected in the Bills and explanatory memoranda in line with stakeholder feedback.
22. Noting the targeted consultation on the Exposure Draft Package, the Department welcomes the PJCIS review as an opportunity for further public consultation and parliamentary scrutiny.

Cyber Security Bill

23. The Cyber Security Bill 2024 seeks to provide additional protections to Australian individuals and businesses, build mitigations for extant cyber risks and improve the Government's visibility of the threat environment to inform protections, incident response procedures and future policy.

24. The Bill proposes the following measures:

- Establishing the power for the Minister for Cyber Security to make mandatory security standards for smart devices, also known as Internet of Things (IoT) devices;
- Introducing a mandatory reporting obligation for entities who are affected by a cyber incident, receive a ransomware demand, then elect to make a payment or give in kind benefits in connection with the cyber security incident;
- Establishing a 'limited use' obligation that restricts how certain cyber security incident information provided to the National Cyber Security Coordinator (the Coordinator) during a cyber incident can be used and shared with other government agencies, including regulators. This measure complements the Intelligence Services and Other Legislation Amendment (Cyber Security) Bill 2024 which introduces a similar limited use obligation on the Australian Signals Directorate (ASD);
- Establishing a Cyber Incident Review Board (the Board) to conduct post-incident reviews into significant cyber security incidents and provide recommendations to industry and government.

25. To give effect to Parts 2, 3 and 5, it is also intended that new subordinate legislation will be developed. The Department intends to undertake formal consultation on draft subordinate legislation after passage of the Bills. The details of the intended operation of the subordinate legislation are outlined at **Attachment A1**.

Part 2 – Security standards for smart devices

The issue to be resolved

26. To date, Australia's voluntary approach to smart device security has been fragmented and insufficient. In 2020, the Government introduced a voluntary Code of Practice, 'Securing the Internet of Things for Consumers', which set out guidance for smart device manufacturers and suppliers aligned to an existing European standard: the European Telecommunications Standards Institute standard applicable to consumer grade devices (ETSI EN 303 645). In 2021, a government study of manufacturers' uptake of the voluntary Code of Practice revealed low levels of adoption across the country. Since then, smart devices have become cheaper and more widely accessible due to advances in technology. During public consultation on the development of the Bill, there was consensus among government, industry, and consumers, that a mandatory approach was required to uplift the cyber security of smart devices in Australia.

27. Smart devices may include technologies such as smart TVs, smart watches, home assistants and baby monitors, which have become ubiquitous in Australian homes and businesses, and increasingly prevalent in Australia for everyday transactions, communication, work and leisure. Industry research forecasts show an average of 33.8 connected smart devices per household in Australia by 2025.

28. Smart devices collect significant volumes of potentially sensitive data about users, sometimes both with and without the express knowledge and awareness of consumers. As smart devices become more accessible to consumers, due to lower cost and greater availability, government, industry and consumers alike are supportive of a mandatory approach to uplift the cyber security of smart devices in Australia.

Stakeholder feedback

29. The majority of stakeholders supported introducing mandatory security standards for smart devices, placing responsibility for compliance with the standard on manufacturers and suppliers. Vendors, distributors, and importers were also suggested as responsible entities, while some stakeholders suggested that all entities in the supply chain should be held responsible (including retailers).

30. Most stakeholders supported mandating the first three principles of the ETSI EN 303 645 standard as a baseline in Australia, given it is a widely supported and accepted global standard. Some stakeholders suggested a higher standard be mandated in Australia such as the first six principles or the whole ETSI standard. Alternatively, a phased implementation of the whole ETSI standard could be considered. Some stakeholders suggested that higher-risk products should adhere to a higher standard.

31. Most stakeholders agreed that the scope of the standard should apply to all IoT devices (internet and network-connected devices) in Australia, subject to exceptions. Feedback included that the definition of the scope of products should be flexible enough to apply to emerging technologies. There was mixed feedback about the inclusion of smart phones, as some stakeholders suggested they should be included, while others noted they are already built to high security standards.

32. Most stakeholders agreed a 12 month implementation timeframe would be sufficient for responsible entities to comply with a new standard. This is consistent with the United Kingdom's (UK) approach.

Our approach

33. Reflecting industry feedback, and aligning with international best practice, the Cyber Security Bill proposes introducing a rule making power for the Minister for Cyber Security to prescribe specific security standards for specified classes of relevant connectable products. All rules will undergo a mandatory 28-day consultation period to ensure further stakeholder feedback can be obtained from affected entities

34. The rule-making power provides the Minister the flexibility to respond to the fast-paced and continually evolving nature of smart devices and their underlying technology. Rules under this Part are intended to align with legislative approaches such as the UK's *Product Security and Telecommunications Infrastructure Act 2022*, modelled off international standards, such as the ETSI EN 303 645 standard. It should be noted international standards are not static and can be updated based on new technical advice, industry and consumer expectations, and advances in technology.

35. The rules will include the scope of smart devices to be covered or exempt under a given standard, the timeframe for implementation and any additional requirements, for example, details required in a statement of compliance to demonstrate an adherence to the standard.

36. The standards will apply to manufacturers (an entity that manufactures a relevant connectable product) and suppliers (an entity that supplies a relevant connectable product) if the entity is aware that the product could be manufactured or supplied in Australia.

37. The regulatory framework sets out a series of enforcement notices, designed to encourage engagement with manufacturers and suppliers of smart devices to the Australian market and uplift industry best practice. A range of penalties were considered in the development of this enforcement framework. Civil penalties have been excluded as they have limited effect on changing behaviours and business decisions of manufacturers and suppliers of smart devices in the Australian market. Recall notices and potential reputational damage are a sufficient enforcement lever for government to ensure that manufacturers and suppliers of smart devices will comply with security standards due to the risk of losing market access in Australia. This could also act as a signal to international markets with similar cyber security standards and frameworks, including the UK and the European Union, that the recalled smart devices may also not meet requirements in those jurisdictions.

38. The established regulatory framework will enable Government to collaborate with industry, raise awareness, and encourage continuous improvement. Given standards introduced under this Part of the Bill will likely emulate international best practice and existing requirements in other jurisdictions, responsible entities found to be non-compliant in Australia may also not be compliant overseas and could be penalised through those regulatory frameworks. It is expected that manufacturers and suppliers will not risk further reputational damage and potential regulatory consequences in Australia.

First proposed standard to be introduced

39. The first standard intended to be introduced under Ministerial rules would uplift the cyber security of consumer-grade smart devices (with some device exceptions) by aligning with existing international approaches. This approach would ensure Australia remains in-step with the international market, minimising regulatory burden for industry and ensuring Australian consumers can trust their digital goods and services. The initial standard for consumer grade devices takes inspiration from the ETSI EN 303 645 standard and the UK's *Product Security and Telecommunications Infrastructure (Security Requirements for Relevant Connectable Products) Regulations 2023* under the *Product Safety and Telecommunications Act 2022*.

40. The scope of smart devices covered by this standard is proposed to include devices that meet the definition of a relevant connectable product, defined in the Bill, and will be purchased by a consumer, defined by section 3 of Australian Consumer Law. A draft of the standard would be released through rules for public consultation following passage of the Bill. The standard is proposed to include:

    - No universal default passwords – where passwords are used in any other state other than factory default, all consumer IoT device passwords need to be unique per device or defined by the user.
    - Implement a means to manage reports of vulnerabilities – allowing security researchers and others to report issues, with status updates on the resolution of these issues.
    - Provide information about how long the device would be supported for – manufacturers and suppliers would be required to provide transparency to consumers about the minimum timeframe that the product will receive security updates.

41. Under this obligation, the expectation is that these standards would be applied by default to the manufacturer of smart devices that consumers use every day, such as smart TVs, smart watches, home assistants, baby monitors and consumer energy resources like certain solar panels. This would subsequently increase the baseline security of these devices and reduce their vulnerability to exploitation or attack.

Exclusions to the standard

42. The proposed format of rules would take an exclusion-based approach for the coverage of devices for each specified security standard. Generally, devices will be excluded if: there is existing legislation that can adequately address the cyber security of these devices, there is work underway across Government to develop a higher or bespoke standard for these devices, or the complexity of these devices means that being mandated under these rules will risk a lower standard being met. The list of excluded devices for each standard can be amended to exclude further devices, or scope devices back under the coverage of the standard.

43. For the consumer-grade smart device standard, devices meeting the defined scope are included, unless they are deliberately scoped out. Exempted products may include, for example, medical devices.

Part 3 – Ransomware payment reports

The issue to be resolved

44. Ransomware incidents pose some of the most significant cybercrime threats to Australian organisations, businesses and the community. Ransomware remained the most destructive cybercrime threat in 2022-23. The impact on small business is disproportionate, noting 60% of small businesses shut down within six months of being subject to a ransomware attack.[1]

45. The Australian Institute of Criminology (AIC) reports that only 19% of members of the public sought help, advice or support from the police or the ASD following a ransomware attack.[2] According to BlackFog, 15% of cyber incidents were reported globally in 2023.[3] In the same year, McGrath Nicol surveyed 500 Australian businesses with 50% of businesses with more than 50 employees noting it should be mandatory to report ransomware attacks to authorities, and 32% noting reporting should be restricted to when a payment is made.[4]

46. Currently, there is no economy wide existing obligation for entities to report ransomware or cyber extortion payments. This lack of timely reporting limits the government's ability to understand the scope of this issue, support victims, and disrupt ransomware and cyber extortion actors. To enhance our national threat picture and better inform government responses, the Government requires clear threat intelligence through up-to-date data.

---

[1] Cyfirma, Tracking Ransomware February 2024, Cyfirma, 8 March 2024 < https://www.cyfirma.com/research/tracking-ransomware-february-2024/>
[2] Isabella Voce and Anthony Morgan, Help-seeking among Australian ransomware victims, Statistical Bulletin no. 38, Australian Institute of Criminology, Canberra, 3 March 2022, pg. 12 <https://doi.org/10.52922/sb78504>.
[3] Brenda Robb, The State of Ransomware 2024, BlackFog, 1 August 2024 <https://www.blackfog.com/the-state-of-ransomware-2024/>.
[4] McGrathNicol Ransomware Report 2023, p 16.

Stakeholder feedback

47. Stakeholder feedback demonstrated support for the policy position of introducing a mandatory reporting obligation in the event of a ransomware or cyber extortion payment. Stakeholders advocated for a reporting obligation that is proportionate and reasonable, and where information provided would be used to produce guidance and support for those impacted by ransomware attacks. Stakeholders did not support the proposal to introduce two reporting obligations; one in the event of a demand following an incident, and another in the event the payment was made.

48. The majority of submissions indicated support for a threshold below the $10 million in annual turnover proposed in the consultation paper. A significant number of submissions in response to the Consultation Paper suggested alignment with the current *Privacy Act 1988* (Privacy Act) $3 million threshold. Some submissions suggested all businesses should be captured by the obligation, or suggested reporting requirements should be based on sector, turnover and sensitivity of information they hold. Several stakeholders raised concerns over the burden of reporting requirements on small business. During Exposure Draft consultation, some industry respondents still had concerns over the $3 million threshold. The Government will consult further on the rules when they come into force but will commence with the policy proposition to align with the $3 million threshold in the Privacy Act.

49. Feedback also supported keeping information contained in a report to a minimum, focusing on threat vectors, attackers, persistent vulnerabilities and other information that can be used to mitigate risks and build resilience across sectors. Submissions overwhelmingly supported the purpose of the reporting obligation to expand the Government's understanding of the ransomware threat picture in order to produce timely and actionable guidance to support industry in responding to ransomware threats. The Government should not seek to find fault or re-victimise businesses subject to ransomware attack.

Our approach

50. Reflecting feedback received, the proposed reporting obligation will only apply to captured businesses who elect to make a ransom payment, or provide an in-kind benefit, in response to a demand following a cyber incident. Captured businesses will be defined by turnover threshold as specified in rules made by the Minister administering the Act. The Department proposes capturing all businesses operating within Australia with an annual turnover of $3 million or more, and all responsible entities for critical infrastructure assets captured under Part 2B of the SOCI Act. Specifying the threshold in rules allows for flexibility to maintain currency through the evolving cyber threat landscape. All rules will undergo a mandatory 28-day consultation period to ensure further stakeholder feedback can be obtained from affected entities.

51. Reflecting stakeholder concerns over regulatory burden, the reporting obligation will not be onerous, requiring only basic information to acquit the obligation. Reporting will not abrogate legal professional privilege, nor will the information be admissible in most legal proceedings (a few specific exceptions are listed in section 32 of the Bill). Information provided will not be shared within government except in limited circumstances as outlined within the Bill. These protections are intended to provide assurance to entities that reporting will not result in further regulatory action. However, the Government is not providing a 'safe harbour'. This obligation will not interfere with any existing laws, or the powers of regulators or law enforcement agencies to gather information in accordance with their legislated functions.

52. Civil penalties of up to 60 penalty units apply where an entity does not make a mandatory ransomware payment report in accordance with their obligations. This penalty is proportionate to incentivise compliance while reflecting industry feedback that penalties should not further victimise a business subject to a ransomware attack. The Department will establish compliance procedures involving engagements and warnings favouring education first approach before electing to pursue civil penalties.

Part 4 – Coordination of significant cyber security incidents

The issue to be resolved

53. The National Cyber Security Coordinator (the Coordinator), and the Australian Signals Directorate (ASD), play a pivotal role in responding to cyber security incidents. Timely and fulsome engagement between industry, the Coordinator and the ASD is essential to ensuring that the negative impacts of cyber security incidents can be mitigated, managed and responded to as soon as possible. Early engagement, especially when there are vital insights, and the sharing of indicators of compromise or early unformed views are vital to an effective and collaborative response.

54. ASD has observed that cyber security incident reporting and engagement by industry has plateaued, despite cyber activity increasing in frequency, scale and sophistication in recent years. This suggests an overall reduction in timely reporting and engagement between industry and Government.

55. Impacted entities requiring support provide information to the National Office of Cyber Security (NOCS) about incidents and response activities on a voluntary basis. In doing so, impacted entities are required to carefully risk manage their considerations of the timing, nature, and extent of information they provide to the Department.

56. There have been some circumstances where cyber security incident response and recovery has been treated as a legal issue, with some entities routinely bringing legal counsel to engage with the Government directly, out of fear that any information they provide may be provided to regulators, to be used against them in future regulatory and law enforcement proceedings. A lack of timely information limits how the Government can respond to and help mitigate a cyber security incident, potentially leading to more severe consequences causing further harm to impacted entities. As such, it is essential that barriers to the timely and fulsome provision of information are removed.

Stakeholder feedback

57. Throughout consultation, consistent support has been provided for the policy position that an obligation be placed on the Coordinator and ASD limiting how information provided voluntarily during a cyber incident is shared and used. An overwhelming majority of submissions to the Consultation Paper supported narrow permitted cyber security purposes for the sharing of information provided, and raised concerns with information being shared with law enforcement agencies even if not for regulatory purposes. Some respondents disagreed with the proposed limited use model, or wanted a ‘safe harbour’ which is not the position the Government has adopted.

58. Submissions noted the Government would need to build trust with industry through partnerships, engagement and regular advice that draws on anonymised reporting. Submissions also noted that information captured by the limited use obligation should be

exempt from the *Freedom of Information Act 1982* (FOI Act). Industry submissions also queried the application of legal professional privilege and if those protections would still apply to information captured by limited use.

Our approach

59. A limited use obligation has been set out for both the Coordinator and ASD, although each is dealt with by a different Bill. In both cases, information received voluntarily by the Coordinator may only be on-shared for permitted cyber security purposes. This narrow set of purposes ensures cyber security incident information may only be shared where necessary to ensure appropriate information sharing can take place to respond to, mitigate or resolve the cyber security incident, or to inform appropriate coordination efforts. Government departments and agencies play a significant role in cyber incident response, both in efforts to respond to and mitigate the ongoing consequences of a cyber security incident. The permitted purposes have been narrowly crafted to ensure the limited use obligation does not have an adverse impact on the ability of the Government to adequately respond to cyber threats, while providing assurances to industry that their information will not be used against them in legal proceedings.
60. Information provided under limited use and shared for a permitted purpose will be inadmissible in the vast majority of civil or criminal proceedings. However, this does not provide a 'safe harbour' and will not restrict operational, regulatory or law enforcement agencies from using their existing powers to obtain information directly from the impacted entity and carrying out their legislated functions.
61. The limited use obligation does not abrogate the protections of legal professional privilege and, in line with industry feedback, information captured by the limited use obligation will be exempt from requests under the FOI Act. Amendments to the FOI Act have been proposed as part of the Intelligence Services and Other Legislation Amendment (Cyber Security) Bill 2024.
62. To support the limited use provision, the Department would develop processes and procedures to ensure the effective implementation of the obligation. These policies and procedures would ensure that the Coordinator and the NOCS appropriately handle and share information provided under the limited use provision.

Part 5 – Cyber Incident Review Board

The issue to be resolved

63. Recent high-profile and high-impact cyber security incidents, such as the Optus and Medibank data breaches in 2022, and the MediSecure data breach in 2024 highlight that Government and industry need to do more to effectively learn lessons from cyber security incidents and prepare contingencies for future attacks.
64. While the United States has a dedicated Cyber Safety Review Board to review significant cyber security incidents and provide public findings, there is currently no such standing mechanism in Australia. In order to enhance our collective cyber resilience, respond better to significant cyber incidents and learn the lessons, we need a mechanism that is responsible for undertaking a review of the vulnerabilities that led to the incident, and provide guidance to support better industry practice and government response. This is particularly important for driving constant improvement and informing policy development, within both the public and private sectors, as cyber-enabled interference grows.

Stakeholder feedback

65. Feedback on the proposed Cyber Incident Review Board (the Board) model highlighted that the Board's remit should focus only on significant cyber security incidents, and on providing lessons learned for both Government and industry. Stakeholders supported clear limitations on what types of incidents should be subject to a review, which could include incidents with severe public impacts, incidents that use innovative methods or those with broad implications for Government and industry.
66. Feedback was supportive of the Board being comprised of several standing members, supported by a pool of industry and other external subject matter experts. Feedback emphasised the need for transparent appointments and diversity, including representation from the public and private sectors, academia and civil society with expertise in cyber security, incident management, digital forensics and key industry sectors and law. Many respondents supported an independent Chair appointed by the Government, while some proposed another Government official, such as the Coordinator.
67. A significant number of stakeholders supported the Board initiating reviews itself or making a decision to review based on referral from the Government, while others suggested the Minister for Cyber Security or the Coordinator should initiate reviews.
68. The majority of submissions expressed support for the Board possessing modest information-gathering powers, with voluntarily approaches being the preference first. Some submissions cited the Australian Transport Safety Bureau and the Board having a similar set of powers. A small number of submissions opposed the Board having any compulsive powers.
69. Submissions emphasised the 'no-fault' principle of the Board, with some expressing concerns about the Board's ability to deliver findings that do not imply fault or prejudice other legal proceedings.

Our approach

70. The Cyber Security Bill proposes the Board be established as a national mechanism to review cyber security incidents and disseminate clear and concrete recommendations to both Government and industry to strengthen Australia's collective cyber resilience. When referred by the Minister for Cyber Security, Coordinator, the Board or an affected entity, the Board will commence a review of a cyber security incident that meets the criteria as set out in the Bill
71. Each review must be conducted by a panel consisting of the Chair, standing members of the Board and select members of an Expert Panel comprised of subject matter experts from industry, academia and civil society that may be called upon on a part time basis to participate in reviews. The Board will be comprised of government officials with a broad range of skillsets, ranging from cyber security to incident management, digital forensics and sectoral knowledge and law.
72. Information gathering powers are available to the Chair where voluntary requests for information have proven ineffective. Legal professional privilege will not be abrogated through the provision of information to the Board, and compensation is available to an entity for costs incurred in compliance with the requirement to provide information.
73. To provide further clarity to industry, the Bill's explanatory memorandum explains that information provided to the Board is inadmissible in the vast majority of civil and criminal proceedings, that information can only be used and disclosed for limited purposes, the Board is

unable to apportion blame and that it is the intention for the Board to cooperate with State and Territory government bodies.

74. To support implementation of the Board framework, the rules (to be made by the Minister for Cyber Security) will establish the governance parameters through which the Board will perform its functions. Establishing the governance and administrative procedures within the rules will ensure operational transparency while allowing change without legislative amendment. The subordinate legislation will provide flexibility to the Board to ensure it can respond effectively to changes that come about as procedures are simplified, as technology evolves and in response to the evolving cyber threat landscape.

Security of Critical Infrastructure and Other Legislation Amendment (Enhanced Response and Prevention) Bill

75. Australians rely on our critical infrastructure ecosystem to provide essential goods and services to sustain our way of life and underpin Australia's national security, defence, and socioeconomic stability. Australia currently faces heightened geopolitical and cyber threats, which means that our critical infrastructure is increasingly at risk from malicious state actors and criminals.

76. Reviews into recent incidents impacting critical infrastructure have identified gaps in the SOCI Act that limit our ability to prepare, prevent and respond to cyber incidents. The Strategy has found opportunities to clarify, enhance and strengthen obligations of critical infrastructure sectors under the SOCI Act to achieve greater security posture and agile, industry-led response to incidents with support from Government.

77. The ERP Bill amends the SOCI Act to give effect to initiatives under 'Shield 4' of the Strategy of 'protected critical infrastructure', and to the PJCIS Review into the TSSR.

    To achieve this, amendments to the ERP Bill include six schedules:

    1. Clarifying that certain data storage systems that store business critical data are part of a critical infrastructure asset and must be protected under the SOCI Act,
    2. Improving our national response to the consequences of significant incidents through enhancement of the government assistance powers,
    3. Simplifying how government and industry share information, including in crisis situations, through amending the protected information provisions,
    4. Enforcing critical infrastructure risk management obligations through the introduction of a remedy power,
    5. Consolidating and aligning telecommunications security requirements from the *Telecommunications Act 1997* (Telecommunications Act) under the SOCI Act, and
    6. Simplifying reporting obligations in regards to the declaration of systems of national significance (SoNS).

78. To give effect to schedules 1 and 5, it is also anticipated that new subordinate legislation and changes to existing subordinate legislation will be required. The Department intends to undertake formal consultation on draft subordinate legislation after passage of the Bills. The details of the intended operation of the subordinate legislation are outlined at **Attachment A1**.

Schedule 1 – Data storage systems that hold business critical data

The issue to be resolved

79. Critical infrastructure entities are a natural target for cyber attacks given their size, function and value. Over the last two years, Australia has seen a growing number of cyber security incidents impacting non-operational data storage systems held by critical infrastructure entities. Recent cyber security incidents that did not directly impact the essential functions of critical infrastructure, have demonstrated the risk to the non-operational systems that hold large quantities of data. This includes both personal information and other 'business critical data'.

80. The SOCI Act currently imposes positive security obligations on data storage and processing assets, where this is the primary function of the critical infrastructure asset. However, these obligations do not extend to the adequate protection of secondary systems related to other classes of critical infrastructure assets that hold 'business critical data'. This data may include research or operational data, such as network blueprints, encryption keys or algorithms that can be exploited or used as a point of entry by malicious actors to cause harm to a critical infrastructure asset.

81. The purpose of the amendments contained within this Bill is to strengthen and standardise obligations across critical infrastructure assets by explicitly outlining that certain data storage systems that hold business critical data do form part of a critical infrastructure asset, regardless of the asset's primary function.

Stakeholder feedback

82. The majority of stakeholders supported consistent standards between in-house and third party data storage and processing systems. Feedback focused on the need to clarify who is responsible for in-house vs third party systems. Feedback also highlighted need for guidance especially concerning the scope of business critical data, what systems are covered and who is responsible for these systems.

83. Feedback also emphasised the need to ensure this measure is complementary to the Privacy Act, and does not impose undue regulatory burden.

84. While many stakeholders indicated they are already considering risks to these systems and viewed this measure as a clarification, some stakeholders requested a grace period to allow time for implementation.

Our approach

85. Schedule 1 clarifies existing obligations under the SOCI Act for critical infrastructure owners and operators to protect data storage systems and business critical data where vulnerabilities, impacts or access to these systems could have a relevant impact on the availability, integrity, confidentiality or reliability of a critical infrastructure asset. The amendments will apply to these systems if they are used (or will be used) in connection with a main critical infrastructure asset. This ensures that these amendments are complementary to, and do not duplicate, regulatory impact under the Privacy Act.

86. The Bill clarifies that the amendments only apply if the responsible entity for the critical infrastructure asset owns or operates the data storage system. This further clarifies that Schedule 1 does not apply to third party data storage providers (captured under the data storage and processing sector in the SOCI Act).

87. Threats to these systems and data are also intended to be clarified as 'material risks' through subordinate legislation made under Part 2A (as detailed in **Attachment A1**).

88. The Department will provide further guidance material for regulated entities and continue ongoing education and engagement to assist entities to determine what systems are captured by these amendments. The Department will also work closely with the Attorney-General's Department and regulators to ensure guidance material reflects how these amendments interact with Schedule 5 and other regulatory regimes, including the Privacy Act and the Australian Prudential Regulation Authority's Prudential Standards.

89. The Department intends to provide a grace period by commencing the provisions by proclamation six months after Royal Assent, and through subordinate legislation.

Schedule 2 – Managing consequences of impacts of incidents on critical infrastructure assets

The issue to be resolved

90. The existing 'government assistance powers' under Part 3A of the SOCI Act are mechanisms to assist with an immediate response to serious cyber security incidents impacting a critical infrastructure asset that pose a material risk to Australia's national interests. The use of current Part 3A powers is limited to responding to a cyber security incident and resolving the technical factors of that incident. This does not extend to other significant incidents impacting critical infrastructure without a cyber-related cause or the cascading consequences of an incident. They include powers for the Minister for Home Affairs to authorise the Secretary for Home Affairs to give:

    a. information gathering directions;

    b. action directions; and

    c. following approval from the Prime Minister and Minister for Defence, intervention requests.

91. As the threat environment evolves, our critical infrastructure protection needs to account for the increasing risk of non-cyber threats, including climate related disasters, physical or personnel security threats and the potential flow on consequences of increasingly interconnected and interdependent critical infrastructure sectors. Our approach to protecting critical infrastructure in this environment will need to be agile to allow for swift action in crisis situations, facilitate effective collaboration between government and industry, and apply an all-hazards framework.

Stakeholder feedback

92. Feedback focused on the need to ensure the powers are a last resort, appropriately confined in their scope and purpose, and subject to robust safeguards, oversight mechanisms and have clear liability and indemnity provisions. Stakeholders also commented on the need for clear guidance on thresholds and parameters, processes for incident management, coordination and response, including coordination with state and territory jurisdictions.

Our approach

93. Schedule 2 amends Part 3A to enhance existing government assistance powers to capture all-hazards and allow for the Minister for Home Affairs to authorise the Secretary of Home Affairs

to issue action and information gathering directions to address the impacts of an incident on critical infrastructure, beyond the existing confines of resolving a technical cyber incident.

94. Requirements for intervention requests remain unchanged and can only be used in the event of a cyber incident. This includes the required approval for the Minister for Home Affairs, Minister for Defence and the Prime Minister given the significance of such an action. Some public commentary has suggested that there has been suggested amendments to the intervention power and it is therefore important to emphasise that there is no change proposed to this power. None of the 'government assistance powers' have been used since the Parliament passed the legislation in 2022 demonstrating that they are truly a last resort powers to be used in extremis.
95. This approach reflects stakeholder feedback by ensuring the existing Part 3A framework applies to limit the scope and purpose of the powers, provide safeguards, oversight mechanisms and indemnity and liability provisions. For example, information gathering and action directions can only be used where there is an impact on the availability, integrity, reliability or confidentiality of a critical infrastructure asset, and where there is a material risk of serious prejudice to Australia's social or economic stability, defence or national security. The powers will remain last resort as they cannot be used unless the Minister is satisfied that no existing regulatory system of a state, territory or the Commonwealth could provide a practical and effective response, and the entity is unwilling or unable to take all reasonable steps to respond to the incident.
96. In addition to existing safeguards in the SOCI Act, where an action direction requires the disclosure of personal information, as defined under the Privacy Act, the Minister administering the Privacy Act must agree.
97. The Department is preparing policies and procedures to guide how these powers will be used in practice, consistent with the principles outlined in the Australian Government Crisis Management Framework (AGCMF). The AGCMF recognises that states and territories are the first responders to incidents that occur within their jurisdictions. Lead Ministers, Australian Government Coordinating Agencies and Lead Coordinating Senior Officials are assigned to manage crises in accordance with the principles outlined in the AGCMF. This ensures a coordinated whole-of-government response, including collaboration with states and territories.
98. For cyber incidents, the National Cyber Security Coordinator and NOCS will continue to coordinate these responses. The Coordinator and the NOCS are not regulators and do not have regulatory compliance functions. However, they can engage with relevant regulators in the context of a cyber incident to understand the impacts of cyber incidents and connect impacted entities with regulators to support the response. The Department will rely on the Coordinator's understanding of the nature and extent of a cyber incident and its impacts, along with other sources of information, to determine whether the thresholds for use of the Part 3A powers have been met, including whether alternative mechanisms would provide an effective response. The relevant lead for non-cyber incidents would be determined according to the AGCMF.
99. The Department remains committed to providing transparency and accountability to the Parliament and public on the operation of the SOCI Act. A copy of Ministerial authorisations given under Part 3A must be provided to the Inspector-General of Intelligence and Security within 48 hours after the authorisation is given. Additionally, under section 60 of the SOCI Act, the Secretary must give the Minister, for presentation to the Parliament, a report on the

operation of the SOCI Act for each financial year including any authorisations given under Part 3A.

Schedule 3 – Use and disclosure of protected information

The issue to be resolved

100. The protection and disclosure of information relating to the operation, structure, and location of critical infrastructure assets is vital to preventing and mitigating the impact of those seeking to do harm to Australia. Since implementation of previous reforms to the SOCI Act, the Department has provided guidance and worked with regulated entities to help them navigate the provisions.

101. However, feedback from Australian governments and industry has demonstrated that these provisions can unnecessarily limit the ability of Government, responsible entities and their employees to use or disclose information in the course of undertaking ordinary business or mitigate relevant risk effectively. These limitations can have the effect of hindering essential information sharing for the purposes of responding to high risk or time sensitive events.

102. This feedback is particularly acute given there are offences for unauthorised use or disclosure of information. Companies and agencies doing the right thing are ultimately not sharing information and erring on the side of caution rather than contributing to the collaborative best practice environment exemplified in the first part of this submission.

Stakeholder feedback

103. Stakeholders broadly support the policy intent of this measure. Feedback has mainly focused on the need to update guidance material to assist regulated entities in applying a harms based assessment to determining whether information or documents are 'protected information' and, where captured, determining if disclosure is permitted.

Our approach

104. Schedule 3 introduces a new definition of 'protected information' to apply to a document or information that, if disclosed, could cause harm, or pose risk to the Australian public, the security of the asset, commercial interests, the socioeconomic stability, national security or defence of Australia. This establishes a 'harms based approach' to simplify and clarify disclosure provisions to enable more effective and timely sharing of information under the SOCI Act.

105. The amendments further clarify the disclosure provisions – including introducing new authorised purposes and streamlining the administrative process for disclosure, by allowing APS employees in the Department to disclose once authorised by the Secretary or SES delegate.

106. The Department has also worked closely with the Attorney-General's Department to ensure the amendments align with the principles for the framing of secrecy offences outlined in the 'Final Report - Review of Secrecy Provisions'. Where appropriate, the principles are reflected in the legislation, for example the 'harms based' definition or their application is described in the explanatory material. In some cases, the principles were not directly applicable to the SOCI Act framework. The Department will continue to consider the principles for any future legislative development.

107. These provisions will be supported by guidance material to ensure stakeholders understand how to apply a harms-based test, and when protected information may be disclosed.

Schedule 4 - Direction to vary critical infrastructure risk management

The issue to be resolved

108. The *Security of Critical Infrastructure (Critical infrastructure risk management program) Rules (LIN 23/006) 2023* (the CIRMP Rules), requires specified entities to maintain, and comply with a written risk management program that manages the material risk of a hazard occurring, which could have a relevant impact on their critical infrastructure asset. Responsible entities must identify, and as far as is reasonably practicable, take steps to minimise or eliminate these material risks that could have a relevant impact on the reliability, availability, integrity or confidentiality of their asset.

109. However, the SOCI Act lacks the power to allow regulators to direct critical infrastructure entities to remedy seriously deficient risk management programs, without court action. The Cyber and Infrastructure Security Centre (CISC) is currently undertaking trial audits of critical infrastructure entity compliance with SOCI Act obligations. Early findings are that a number of entities are not fully compliant with the existing CIRMP obligation. In addition, a significant proportion of entities self-reported that they did not have a CIRMP in place by 30 June 2024 - noting the requirement is to have a CIRMP in place by 18 August 2024.

Stakeholder feedback

110. Stakeholders emphasised that regulated entities are best placed to manage risks to their assets, and highlighted the importance on voluntary engagement and consultation with regulated entities, and a high threshold for the directions power to ensure it is used as a last resort. A number of submissions requested clarity on the expectations, timeframes and definitions, particularly how a serious deficiency would be determined.

Our approach

111. Schedule 4 introduces a power for the regulator to issue a formal written direction to address seriously deficient elements of a risk management program.

112. A direction can only be issued in relation to a ‘serious deficiency’, which is defined to mean a deficiency that poses a material risk to national security, the defence of Australia, or the social or economic stability of Australia or its people.

113. The explanatory memorandum outlines that the Department’s intention is that where deficiencies are identified, these directions would be issued in accordance with the CISC’s Compliance and Enforcement Strategy. Wherever possible, the CISC seeks to work in partnership with industry to ensure regulated entities understand and effectively manage their risks, reserving compliance levers as last resort measures.

114. Additionally, the Bill introduces consultation requirements for the regulator to inform the entity they are considering issuing a direction to the entity to vary their risk management program to address a specified serious deficiency. The regulator must consider their response prior to issuing the direction.

115. These safeguards ensure this power is reserved for last resort action in rare circumstances where an entity is egregiously or wilfully non-compliant with their obligations, allowing for government to intervene when needed.

116. The Department remains committed to providing transparency and accountability to the Parliament and public on the operation of the SOCI Act. Under section 60 of the SOCI Act, the Secretary must give the Minister, for presentation to the Parliament, a report on the operation of the SOCI Act for each financial year including any directions given under this new power.

Schedule 5 – Security regulation for critical telecommunications assets

The issue to be resolved

117. Currently, telecommunications security obligations are legislated under both the Telecommunications Act and the SOCI Act, which has unintentionally caused unnecessary regulatory duplication and confusion. Schedule 5 will move current security and related obligations under the TSSR (which are amendments made by the *Telecommunications and Other Legislation Amendment Act 2017*) into the SOCI Act. These amendments have been consulted on in detail through the ATSRG.

Stakeholder feedback

118. While individual members in the ATSRG have represented unique views through the co-design process, general themes include:

- Promoting proportionate legislation targeted to assets that are critical to Australia;
- Ensuring that definitions are clear and actionable; and
- Emphasising the need for clear guidance material and engagement throughout implementation.

119. In addition to the co-design process through the ATSRG, commentary on this proposal during broader consultation was sparse, relative to the other proposals. However, those that commented broadly supported the proposal and encouraged further engagement and the reduction of regulatory burden and duplication.

Our approach

120. These amendments simplify security obligations for the telecommunications sector by uplifting and aligning key security obligations from Part 14 of the Telecommunications Act into the SOCI Act.

121. The SOCI Act primarily regulates Australia's most critical assets through the entities who own, operate and influence them. The Telecommunications Act regulates the conduct of carriers and carriage service providers (CSPs). One of the main aims of uplifting security regulation from the Telecommunications Act to the SOCI Act is to balance the regulatory burden on entities while ensuring improved national security outcomes. The Government must maintain its ability to oversee and intervene as required in Australia's telecommunications infrastructure.

122. To achieve this, amendments to the SOCI Act intend to maintain a high-level capture of all carriers and CSPs in Australia; with the details on limiting the application of obligations in subordinate legislation as detailed in **Attachment A1**. The Department intends for Schedule 5

to commence on proclamation at the same time as the subordinate legislation. The TSSR obligations will continue until this occurs. This will ensure sufficient time for implementation.

123. The Department intends to continue to engage with the ATSRG to co-design the details of the subordinate legislation and develop guidance on what assets are intended to be captured by the definitions, and how to comply with the obligations.

Schedule 6 – Notification of declaration of systems of national significance (SoNS)

The issue to be resolved

124. Currently the Secretary is required to notify all entities that have a reporting obligation (responsible entities and direct interest holders) under Part 2 of the SOCI Act in relation to a critical infrastructure asset, if that asset is declared a SoNS. In addition, critical infrastructure entities are obligated to track and report changes to joint interest arrangements for assets that have been declared SoNS which can be an unreasonably onerous responsibility. This is particularly the case when responsible entities and direct interest holders are also required to report changes directly to the Secretary through the Register of Critical Infrastructure Assets obligation under Part 2 of the SOCI Act.

Stakeholder feedback

125. Feedback on Schedule 6 was minimal but positive, with those that commented expressing support for simplifying and reducing reporting obligations.

Our approach

126. Schedule 6 will remove the notification to direct interest holders by the Secretary and the tracking and reporting of changes to joint interest arrangements for a critical infrastructure asset to simplify reporting obligations for SoNS.

127. Reporting obligations for responsible entities and direct interest holders come into effect at the time the asset becomes a critical infrastructure asset. As an asset must be a critical infrastructure asset prior to the asset being declared a SoNS, the declaration of an asset as a SoNS does not remove or alter these existing reporting obligations. Responsible entities would not be inhibited from notifying direct interest holders or relevant entities themselves, where appropriate, in accordance with the protected information sharing provisions in the SOCI Act.

128. These changes will reduce duplicative and onerous reporting obligations on SoNS entities. Direct interest holders will still be required to report on changes through the Register of Critical Infrastructure Assets obligation in Part 2 of the SOCI Act. The changes will also help protect the identity of the SoNS assets and avoid the risk of incorrect or inappropriate information disclosures to entities that are not the responsible entity for the asset.

Impact Analysis

Cyber Security Bill

129. An impact analysis has been prepared for the mandatory ransomware payment reporting obligation, noting the additional obligation it places on captured entities. The analysis can be found in full at Attachment B to the explanatory memorandum for the Cyber Security Bill.

130. The impact analysis contributed substantially to the final design of the measure as proposed by the Department, including the proposed threshold for captured businesses (to be detailed in the rules), the timeframes for reporting, what should be reported and the appropriate penalty for non–compliance with the obligation. The impact analysis considered all feedback to the Consultation Paper, and subsequent targeted consultation on the Exposure Draft of the Cyber Security Bill.

131. A further impact analysis is being prepared in relation to the smart device rules.

ERP Bill

132. An impact analysis has also been prepared on the ERP Bill (OIA23-04441), which can be found in full at Attachment B to the explanatory memorandum. The impact analysis found the benefits of uplifting the security of critical infrastructure assets through the reforms outweighs the cost and regulatory burden of implementation for industry, as this embedded preparedness may reduce the severity of costs incurred in the event of a significant incident in the future. A further impact analysis is being prepared in relation to the TSRMP Rules.

Conclusion and Next Steps

133. The Department is committed to working in partnership with industry to ensure seamless implementation of the legislative reforms to implement the Strategy, uplift Australia's cyber security posture and protect our critical infrastructure from all hazards. The Department aims to deliver best practice regulation by leading proactive engagement with regulated entities to achieve outcomes that are beneficial to the Australian community, regulated entities and the economy at large. Following passage of the Bills, the Department is committed to supporting industry to understand and meet the requirements of the measures proposed under the Package through guidance, further consultation on the proposed rules, and continued engagement and education to promote voluntary compliance.

134. Consultation across government and industry has shown that the Package strikes the right balance to reflect an industry-led and agile approach to cyber security and critical infrastructure protection, while allowing Government the legislative levers to assist when needed. The Bills also take into consideration the extensive feedback from industry throughout various consultation periods to ensure the obligations placed on businesses are reasonable and necessary, and that the correct safeguards are in place for the measures to meet their intended aims and avoid regulatory overreach. As the threat environment continues to evolve, this package of legislative reforms will equip industry with guidance and support to enhance their cyber resilience, the clarity of their obligations to protect their critical infrastructure assets and the legislative levers for Government to intervene to assist with incident response, enhancing and embedding Australia's preparedness to cyber security threats.

Australian Government
Department of Home Affairs

Cyber Security Legislative Reforms – Explanatory Document

Cyber Security Rules

Security of Critical Infrastructure Rules

Contact us

Enquiries regarding the licence and any use of this document are welcome at:

Department of Home Affairs

PO Box 25

BELCONNEN AC 26 P

- 23-02503-

Contents

Cyber Security Rules

Context

Australia's cyber security landscape is evolving quickly, with malicious activities targeting Australia becoming more frequent and sophisticated. The Cyber Security Bill is designed to provide a clear legislative framework for broad, whole-of-economy cyber security issues, positioning the Australian Government to respond to new and emerging cyber security threats. The Bill is intended to provide additional protections to Australian citizens and businesses, build mitigations for extant cyber risks, and improve the Government's threat picture to inform protections, incident response procedures, and future policy.

Part 2—Security standards for smart devices

To date, Australia's voluntary approach to smart device security is fragmented and insufficient. In 2020, the Government introduced a voluntary Code of Practice: Securing the Internet of Things for Consumers setting out guidance for smart device manufacturers and suppliers aligned to the European Telecommunications Standards Institute (ETSI) standard. A government study of manufacturers' uptake of the Code revealed a low level of adoption across the country. Mandatory standards will uplift the cyber security of smart devices in Australia and ensure that Australians can trust in the security of their digital products.

The power within the Bill will enable the Minister for Cyber Security to prescribe security standards for all, or a subclass of, smart devices, through subordinate legislation, also known as rules. As the initial application of the power, it is intended the rules will detail the technical security standards required for consumer-grade relevant connectable products. Future applications of the rules will be considered as required, for example to address risks with evolving technology.

Standards making power

It is the Department's intention to define a ***consumer*** in the same way as section 3 of the Australian Consumer Law.

Products that are included in the scope of the security standard will be set out in the rules and those that meet the definition of ***relevant connectable product*** as defined in section 13 of the Cyber Security Act and would be expected to be reasonably acquired by a ***consumer***. The combined definitions means that this set of rules applies only to consumer-grade smart devices unless otherwise exempted from the rules.

It is proposed the rules would provide that the security standard for the specified class i.e. consumer-grade, apply to products that will be acquired in Australia, and the security standard applies to products that are intended by the manufacturer of the product to be acquired for personal, domestic, or household use. The rules further specify that the acquisition is intended to be in Australia by a ***consumer***. Where a business acquires a product as a consumer, the business will have the same protections as outlined in the Australian Consumer Law.

Exempt devices

The proposed format of rules would take an exclusion-based approach for the coverage of devices for each specified security standard. Generally, devices will be excluded if: there is existing legislation that can adequately address the cyber security of these devices, there is work underway across Government to develop a higher or bespoke standard for these devices, or the complexity of these devices means that being mandated under these rules will risk a lower standard being met. The list of excluded devices for each standard can be amended to exclude further devices, or scope devices back under the coverage of the standard.

The rules may provide that some types of consumer-grade relevant connectable products could be exempt from needing to comply with the security standard set out in Schedule 1. For example, the rules could provide that medical devices would be exempt from needing to comply with a security standard because these devices are already covered by the powers provided in the *Therapeutic Goods Act 1989.*

Statements of compliance

It is the Department's intention that the rules set out the minimum details necessary for a statement of compliance for devices that are required to meet the security standard as set out in the rules. It is proposed that the rules would outline that responsible entities, manufacturers and suppliers, must retain the statements of compliance of products in scope under this security standard for a minimum of 10 years.

Notification of recall

Section 20 of the Cyber Security Act establishes that if a manufacturer fails to comply with a recall notice per section 19 of the Cyber Security Act, the Minister may publish a notification that the relevant entity has failed to comply with the notice on a public website.

It is the intention that the rules would provide that if a product has been subject to a recall notice under section 19 of the Cyber Security Act, and a manufacturer or supplier has failed to make the product unavailable for acquisition or supply in Australia, a consumer may wish to consider destroying that product or take extra precautions when using the product.

Security standards for relevant connectable products

As the initial application of the power, it is intended the rules will detail the technical security standards required for consumer-grade relevant connectable products. The rules would explain any relevant technical definitions related to the security standards.

It is the Department's intention that the rules prescribe security requirements on the application of passwords in consumer-grade relevant connectable products. Where the hardware or software of a product requires the use of a password, the security standard would require that this password must be:

- unique per product – meaning that universal default passwords (sometimes as simple as "admin" or "default") that are applied consistently across all units of a product must not be used; or
- defined (or, set) by the user of the product.

Further, it is intended the rules would prescribe additional requirements on passwords that are unique per product. These requirements would prevent the password from being otherwise easily guessable by someone other than the user of the product. It is intended the rules prohibit passwords, which are unique per product, from being:

- based on incremental counters;
- based on or derived from publicly available information;
- based on or derived from unique product identifiers, such as serial numbers, unless this is done using an encryption method, or keyed hashing algorithm, that is accepted as part of good industry practice; or
- otherwise guessable in a manner unacceptable as part of good industry practice.

The proposed rules would also prescribe requirements surrounding security issue disclosure mechanisms for the hardware or software of consumer-grade relevant connectable products. Manufacturers would be required to publish information regarding these requirements, including:

- at least one point-of-contact to allow a person to report security issues related to the hardware or software of the product to the manufacturer; and
- details of when a person who makes a security issue report will receive an acknowledgement of receipt of the report and status updates regarding the report until the resolution of the reported security issue.

Importantly, the rules would place clear requirements on the way this information must be published to ensure that it is accessible, clear and transparent, and in English. Additionally, it is proposed the information must be made available without request, free of charge, and without seeking or collecting personal information about the person making the report.

The rules are intended to prescribe the requirement for manufacturers of consumer-grade relevant connectable products to define and publish a support period for security updates for their products. A security update is the elements of a software update that protect or enhance the security of a product, including addressing security issues that have been discovered by or reported to the manufacturer. Notably, any software update may be entirely, partially, or in no part a security update.

To meet this requirement, a manufacturer would be required to first define a support period (with an end date) for which security updates for the product will be provided by, or on behalf of, the manufacturer. This defined support period would then be required to be published in a manner such that it is:

- accessible;
- clear and transparent;
- in English;
- understandable by a reader without prior technical knowledge; and
- made available without request, free of charge, and without seeking or collecting personal information about the reader.

In the case where a manufacturer offers to supply the product on their website or another website under their control, the defined support period would need to be published alongside or otherwise given equal prominence as the main characteristics of the product published on that website. This is to ensure that a person contemplating the purchase of a product can easily find the defined support period while examining information on the features, specifications or benefits of the product – and subsequently be able to consider the defined support period in their purchasing decision.

It is intended the defined support period could not be shortened after it is published by the manufacturer. However, the period would be able to be extended. If extended, the new defined support period would need to be published by, or on behalf of, the manufacturer as soon as practicable in a manner consistent with the publishing of the original defined support period.

Part 3—Ransomware reporting obligations

Turnover threshold

The Cyber Security Bill establishes a rule making power for the Minister for Cyber Security, to prescribe the annual turnover threshold for a business, which if earned in the previous financial year, would ensure they are captured by the mandatory ransomware reporting obligation. It is proposed, in the rules, this turnover threshold would be specified at AUD $3 million.

The $3 million threshold would be chosen as it was supported by a majority of stakeholders during rounds of consultation, and aligns with the *Privacy Act 1988*, where entities with an annual turnover of less than $3 million are considered to be small businesses and exempt from reporting requirements of notifiable data breaches. This does not directly reference the Privacy Act and does not carry the same series of exclusions as provided in the Privacy Act. Should the relevant threshold be amended in the Privacy Act, this threshold will not be impacted.

The selection of this threshold captures approximately 6.56% of registered Australian businesses. This threshold aims to provide the best balance of regulatory impact versus reporting burden on industry and provide the Australian Government with enhanced visibility and understanding of the ransomware threat and impact.

The Cyber Security Bill also establishes a rule making power for the Minister for Cyber Security to specify a formula that applies if a business has been carried on for only part of the previous financial year (to determine their turnover, and whether or not they are captured by the turnover threshold). In the rules, this formula would include the figure '$3 million' multiplied by the number of days in the part, divided by the number of days in the previous financial year. For example, if a business was established in January of a year, and has been operating for 6 months (until the new financial year), the business will use this formula to determine their annual turnover threshold. If this threshold is less than $3 million, the business is not captured by the mandatory ransomware reporting obligation. If this threshold is more than $3 million, the business is captured by the mandatory ransomware reporting obligation.

Information that must be included in reports

The Cyber Security Bill establishes a rule making power for the Minister for Cyber Security to provide additional clarity about the specific information that must be included in a ransomware payment report. The core detail of what must be included in a ransomware payment report is outlined in section 27 of the Cyber Security Bill.

The information required in a ransomware payment report is qualified to such information that 'at the time of making the report, the reporting business entity knows or is able, by reasonable search or enquiry, to find out' as outlined under subsection 27(2) Cyber Security Bill. It is proposed that the rules would provide further clarity in relation to the details to be provided under the Bill.

By enabling clarity in the rules, entities can be certain what information is required to satisfy the requirements of the legislation. This also enables the relevant flexibility to add new information as technology develops, or to remove information that has become redundant or is no longer helpful.

Part 5—Cyber Incident Review Board

The Board will play a key role in uplifting the cyber security and national resilience of Australia by supporting the Australian Government to review and assess significant cyber incidents and make concrete recommendations that would aid in the prevention, detection, response and minimisation of cyber security incidents. To support implementation of the Cyber Incident Review Board framework, the rules would establish the governance parameters through which the Board will perform its functions.

Reviews by the Board

The rules would provide that the Board may undertake a Review concurrently to other investigative or regulatory actions, however it will not interfere with these processes. This separation is crucial to supporting the function of the Board to undertake no-fault reviews of incidents, while maintaining non-interference with other investigative processes. Appropriate consultation with regulators and law enforcement agencies will be undertaken to ensure this non-interference is maintained for the duration of a review. This will operate in conjunction with section 46(2)(b) of the Bill which prescribes that a review may only be conducted after the incident or series of incidents, and the immediate response, has ended.

Upon referral, the decision to undertake a review is at the discretion of the Chair and standing members, subject to the cyber security incident or series of incidents satisfying at least one of the criteria set out at subsection 46(3) of the Cyber Security Bill. The governance rules would outline that the Board must consider all written referrals received from persons or entities prescribed in section 46(1), and decide whether a review should occur.

When making decisions regarding prioritisation of referrals and conduct of reviews, it is proposed the rules would outline that the Board must have regard to:

- the severity and scale of the cyber incident, or incidents, to which the referral or review relates,
- the availability of Board members,
- the availability of members of the Expert Panel,
- the relevance of skills, knowledge or experience of members to the Expert Panel to assist in undertaking a review.

Should the Board consider a Review should proceed, they must establish a Terms of Reference.

Upon causing a review to be conducted, the rules provide that the Terms of Reference would be drafted to include details on elements of the review such as:

- the number of Board members and members of the Expert Panel appointed to assist the Board who will conduct the review;
- specify the minimum security clearance required to participate in the review; and
- specify any eligibility requirements, beyond those established by the Minister, for the appointment of members of the Expert Panel to assist the Board in relation to the review.

The Terms of Reference will be made public to maintain appropriate transparency of the review process.

The Cyber Security Bill establishes a rule-making power for the Minister for Cyber Security to prescribe the eligibility requirements for members of the Board. The rules will include a requirement to hold or be eligible to obtain a security clearance, as well as demonstrated qualifications and/or experience in the field of law, cyber security, information security, incident response and crisis management, public administration, critical infrastructure sectoral experience, critical infrastructure regulation, or audit and assurance experience. This will ensure the Board has an appropriate mix of skills, experience and diversity.

It is the Department's intention that the rules will also provide the Board with the flexibility to identify additional requirements for each review, if considered necessary, to ensure the Board can leverage the deep subject matter expertise and sectoral knowledge of industry as it relates to a specific incident, or series of incidents.

It is the intention of the rules that the Minister may appoint a person as an acting member of the Board if a Board member, other than the Chair is absent from duty or otherwise unable to perform their role. The Minister must ensure that the acting Board member meets the eligibility criteria.

It is proposed that the rules will require the board to disclose to the Minister all interests, pecuniary or otherwise, that the person has in relation to the Board, or its equities. Disclosures after appointment must be made in accordance with section 29 of the *Public Governance, Performance and Accountability Act 2013.* Board members must not engage in paid, full-time work of any kind that in the Minister's view, could conflict with the Board member's ability to carry out their functions or would negatively affect their performance.

It is proposed that the rules allow the Minister may also determine the conditions for leaves of absence for the Chair, with the Chair, in turn, determining the conditions for leaves of absence for Board members.

It is the Department's intention that the rules establish governance processes for Board members to resign from the Board and the circumstances and processes in which the Minister may terminate members of the Board. The rules allow the Board member to make submissions to the Minister regarding termination of employment and the Minister must consider any submissions that are made, including to give written notice of the termination.

Expert Panel

The Cyber Security Bill establishes a rule making power for the Minister for Cyber Security to determine the details of appointments to the Expert Panel. The Department's intention is that appointments to the Expert Panel are on a part-time basis and may be for any period prescribed by the Minister, provided the period is no longer than four years.

As with Board members the rules propose to establish eligibility criteria for the Expert Panel to ensure it also has an appropriate mix of skills, experience and diversity and while it may differ from the eligibility criteria for the board is intended to include a requirement to hold or be eligible to obtain a security clearance, demonstrated qualifications and/or experience in the field of law, cyber security, information security, incident response and crisis management, public administration, critical infrastructure sectoral experience, critical infrastructure regulation, or audit and assurance experience. The Department intends to enable persons to register their interest to participate in the Expert Panel via a public webpage. There would be no restrictions on the number of persons that can be appointed to the Expert Panel at any given time.

To ensure the rights, limitations and duties under the *Public Service Act 1999* are applicable to all members of the Board, Expert Panel members are considered APS employees when exercising their duties as a member of the Board. This ensures the expectations on full-time Board members and part-time Expert Panel members are consistent. Remuneration and other allowances of members of the Expert Panel would be determined by the Chair of the Board through rules.

The rules also provide that the Expert Panel would be subject to the same disclosure requirements, resignation, and termination processes as the Board, however, the Chair would be the decision maker, rather than the Minister.

Other matters

To support transparency in Board operations, the governance rules would prescribe certain administrative processes that the Board must follow in the performance of its functions while ensuring it may regulate proceedings as it (the Board) considers appropriate.

It is the intention that the rules allow the Board the flexibility to operate as it sees fit specific to each different review it undertakes, with the condition that all deliberations and decisions are accountable and documented.

It is the intention that the rules would establish when meetings are to be convened, providing the Chair and the Board with the flexibility to determine how to conduct themselves and what matters warrant meetings, for example, progress or milestone meetings, if there has been public reporting about the cyber security incident or a member of the Board comes across new information relevant to a review.

The rules would prescribe that there must be a majority of Board members present in a meeting to constitute a quorum, to give effect to the deliberations or decisions of the Board. However, if Board members are not present for meetings either voluntarily, or because they are required not to be present for deliberations, the remaining members of the Board may constitute a quorum for the purposes of carrying out subsequent deliberations.

Security of Critical Infrastructure Rules

Context

Threats to the operation of Australia's critical infrastructure continue to be significant and far-reaching. From natural hazards through to human-induced threats—all have the potential to significantly disrupt critical infrastructure. The *Security of Critical Infrastructure and Other Legislation Amendment (Enhanced Response and Prevention) Bill 2024* (ERP Bill) is designed to enhance the security and resilience of critical infrastructure in the face of all hazards. To support implementation of the ERP Bill, it is anticipated that amendments to existing rules and new rules under the SOCI Act will be required. These amendments will be subject to mandatory consultation for a minimum 28 day period, following passage of the ERP Bill, however the intended operation of these amendments is detailed below.

Part 1 – Telecommunications security and risk management program

Background

The Telecommunications Security and Risk Management Program Rules (TSRMP Rules) would be a new instrument, to be made by the Minister of Home Affairs under the existing Part 2A (critical infrastructure risk management programs) and the new Part 2D (security regulation for critical telecommunications assets) of the SOCI Act. The intention of the TSRMP Rules is to proportionately apply and clarify security obligations for critical telecommunications assets under the SOCI Act. The proposed details of the TSRMP Rules, as outlined in this document, has been consulted on with key government agencies and co-designed with industry through the Australian Telecommunications Security Reference Group (ATSRG).

The Department's intention is for entities to be able to group their assets for the purposes of their risk management program. For example, if an entity operates assets in multiple asset classes, compliance with the TSRMP Rules for all assets will be taken to be compliance with the CIRMP Rules. However, compliance with the CIRMP Rules is not the equivalent of compliance with the TSRMP Rules.

Proportionate obligation application

The TSRMP Rules would contain a mechanism to proportionately apply key obligations in Parts 2A and 2D of the SOCI Act to asset types of varying size and criticality. The mechanism would preserve the broad capture of all critical telecommunications assets in the SOCI Act for the purposes of Government assistance, information gathering and directions powers while limiting positive security obligations to a critical subset of critical telecommunications assets. The intention is to balance security outcomes with regulatory burden and allow flexible collaboration between government and industry as the security and threat environment evolves.

The TSRMP Rules would apply key obligations to the critical telecommunications assets of all carriers and a subset of carriage service providers that meet the prescribed threshold of 20,000 active carriage services or supply to government or defence. As detailed further below under "Application Rules", this threshold is also intended to apply to obligations under the existing Part 2 (register of critical infrastructure assets) and Part 2B (mandatory cyber incident reporting – MCIR).

The intended effect is to apply powers and obligations under the SOCI Act according to the following table:

	Notify data service providers s. 12F(3)	Asset Register Part 2	MCIR Part 2B	Obligation to protect asset, including risk management program Parts 2A and 2D	Notification obligation Part 2D	ECSOs for declared systems of national significance Part 2C	Government assistance; directions & information gathering power Parts 2D, 3, 3A, & 4
Carrier's assets	✓	✓	✓	✓	✓	May apply	✓
Carriage service provider's assets (meet threshold)	✓	✓	✓	✓			✓
Critical telecommunications assets that do not meet threshold	✓						✓

Relevant carriage service provider threshold

The TSRMP would introduce a definition to specify *relevant carriage service provider assets* as a subset of in-scope carriage service provider assets for the risk management program obligation (Part 2A). The intent is for captured carriage service providers to comply with the obligations above when they provide 20,000 or more active carriage services or supply to government or defence. The Department intends for the scope of carriage services to be captured as follows:

- Broadband services, which includes services connected by means of a:
    - fibre to the Building connection;
    - fibre to the Curb connection;
    - fibre to the Node connection;
    - fibre to the Premises connection;
    - fixed wireless internet connection;
    - hybrid Fibre Coaxial connection;
    - fixed line services;
    - satellite connection;
    - any other connection type;
- fixed telephone services;
- public mobile telecommunications services;
- voice only services.

The Department intends for the responsible entity for an asset that meets the definition to comply with the positive security obligations to:

- Protect the critical telecommunications asset (including by complying with risk management obligations under Part 2A of the Act)
- Comply with MCIR requirements (Part 2B of the Act);

- Provide information to the register of critical infrastructure assets (Part 2 of the Act).

Compliance grace period

The Department intends for the TSRMP Rules to establish a compliance grace period for the subset of critical telecommunications assets required to comply with the risk management program obligation (Part 2A). The intention is that the risk management program obligation would not apply in the 6 months following the commencement of the instrument and, if an asset becomes a critical infrastructure asset after that period, 6 months after it become a critical telecommunications asset. As detailed below, the Department would provide an additional grace period for compliance with a prescribed cyber security framework.

Requirement for a responsible entity to protect their critical telecommunications asset

The TSRMP Rules would largely mirror the existing *Security of Critical Infrastructure (Critical infrastructure risk management program) Rules (LIN 23/006) 2023* (CIRMP Rules) with additions to reflect telecommunications-specific risks and to provide further information on compliance with the obligation to notify certain changes and proposed changes to telecommunications service or system (section 30EC). While section 30EB(3)(c) states that an entity must comply with any other requirements prescribed by the rules, the Department does not intend to prescribe additional requirements at this time.

Material risk

Material risks would be defined by the TSRMP Rules to include a variety of risks that could significantly impact a critical infrastructure asset if they occurred. The intention is for material risks under the TSRMP Rules to include:

- a stoppage or major slowdown of the critical asset's function for an unmanageable period;
- an impairment of the critical asset's functions that prejudices the social or economic stability, or defence or national security, of Australia;
- a substantive loss of access to, or deliberate or accidental manipulation of, a critical component of the critical asset;
- an interference with the critical asset's operational technology or information communication technology essential to the functioning of the asset;
- the storage, transmission or processing of sensitive operational information outside Australia;
- remote access to operational control or operational monitoring systems of the CI asset;
- compromise, theft or manipulation of communications;
- unauthorised access to or unauthorised use of a critical asset by a:
    - major supplier; or
    - critical worker; or
    - managed service provider;
- risks to data storage systems that hold business critical data, where vulnerabilities could impact the availability, integrity, reliability or confidentiality of the asset.

This broadly replicates the material risks captured within the CIRMP Rules, with some amendments to reflect material risks unique to critical telecommunications assets.

General – all hazards

The Department intends for the 'General – all hazards' section of the TSRMP Rules to mirror the existing CIRMP Rules. These require the responsible entity for a critical asset to identify all material risks to their asset across 'all hazards' and to minimise or eliminate those risks so far as it is reasonably practicable to do so. The Department intends for the TSRMP Rules to set out the conditions that an entity's written risk management program must satisfy, including that it:

- is reviewed and up to date;
- identifies and provides contact details for each position within the entity that is responsible for developing, implementing and complying with the risk management program;
- contains a risk management methodology;
- describes how the risk management program will be reviewed.

Cyber and information security hazards

The Department intends for this section of the TSRMP Rules to require responsible entities to minimise or eliminate any material risk of a cyber and information security hazard from occurring and mitigate the relevant impact of a cyber and information hazard on the asset. This section would prescribe minimum cyber security maturity frameworks for entities to meet within prescribed time periods.

All entities responsible for an in-scope critical telecommunications asset would need to establish and maintain a process or system to meet, where relevant, at least maturity indicator 1 in one of the cyber security frameworks listed in the TSRMP Rules or an equivalent framework. The entity would be required to meet this condition within 12 months after the end of the 6-month grace period. Responsible entities for carrier owned or operated assets would additionally need to meet maturity indicator 2 of the relevant frameworks within 12 months of meeting maturity indicator 1. The proposed timings are laid out in the table below:

	Compliance Period After Switch-on of the Rules (or when the asset later becomes a critical telecommunications asset)		
	6 months	18 months	30 months
Carrier's assets	TSRMP	Cyber Framework – Maturity indicator 1	Cyber Framework – Maturity indicator 2
Carriage service provider's assets (that meet threshold)	TSRMP	Cyber Framework – Maturity indicator 1	

The Department, in close consultation with industry through the ATSRG, has determined that it would be appropriate for a subset of critical telecommunications assets to have more mature cyber maturity prescriptions than other critical infrastructure assets. This responds to the heightened risk environment for critical telecommunications assets and their centrality to the security and prosperity of Australians.

Because some cyber security frameworks do not contain maturity indicator levels, the TSRMP Rules would allow an entity to comply with their preferred cyber security framework where they document, in their written risk management program, the steps taken to make their program equivalent to maturity indicator 2 of an appropriate cyber maturity framework. This measure would require entities to demonstrate that, where no maturity indicator is built into the framework, such as the *Framework for Improving Critical Infrastructure Cybersecurity* published by the National Institute of Standards and Technology of the United States of America (NIST framework), that their use of the framework is equivalent to maturity indicator 2. The NIST framework has been highlighted as a preferred cyber maturity framework during industry consultation due to its international application and operating system-agnostic approach.

Personnel hazards

The Department intends for the 'personnel hazards' section of the TSRMP Rules to mirror the existing CIRMP Rules. These require a responsible entity to establish and maintain in their risk management program, as far as it is reasonably practicable to do so, a system to minimise or eliminate material risks relating to malicious or negligent personnel. There would be a requirement for a responsible entity to identify critical workers and assess their suitability to access critical components of the asset. Entities may choose to engage the AusCheck background check scheme to conduct this suitability assessment.

An AusCheck check allows entities to conduct a background check that includes:

- identity verification;
- a criminal record assessment against CIRMP security relevant offences by AusCheck using information collected by the Australian Criminal Intelligence Commission (ACIC);
- a national security assessment by the Australian Security Intelligence Organisation (ASIO);
- a 'right to work in Australia' check if a person is not an Australian citizen, conducted through the Visa Entitlement Verification Online (VEVO) system.

Entities would not be compelled to use the AusCheck scheme and may choose how they comply with the suitability assessment requirement.

Supply chain hazards

The Department intends for the 'supply chain hazards' section of the TSRMP Rules to mirror the existing CIRMP Rules. It is intended that this section will require a responsible entity to address vulnerabilities in the supply chain, including the

following material risks:

- unauthorised access, interference or exploitation of the asset's supply chain; and
- misuse of privileged access to the asset by any provider in the supply chain; and
- disruption of the asset due to an issue in the supply chain; and
- arising from threats to people, assets, equipment, products, services, distribution and intellectual property within supply chains; and
- arising from major suppliers; and
- any failure or lowered capacity of other assets and entities in the entity's supply chain; and
- as far as it is reasonably practicable to do so, mitigate the relevant impact of a supply chain hazard on the asset.

Physical security and natural hazards

The Department intends for the 'physical security and natural hazards' section of the TSRMP Rules to mirror the existing CIRMP Rules. This would require a responsible entity to establish and maintain in their risk management program a process or system:

- to identify the physical critical components of the CI asset; and
- to control access to physical critical components; and
- for responding to incidents where unauthorised access to a physical critical component occurs; and
- for managing and mitigating a variety of physical security hazards and natural hazards to their CI assets; and
- to test that security arrangements are effective and appropriate and promote resilience.

Responsible entity's notification obligations

Provisions will be included in the TSRMP Rules to clarify the information relevant to an entity's circumstances that they should provide to the Secretary under the section 30EC requirement to notify of certain changes and proposed changes to telecommunications service or system. This section of the TSRMP Rules would promote a flexible system, driven by the principle of providing sufficient information to allow the Secretary to collaborate with industry and offer pertinent risk advice.

The Department intends for this section of the TSRMP Rules to enhance clarity for a responsible entity on what is expected of them to protect national security interests and promotes transparency and accountability. Government and industry anticipate that this would encourage engagement with government agencies on managing security risks such as espionage, sabotage and foreign interference and speed up the assessment process.

Where reasonably practicable to produce and relevant to the context of the change or proposed change, the Department intends that these provisions would require a responsible entity's notification to include:

- a security risk assessment;
- information about relevant controls for identified risks;
- descriptions of hardware and software being introduced;
- details about major suppliers for the project;
- schematics and system documentation;
- a timeline of the proposed change;
- any other relevant information.

Part 2 – Amendments to the Application Rules

Summary of changes

Some critical telecommunications assets are currently subject to 'SOCI-like' obligations applied under the Telecommunications Act, namely the Asset Register and MCIR obligations, through the *Telecommunications (Carrier License Conditions—Security Information) Declaration 2022* and the *Telecommunications (Carriage Service Provider—Security Information) Determination 2022*. These instruments would be repealed.

The *Security of Critical Infrastructure (Application) Rules (LIN 22/026) 2022* would be amended to apply these obligations to a subset of critical telecommunications assets. This subset would mirror the assets captured by the TSRMP Rules, i.e. all carrier assets and 'relevant carriage service provider assets', as per the above heading 'Relevant carriage service provider threshold'.

Part 3 – Amendments to the Critical Infrastructure Risk Management Program Rules

Context

Schedule 1 of the ERP Bill, once enacted, amends the SOCI Act definition of 'critical infrastructure asset' to specify that data storage systems that store or process business critical data are part of the critical infrastructure asset, where vulnerabilities in those systems could impact the function of that asset.

The effect of Schedule 1 would be to clarify the application of obligations for critical infrastructure assets under the SOCI Act, including the CIRMP obligation, to those data storage systems. Under the amendments, critical infrastructure entities currently captured by the SOCI Act would be required to identify and control against risks to their data storage assets as part of their CIRMP.

Amendments to the CIRMP Rules would reflect the Schedule 1 amendments to the SOCI Act and provide further details on the responsible entity's obligation.

Summary of changes

Section 6 of the CIRMP rules would be amended to include risks to data storage systems holding 'business critical data' as 'material risks'.

This would require the responsible entity to identify material risks to data storage systems holding 'business critical data' and minimise or eliminate those risks across 'all hazards', including cyber, personnel, supply chain, physical security and natural hazards.

Put simply, the amendment to Section 6 would require responsible entities to include risks to relevant data storage systems within their CIRMP.