Australian Government
Department of Home Affairs

Department of Home Affairs submission into the Review of the Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022

Parliamentary Joint Committee on Intelligence and Security

February 2022

Introduction

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 Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022 (the SLACIP Bill).

This submission addresses the PJCIS' terms of reference and provides an overview of the SLACIP Bill.

The Department notes that the PJCIS' Advisory Report on the Security Legislation Amendment (Critical Infrastructure) Bill 2020 (SLACI Bill 2020) and Statutory Review of the Security of Critical Infrastructure Act 2018 (the Advisory Report) dated 29 September 2021, made 14 recommendations.

The Department notes that the recommendations included that the SLACI Bill 2020 be split and the urgent elements of the critical infrastructure reforms be legislated in the shortest timeframe possible. Government amendments were introduced to carve out elements from the SLACI Bill 2020. Following this, the *Security Legislation Amendment (Critical Infrastructure) Act 2021* (the SLACI Act) received the Royal Assent on 2 December 2021, amending the *Security of Critical Infrastructure Act 2018* (the SOCI Act). Government has now prepared the SLACIP Bill, which includes the remaining elements of the critical infrastructure reforms from the SLACI Bill 2020 and some minor technical amendments.

The provisions of the SLACIP Bill are drawn in substance from the SLACI Bill 2020. In line with Recommendation eight of the Advisory Report, the measures in the SLACIP Bill have been amended in accordance with PJCIS Recommendations and released for feedback as the SLACIP Bill Exposure Draft (Exposure Draft), which was consulted on for a period of 6 weeks from 15 December 2021 to 1 February 2022. A range of further amendments detailed below have been incorporated into the SLACIP Bill, based on that feedback received.

This submission outlines the substance of that industry consultation and describes how consultation and feedback drove over 70 amendments in the SLACIP Bill, from the original provisions presented to the PJCIS in the form of the SLACI Bill 2020.

This submission also includes a preliminary analysis of the economic costs and benefits of the proposed risk management program, noting that the risk management program rules are subject to further mandatory consultation under the provisions of the SLACIP Bill. The Department has developed a draft Regulation Impact Statement (RIS) relating to the risk management program rules showing the costs of inaction significantly outweigh the expense of introducing these reforms. Draft rules and a draft extract from the Explanatory Statement to the draft rules are included in the Explanatory Memorandum to the SLACIP Bill. A copy of this material is at **Attachment A** to this submission.

Background

Threats ranging from natural hazards to human-induced threats (including malicious cyber activity) all have the potential to significantly disrupt Australia's critical infrastructure. The interconnected nature of our critical infrastructure means that the compromise of one essential function could have cascading consequences which could impact the essential services that all Australians rely on and lead to severe economic impacts. The Australian Government and industry report a worsening critical infrastructure threat environment, exacerbated by malicious cyber activity by state and criminal actors. Australia is not immune and cannot be complacent, as the threat of a significant cyber attack (or attacks) is possible and growing ever more likely.

The security and resilience of critical infrastructure also underpins Australia's national security and defence capability. The Government recognises that while foreign involvement brings many benefits, it can also greatly increase a malicious actor's ability to access and control Australia's critical infrastructure, in a way that is much more difficult to detect, deter and prevent. A disruption to critical infrastructure assets could have a range of serious implications for business, government and the community.

As threats and risks to Australia's critical infrastructure continuously evolve in an increasingly interconnected world, so too must our approach to ensuring the ongoing security and resilience of these assets and the essential services they deliver, protecting our economy and sovereignty.

Reform Overview

Over 70 changes have been made by the provisions introduced under the SLACIP Bill to those provisions that were introduced in the SLACI Bill 2020 (see **Attachment B**). These changes were made largely in response to industry feedback, and range from whole sections that outline recognised international and domestic risk management standards, to minor corrections to references between pieces of legislation.

To illustrate the types of changes that have been made, below is a summary of the key 30 proposed changes in the SLACIP Bill (compared to the SLACI Bill 2020).

Proposed amendment	Figures
Minor/Technical	Four (4) technical or minor clarifying amendments
Industry consultation—asset definitions	Five (5) asset definitions narrowed and clarified in line with stakeholder feedback
Industry consultation—risk management programs	One (1) new streamlined reporting regime to recognise Digital Transformation Agency's (DTA's) Hosting Certification Framework (HCF); new rule making power to specify additional frameworks (Part 2AA) Two (2) key amendments to enable recognition of existing standards, including international standards
Industry consultation—enhanced cyber security	Six (6) amendments to add additional criteria the Secretary must consider when applying enhanced cyber security obligations
Enabling appropriate and lawful exchange of protected information	Four (4) new authorisations for sharing protected information One (1) new exceptions to the offence of unauthorised disclosure
Reconsideration of breadth of immunities	Four (4) key amendments to expand the types of entities protected for existing immunities when complying with Parts 2B, 3 and 3A
Industry consultation—other amendments	Three (3) amended or new exceptions to the definition of 'direct interest holder' to prevent unintended capture of certain entities

The SLACI Act was the first stage of reforms to the SOCI Act, receiving the Royal Assent on 2 December 2021. The PJCIS referred to the SLACI Act as 'Bill One' in its Advisory Report.

The SLACIP Bill, or as the PJCIS referred to it, 'Bill Two' proposes two key measures to amend the SOCI Act:

- A new positive security obligation for responsible entities to create and maintain a **critical infrastructure risk management program**, and
- A new framework for **enhanced cyber security obligations** required for operators of **systems of national significance** (Australia's most important critical infrastructure assets).

Security Legislation Amendment (Critical Infrastructure) Bill 2020

The Government accepted the PJCIS Recommendation One of the Advisory Report, that the original SLACI Bill 2020 should be split into two separate Bills, in order to promptly legislate urgent measures, which sought to address the immediate threat to Australia's critical infrastructure, while deferring the remainder of the proposed framework to be revisited following a period of further consultation with industry. The Government's response to the PJCIS Advisory Report's recommendations one to five, 10 and 14 were acquitted through the SLACI 2021.

The SLACI Act has expanded the scope of the SOCI Act from applying to four asset classes to eleven sectors and 22 asset classes; expanded the Register of Critical Infrastructure Assets requirement for responsible entities to provide ownership, operational, interest and control information; provided a regime for the Commonwealth to receive mandatory reports in relation to cyber security incidents to the Australian Cyber Security Centre's (ACSC's) online cyber incident reporting portal, and provided a regime for the Commonwealth to respond to serious cyber security incidents immediately prior to, during, or following a significant cyber security incident to ensure the continued provision of essential services through Government Assistance or step in powers.

The SLACI Act and the Minister for Home Affairs' second reading speech provides a response to all of the remaining elements of the Advisory Report (relevantly recommendations six to nine, 11, 12 and 13).

Consultation Process

The Department works in partnership with industry to address the challenges each sector faces and how those challenges can be overcome. While the Government has access to classified threat information, industry understands the dynamics, technologies and interdependencies of each sector. The proposed reforms can only succeed through a public-private partnership between Government and industry, and this partnership has been essential throughout the development of the broader reform process, including the SLACIP Bill.

As outlined in the Department's engagement with the Committee previously, the Government has documented its intended approach to develop this reform in partnership with industry and has said it will undertake meaningful and genuine engagement to develop the rules which underpin the risk management program, as proposed in SLACIP.

In accordance with Recommendations 8 and 9 of the Advisory Report, the Department undertook a comprehensive program of stakeholder engagement to finalise rules to underpin the risk management program and to consult on the Exposure Draft of the SLACIP Bill.

Date	Description
4 February 2022	Department held a final town hall to summarise the key feedback from the consultation process on the exposure draft of the SLACIP Bill.
1 February 2022	Consultation on the SLACIP Bill concluded

December 2021 - February 2022	Department supported the Minister for Home Affairs (the Minister) to hold sector-specific roundtable meetings with representatives from six sectors to ensure the intent of the reforms was understood and supported at the highest levels of industry.
25 January 2022	Department held a virtual town hall on the SLACIP Bill
20 January 2022	Department engaged with the data or storage processing sector, discussing the amended definition introduced in the SLACIP Bill.
18 January 2022	Department held a virtual town hall on the SLACIP Bill
21 December 2021	Department held a virtual town hall on the SLACIP Bill
15 December 2021	Exposure draft of the SLACIP Bill was released for public consultation.
8 December 2021	Energy Market Operators Risk Management Program Rules Final Consultation Session
7 December 2021	Department consulted with trusted industry representatives of the Resilience Expert Advisory Group (REAG) on the revised Critical Incident Reporting System (CIRS).
2 December 2021	SLACI Bill received the Royal Assent and the SLACI Act took effect from 2 December 2021.
25 November 2021	Department held a final virtual town hall concluding its consultation process on the risk management program rules.
24 November 2021	Freight and Logistics and Critical Hospitals Risk Management Program Rules Final Consultation Session
23 November 2021	Domain Name System Risk Management Program Rules Final Consultation Session
22 November 2021	Liquid fuels Risk Management Program Rules Final Consultation Session
19 November 2021	Data storage or processing final asset definition and Risk Management Program Rules Consultation Session.
17 November 2021	Broadcasting Risk Management Program Rules Consultation Session. Water and sewerage sector specific roundtable discussion.
16 November 2021	Financial services and markets (payment systems) Risk Management Program Rules Consultation Session.
15 November 2021	Data storage or processing sector specific Roundtable on asset definition

12 November 2021	Gas introduction to sector agnostic risk management program rules consultation session. Critical Hospitals discuss principles-based sector agnostic new approach consultation session.
11 November 2021	Electricity introduction to sector agnostic risk management program rules consultation session. Domain name system discuss principles-based sector agnostic new approach consultation session.
10 November 2021	Water and sewerage introduction to sector agnostic risk management program rules consultation session. Liquid fuels discuss principles-based sector agnostic new approach consultation session.
4 November 2021	Freight and logistics discuss principles-based sector agnostic new approach consultation session.
3 November 2021	Data storage or processing introduction to sector agnostic risk management program rules and asset definition consultation session.
29 October 2021	Financial services and markets (payment systems) discuss principles-based sector agnostic new approach consultation session.
28 October 2021	Broadcasting discuss principles-based sector agnostic new approach consultation session.
19 October 2021	Department held a town hall with all sectors on the updated co-design process, with the sector-agnostic risk management program rules.
18 October 2021	Department engaged with the Critical Infrastructure Advisory Committee(CIAC) on the outcomes of the PJCIS Advisory Report
6 October 2021	Department engaged with CIAC on the outcomes of the PJCIS Advisory Report
9 September 2021	Department commenced stage one of consultation, providing the CIAC and senior executives across Commonwealth Government a consultative draft of the refreshed CIRS
September 2021	Financial services and markets (payment systems) sector co-design commenced
August 2021	Data storage or processing, and water and sewerage sector co-design occurred between August and September.
14 May 2021	Rules for critical infrastructure thresholds and definitions submissions closed

23 April 2021	Department commenced a three-week public consultation process on the rules for critical infrastructure thresholds and definitions
April 2021	Department commenced co-design of sector-specific rules to underpin the risk management program. Electricity and gas sector co-design occurred between April and August
March 2021	Department conducted four town hall forums and seven workshops on the sector-agnostic governance rules
2 March 2021	Department commenced co-design to develop the rules underpinning the risk management component of the SLACI Bill with all 11 critical infrastructure sectors

Risk management program

The SLACIP Bill introduces Part 2A, which outlines the requirements for responsible entities of critical infrastructure assets to implement and maintain a risk management program. The purpose of a risk management program is for entities, so far as it is reasonably practicable, to minimise or eliminate risks arising from hazards in order to reduce the likelihood and severity of incidents in the most appropriate way for their own circumstances. Once implemented, the responsible entities will be required to comply with the risk management program, as well as maintain the risk management program and ensure that it remains up to date.

The risk management program will be underpinned by rules which will detail requirements for responsible entities to mitigate and minimise material risks that arise from hazards. Responsible entities must consider all hazards in their risk management program. These rules, developed with industry during an extensive consultation process from March 2021 to November 2021, will cover a range of specified hazards including, but not limited to:

- Physical and natural hazards
- Cyber and information hazards
- Personnel hazards
- Supply chain hazards

The Rules will provide a common baseline of minimum requirements for preparing for and managing risks across critical infrastructure assets. Many entities already have in place risk management programs that exceed those proposed by the risk management program rules, however, through the industry consultation process it has become apparent that many entities do not yet have in place even basic measures.

- The risk management program has been designed to establish safeguards where there is currently no other regulatory settings that achieve the same purpose. For example, those entities subject to the Australian Prudential Regulation Authority's (APRA's) prudential regulation or the defence industry security program will not (with some exceptions) be subject to the risk management program obligations as they already have existing and equivalent obligations in place.

On 1 February 2022, the Minister indicated her intent to apply the risk management program obligations to the following to the following critical infrastructure assets shortly after the passage through Parliament of the SLACIP Bill:

- Critical broadcasting assets

- Critical domain name systems
- Critical data storage or processing assets
- Critical hospitals
- Critical energy market operator assets
- Critical water and sewerage assets
- Critical electricity assets
- Critical gas assets
- Critical liquid fuel assets, and
- Critical financial market infrastructure assets that are specified payment systems operator assets.

The Minister also indicated her intent that risk management program obligations for critical food and grocery assets, critical freight services assets and critical freight infrastructure assets will not commence before 1 January 2023, recognising the particular challenges these sectors have faced during the pandemic.

The Minister is not able to make risk management program rules until the commencement of the provisions of the SLACIP Bill, which also require the Minister to undertake a mandatory consultation process of not less than 28 days prior to the creation of, or amendment to, such rules.

Regulation Impact Statements – the costings process

The Department has worked closely with industry experts and industry stakeholders from across the sectors who will be affected by the risk management program to understand the regulatory impact of this. When the rules are made, a RIS outlining the impact to industry which has been agreed to by the Office of Best Practice Regulation (OBPR) is required to be publically released.

Following in excess of 100 engagements with industry and State and Territory governments to consult on the risk management program rules and potential impact, the Department has commenced developing a draft RIS, based on the draft risk management program rules circulated for industry consultation. Analysis of costing figures received through the consultation process indicates that the potential cost of the required security uplift would be significantly outweighed by the net benefits to the economy as a whole.

The regulatory costs of the risk management program rules is minimal when compared to the damage to the economy if businesses underinvest in security and allow breaches to occur.

Analysis completed by KPMG for the electricity and gas sectors, shows a severe incident on the electricity sector could cost as much as $1.280 billion to the economy in direct and indirect costs. Consumers could also face flow-on price increases as a result of an incident.

A moderate incident to the electricity sector is estimated to cost approximately $850 million - more than triple the estimated $225.6 million annual ongoing cost of the mitigating measures.

A severe incident for the gas asset class could cost as much as $1.913 billion to the economy, as compared to estimated annual ongoing regulatory costs of $92.0 million for the sector.

- In addition to the costs to the economy, a disruption to these services would have a significant impact on Australia's social stability, defence, national security capabilities and could have an effect on the ability of the Australian government to govern effectively.

The risk management program reforms under the SLACIP Bill have a strong cost prevention element, ensuring that the net benefits to the economy as a whole outweigh the initial costs on industry.

In contrast, analysis of the average expected costs for responsible entities to implement, and maintain, the risk management program rules is currently an average one-off cost of $9.2 million followed by an average ongoing cost of $3.7 million per annum (p.a.), from the data provided so far. Although these figures are, in a relative sense, quite low, they do provide an insight into the current state of risk management amongst Australia's critical infrastructure entities and the need for further action to be taken.

Critical infrastructure asset	Costs ($ million)	
	Average one-off cost per entity (submissions)	Average annual ongoing cost per entity (submissions)
Critical electricity assets	10.2	5.6
Critical gas assets	10.4	2.1
Critical water assets	14.3	6.0
Critical data processing or storage assets	1.6	1.8
Critical broadcasting and domain name system assets	0.7	0.5
Critical financial market infrastructure assets (payment systems)	0.1	1.3
Critical liquid fuels assets	8.9	2.6
Critical hospitals	8.5	5.8
Critical energy market operator assets	28.1	7.3
Total average cost per entity	**9.2**	**3.7**

Source: Draft RIS for draft RMP rules dated February 2022.

Enhanced cyber security obligations and systems of national significance

The SLACIP Bill introduces Part 6A, which enables the Minister to privately declare a critical infrastructure asset to be a system of national significance. Before making such a declaration, the Minister is required to have regard to the asset's interdependencies with other critical infrastructure assets, and the consequences to Australia's national interest if the asset is significantly impacted.

The SLACIP Bill also introduces Part 2C, which provides for a series of enhanced cyber security obligations which may apply to the responsible entity for a system of national significance. There are four legislative mechanisms that implement the enhanced cyber security obligations outlined in the SLACIP Bill:

- statutory incident response planning obligations (Division 2);
- cyber security exercises (Division 3);
- vulnerability assessments (Division 4); and
- access to system information (Division 5).

Amendments arising out of consultation process

As at 0900 10 February 2022, the Department had received 70 submissions on the Exposure Draft of the SLACIP Bill, which closed for submissions on 1 February 2022. Various amendments have been made to the Exposure Draft of the SLACIP Bill arising out of this consultation process, these include:

- Amendments to the definitions of critical data storage or processing asset, critical education asset, higher education and research sector, critical gas asset, critical superannuation asset, critical telecommunications assets and critical food and grocery asset based on stakeholder feedback to ensure the appropriate capture of critical infrastructure entities.
- A rule-making power is being inserted into the definition of critical domain name system and critical data storage or processing asset to provide for these definitions to be refined by delegated legislation following the passage of the SLACIP Bill, if necessary.
- Expansion of the provision under which rules made for the purposes of requiring certain content in, or for certain content to be considered, in adopting a critical infrastructure risk management program. A risk management program may apply, adopt or incorporate additional documents as in force from time to time and may include additional documents such as the Essential Eight Maturity Model published by the Australian Signals Directorate.
- A new Part 2AA which recognises that an asset that is used in connection with a service that is 'certified strategic' under the Hosting Certification Framework administered by the Digital Transformation Agency is excluded from the obligation to establish, maintain, comply with etc. a risk management program.
- The practical expansion of the current scheme under the SOCI Act by which sensitive information in relation to critical infrastructure assets, defined as protected information, must not be accessed, recorded or disclosed unless an authorisation or exception applies (subject to a criminal offence with a penalty of up to 2 years imprisonment).

And some minor additional amendments to:

- clarify the scope of immunities that apply in relation to various obligations under the SOCI Act, including to expand the scope of the immunities to officers, employees and agents of related company groups and contracted service providers, consistent with PJCIS recommendation seven;
- amend the purpose of a critical infrastructure risk management program to minimising material risks and mitigating relevant impacts so far as it is reasonably practicable (minimising material risk was previously those minimisations that are reasonably possible, and mitigating relevant impacts was not limited);
- allow rules to be made to specify requirements of a risk management program to permit the conduct of background checks under the *AusCheck Act 2007* (AusCheck Act)(a relaxation of the language of the 2020 Bill that such rules may require background checks in specified circumstances), in response to stakeholder feedback on the proposed policy for such rules;

- ensure that the ability of risk management program rules to trigger a background check under the AusCheck Act provides for the types of checks to be specified in those rules (with the types of checks available being identity, immigration status, criminal history and security assessment), and to specify how an identity check may be conducted (either in-person or online);
- clarify that certain consultation periods that the Minister is required to provide to stakeholders can be 28 days or longer, not limited to strictly 28 days (consultation can be shorter in urgent circumstances for decisions to make an asset a critical infrastructure asset or a system of national significance, or in respect of Ministerial directions to prevent prejudice to security);
- make a requirement that the Secretary consider certain matters before making a number of administrative decisions, including decisions to impose enhanced cyber security obligations. The matters being the likely cost to the affected entity of complying with the decision, the reasonableness and proportionality of the decision, and any other matter the Secretary considers relevant;
- correct a reference to a provision of the *Australian Security Intelligence Organisation Act 1979* in the Criminal Code;
- make a technical clarification to the existing exemption from the definition of direct interest holder for moneylenders, in response to feedback received from the financial sector;
- insert a further exemption from the definition of direct interest holder in relation to a critical infrastructure asset that will apply to an entity if the entity provides a custodial or depository service, the entity holds an interest in the asset solely in the entity's capacity as the provider of the service, and holding the interest does not put the entity in a position to directly or indirectly influence or control the asset. 'Custodial or depository service' would be defined by reference to the *Corporations Act 2001*. This exemption is inserted in response to stakeholder feedback on the operation of the SOCI Act; and
- insert an additional exemption from the definition of direct interest holder in relation to a critical infrastructure asset that corresponds to the exemption for custodial or depository service providers above, but instead applies to a provider of a service specified by rules.

Clarification on amendments with respect to the AusCheck regime

The SLACI Bill 2020 originally proposed to permit the creation of rules that would 'require background checks of individuals to be conducted under the AusCheck scheme'. Messaging from industry in relation to the AusCheck regime has been consistent: industry is best placed to determine what the 'critical workers' in their business are that will require an AusCheck background check.

To respond to this feedback, the SLACIP Bill proposes to instead introduce the ability for rules to **enable** entities to access AusCheck background checks, where the business sees a need to mitigate a material risk of a relevant hazard occurring. This amendment is one of a suite of changes to the proposed risk management program regime, to further empower owners and operators of Australia's critical infrastructure to improve the resilience of their assets in a way that is suitable to their sector.

Clarification on 'essential groceries'

The SOCI Act defines a *critical food and grocery asset* as a network that is used for the distribution or supply of food or groceries and is owned or operated by a critical supermarket retailer, food wholesaler or grocery wholesaler. The *Security of Critical Infrastructure (Definitions) Rules 2021* define that a critical supermarket retailer includes Aldi, Coles and Woolworths, and that a critical grocery wholesaler includes MetCash.

In response to the Exposure Draft, the Department received feedback from the food and grocery sector that the inclusion of all 'food' and 'groceries' that are distributed or supplied by Aldi, Coles, Woolworths and MetCash would have the unintended consequence of capturing non-critical elements of the network.

To remedy this, the SLACIP Bill proposes to amend the definition of *critical food and grocery asset* to limit the definition to the network that supplies or distributes *essential* food and groceries. Essential groceries were considered by some members of the food and grocery sector to include fruit and vegetables, grains, dairy products, eggs, oils, tinned and dried produce, meat, fish, toiletries and over-the-counter health products.

This list has not been included in the legislation as what is considered 'essential' may evolve over time.

Educative focus for implementation under a reinvigorated TISN

A key focus of the Department moving forward will be a comprehensive program of engagement and education for critical infrastructure entities, to enable them to better meet these new obligations through the reinvigorated Trusted Information Sharing Network (TISN). This will ensure we can collectively and effectively strengthen the security and resilience of Australia's critical infrastructure.

- The critical infrastructure resilience strategy, regulatory settings provided by government, and strong industry-government partnerships are interconnected and are required to ensure the enhanced national security and resilience of critical infrastructure.

The TISN is Australia's primary engagement mechanism to enhance the security and resilience of critical infrastructure.

- The TISN aims to be a forum where members of the critical infrastructure community collaborate to strengthen the resilience of their organisations, sectors, and the overall network.
- It brings together critical infrastructure owners and operators, supply chain entities, peak bodies and all levels of government in partnership, and is a trusted, non-competitive environment for the critical infrastructure community to better plan, prepare, respond and recover in the face of all hazards.

The TISN is evolving as a flexible network that enables the critical infrastructure community members to collaborate more effectively between sectors on cross-sector and cross-network issues. Members have an increasing ability to self-select where they engage, focus on areas of interest and more easily collaborate with other members who are addressing similar issues. This better enables them to increase the resilience capability of their organisations

What's next?

The Cyber and Infrastructure Security Centre (CISC), within the Department, is committed to working in partnership with industry to protect Australia's critical infrastructure from all hazards. The CISC aims to deliver best practice regulation by leading proactive engagement with critical infrastructure providers to achieve outcomes that are beneficial to the Australian community, regulated entities and industry. In 2022, the CISC will continue to draw on the valuable knowledge of industry to inform our regulatory activities and improve our regulatory performance.

Consistent with the Committee's Advisory Report, the CISC has established several new teams and built upon our existing capability to provide technical support and advice to industry regarding the functions of the SOCI Act. In 2022, the CISC has also commenced publishing monthly Newsflash articles to provide information to industry on what is happening over the forward estimates, answer frequently asked questions and provide information on how industry can get involved.

Since the Committee released its advisory report, we have held hundreds of engagement sessions with critical infrastructure providers, other regulators and State and Territory partners on the SLACIP Bill and the proposed Risk Management Program. Throughout December 2021 and January 2022, the Minister for Home Affairs also held 9 Roundtables with industry representatives. The Secretary of the Department of Home

Affairs has also engaged with industry executives through a series of public information sessions. These engagements are ongoing.

Since passage of the SLACI Act, CISC has turned its mind to implementation and is working to increase existing industry engagement efforts to ensure industry understands what obligations they must meet under the new framework and to make it as easy as possible for industry to comply. To this end, CISC has published a number of Fact Sheets, held several town hall events, undertaken in excess of 100 engagements with industry and state and territory governments and released video messages updating industry on the specific measures within the reforms. Further guidance material to support implementation of the critical infrastructure security reforms is being developed in collaboration with industry and will released in the coming weeks and months. This will include a legislative handbook on the Serious Cyber Security Response Measures (also known as government assistance measures) and a supporting playbook that steps through how the government assistance measures will work in practice. Further industry guidance on the mandatory cyber security incident reporting regime will also be released jointly with the Australian Cyber Security Centre.

Should the Parliament pass the SLACIP Bill CISC will publish further industry guidance in the form of Fact Sheets on our website (CISC.gov.au) on the proposed measures (including the risk management program, Systems of National Significance (SoNS) and the enhanced cyber security obligations). CISC would look to hold additional public town hall events on both the broader SLACIP package as well as individual sessions on specific measures (i.e. targeted SoNS, ECSO and RMP town hall events). These efforts would build upon the existing engagement undertaken to date with industry on the Risk Management Program Rules which has seen CISC meet with over 2500 people, and over 100 engagements since October 2021.

LIN 22/018

Security of Critical Infrastructure (Critical infrastructure risk management program) Rules (LIN 22/018) 2022

I, Karen Andrews, Minister for Home Affairs, make this instrument under section 61 of the *Security of Critical Infrastructure Act 2018* (the ***Act***).

Dated 2022

DRAFT ONLY—NOT FOR SIGNATURE

Minister for Home Affairs

Contents

Part 1 Preliminary

1 Name

This instrument is the *Security of Critical Infrastructure (Critical infrastructure risk management program) Rules (LIN 22/018) 2022*.

2 Commencement

This instrument commences on the day after registration.

Note The Minister can only make this instrument after the requirements mentioned in section 30AL of the Act are completed.

3 Definitions

Note A number of phrases used in this instrument are defined in the Act, including:

(a) critical infrastructure asset;

(b) material risk;

(c) relevant impact;

(d) responsible entity.

In this instrument:

asset means a critical infrastructure asset.

critical component means an asset, part of an asset or system that <TBA>.

critical worker means an individual, including a position holder:

(a) who is an employee, intern, contractor or subcontractor of an entity; and

(b) whose absence or compromise would prevent the proper function of the asset or could cause significant damage to the asset, as assessed by the entity; and

(c) who has access to, or control and management of, a critical component of a Part 2A asset.

cyber and information security hazard includes where a person, whether authorised or not, improperly accesses or misuses information or computer systems about or related to the asset, or where such person by use of a computer system obtains unauthorised control of or access to any function which may impair the proper functioning of the asset.

entity means the responsible entity for a Part 2A asset.

high risk vendors has the meaning given by the *Cyber Supply Chain Risk Management* document published by the Australian Signals Directorate as in force from time to time.

Note Section 30ANA of the Act provides for the incorporation of this document as in force from time to time.

natural hazard includes a bushfire, flood, cyclone, storm, heatwave, earthquake, tsunami or health hazard (such as a pandemic).

Part 2A asset means a critical infrastructure asset to which Part 2A of the Act applies.

personnel hazard includes where a critical worker acts, through malice or negligence, to compromise the proper function of the asset or cause significant damage to the asset, as assessed by the entity, such as by causing a material risk to the asset.

physical security hazard includes the unauthorised access, interference, or control of critical assets, other than those covered by cyber and information security hazards, including where persons other than critical workers act, through malice or negligence, to compromise the proper function of the asset or cause significant damage to the asset, as assessed by the entity.

program means a critical infrastructure risk management program.

sensitive operational information includes any of the following for a Part 2A asset:

(a) layout diagrams;

(b) schematics;

(c) geospatial information;

(d) configuration information;

(e) operational constraints or tolerances information;

(f) data that a reasonable person would consider to be confidential or sensitive about the asset.

4 Material risk

For subsection 30AH(8) of the Act, material risks for an asset are taken to include a risk of the following relevant impacts occurring:

(a) an impairment of the asset that may prejudice the social or economic stability of Australia or its people, the defence of Australia or national security;

(b) a stoppage or major slowdown of the asset's function for an unmanageable period;

(c) a substantive loss of access to, or deliberate or accidental manipulation of, a critical component of the asset;

Example The position, navigation and timing systems affecting provision of service or functioning of the asset.

(d) an interference with the asset's operation technology or information communication technology essential to the functioning of the asset;

Example A Supervisory Control and Data Acquisition (SCADA) system.

(e) an impact resulting from the storage, transmission or processing of sensitive operational information outside Australia;

(f) an impact resulting from remote access to operational control or operational monitoring systems of the asset;

(g) any other material risks as identified by the entity that affect the functioning of the asset.

Part 2 Requirements etc. for a critical infrastructure risk management program

5 General

(1) For paragraph 30AH(1)(c) of the Act, an entity must establish and maintain in the entity's program:

(a) a process or system for identifying the operational context of each Part 2A asset for which the entity is responsible; and

(b) a principles-based risk identification process that the entity used to identify risks to the entity's Part 2A asset; and

(c) a risk management process or system that includes, for each material risk mentioned in section 5, a process or system to:

(i) consider the risk; and

(ii) as far as it is reasonably practicable to do so—minimise or eliminate the risk; and

(d) a process:

(i) for reviewing the program so that it complies with section 30AE of the Act; and

(ii) for keeping the program up to date so that it complies with section 30AF of the Act.

(2) In this subsection:

(a) for subsection 30AKA(1) of the Act—in deciding whether to adopt a program; and

(b) for subsection 30AKA(3) of the Act—in reviewing the program in accordance with section 30AE; and

(c) for subsection 30AKA(5) of the Act—in deciding whether to vary the program

an entity must have regard to the following matters:

(d) whether the program describes the outcome of the process or system mentioned in paragraph (1)(a);

(e) whether the program describes interdependencies between each of the entity's Part 2A assets and other critical infrastructure assets;

(f) whether the program identifies each position within the entity:

(i) that is responsible for developing and implementing the program; and

(ii) for each minimisation or elimination mentioned in subparagraph (1)(c)(ii)—that is responsible for developing and implementing the minimisation or elimination; and

(iii) for the processes mentioned in paragraph (1)(d)—that is responsible for reviewing the program or keeping the program up to date;

(g) whether the program contains the contact details for the positions described under paragraph (f);

(h) whether the program contains a risk management methodology or principles of a reasonable risk management methodology;

(i) whether the program describes the circumstances in which the entity will review the program (even if not required by section 30AE of the Act).

6 Cyber and information security hazards

(1) For paragraph 30AH(2)(c) of the Act, subsections (2) and (3) specify requirements.

(2) The entity must establish and maintain a process or system in the entity's program:

(a) to minimise or eliminate a material risk that a cyber and information security hazard for which there is a material risk that the hazard could have a relevant impact on the asset; and

(b) to mitigate the relevant impact of a cyber and information security hazard on the asset.

(3) Within 12 months of this instrument applying to an asset, an entity must comply with subsection (4) or (5).

Example If an asset becomes a Part 2A asset on 1 January 2023, the entity for the asset would need to comply with this subsection on or before 1 January 2024.

Note See also section 30AB of the Act and the *Security of Critical Infrastructure (Application) Rules 2022*.

(4) The entity must:

(a) comply with a framework contained in a document in an item in the following table as in force from time to time; and

(b) if a condition is mentioned in the item—comply with the condition.

Item	Document	Condition
1	Australian Standard *AS ISO/IEC 27001:2015*	
2	*Essential Eight Maturity Model* published by the Australian Signals Directorate	Required to meet maturity level one as indicated in the document
3	*Framework for Improving Critical Infrastructure Cybersecurity* published by the National Institute of Standards and Technology of the United States of America	
4	*Cybersecurity Capability Maturity Model* published by the Department of Energy of the United States of America	Required to meet Maturity Indicator Level 1 as indicated in the document
5	*The 2020-21 AESCSF Framework Core* published by Australian Energy Market Operator Limited (ACN 072 010 327)	Required to meet Security Profile 1 as indicated in the document

Note Sections 30AN and 30ANA of the Act provide for the incorporation of the documents mentioned in this subsection as in force from time to time.

(5) The entity must comply with a framework that is equivalent to a framework in a document mentioned in subsection (4), including a condition (if any) mentioned for that document.

(6) In this subsection:

(a) for subsection 30AKA(1) of the Act—in deciding whether to adopt a program; and

(b) for subsection 30AKA(3) of the Act—in reviewing the program in accordance with section 30AE; and

(c) for subsection 30AKA(5) of the Act—in deciding whether to vary the program

an entity must have regard to whether the cyber and information security risks, the occurrence of which could have a relevant impact on the asset, are described in the program.

7 Personnel hazards

(1) For paragraph 30AH(1)(c) of the Act, subsection (2) specifies a requirement in relation to a material risk that an occurrence of a personnel hazard could have a relevant impact on a Part 2A asset.

(2) Beginning on the compliance day, an entity must establish and maintain a process or system in the entity's program:

(a) to identify the entity's critical workers; and

(b) to assess, on an ongoing basis, the suitability of a critical worker to have access to the critical components of the asset; and

(c) minimise or eliminate material risks that negligent employees and malicious insiders may cause to the functioning of the asset; and

(d) minimise or eliminate material risks arising from the off-boarding process for outgoing employees and contractors.

(3) For paragraph (2)(b) and paragraph 30AH(4)(a) of the Act, the process and system for assessing the suitability of a critical worker to have access to the critical components of the asset may be a background check under the AusCheck scheme at regular intervals.

(4) For a background check of an individual permitted under subsection (3):

(a) for paragraph 30AH(4)(b) of the Act—the background check must include assessment of information relating to the matters mentioned in paragraphs 5(a), (b), (c) and (d) of the *AusCheck Act 2007*; and

(b) for paragraph 30AH(4)(c) of the Act, as the background check includes an assessment of information relating to the matter mentioned in paragraph 5(a) of the *AusCheck Act 2007*—the criteria against which that information must be assessed are the criteria specified in [TBD]; and

(c) for paragraph 30AH(4)(d) of the Act, as the background check includes an assessment of information relating to the matter mentioned in paragraph 5(d) of the *AusCheck Act 2007*—the assessment must consist of [an electronic identity verification check/an in person identity verification check/both an electronic identity verification check and an in person identity verification check].

Note In this exposure draft, subsections (3) and (4) are included to indicate how background checks under the AusCheck scheme will be enabled. The specific operation of the AusCheck scheme, including the criteria against which the background check will be conducted and the associated amendments required for the *AusCheck Regulations 2017* to enable such background checks, will be the subject of further consultation before being finalised.

(5) In this subsection:

(a) for subsection 30AKA(1) of the Act—in deciding whether to adopt a program; and

(b) for subsection 30AKA(3) of the Act—in reviewing the program in accordance with section 30AE; and

(c) for subsection 30AKA(5) of the Act—in deciding whether to vary the program

an entity must have regard to:

(d) whether the program lists the entity's critical workers; and

(e) whether the personnel risks, the occurrence of which could have a relevant impact on the asset, are described in the program.

8 Supply chain

(1) Subsection (2) specifies a requirement for paragraph 30AH(1)(c) of the Act.

(2) Beginning on the compliance day, the entity must establish and maintain in the entity's program a process or system that the entity uses to minimise or eliminate the material risk of, or mitigate, the relevant impact of:

(c) unauthorised access, interference or exploitation of the asset's supply chain; and

(d) misuse of privileged access to the asset by any provider in the supply chain; and

(e) disruption and sanctions of the asset due to an issue in the supply chain; and

(f) threats to people, assets, equipment, products, services, distribution and intellectual property within supply chains; and

(g) high risk vendors; and

(h) any failure or lowered capacity of other assets and entities in the entity's supply chain.

9 Physical security hazards and natural hazards

(1) Subsection (2) specifies a requirement for paragraph 30AH(1)(c) of the Act.

(2) Beginning on the compliance day, an entity must establish and maintain a process or system in the entity's program:

(a) to identify the parts of the asset that are critical to the functioning of the asset (the ***critical sites***); and

(b) to minimise or eliminate a material risk of, or mitigate, a relevant impact of a physical security hazard on a critical site; and

(c) to respond to incidents where unauthorised access to a critical site occurs; and

(d) to control access to critical sites, including restricting access to only those individuals who are critical workers or accompanied visitors; and

(e) to test that security arrangements for the asset are effective and appropriate to detect, delay, deter, respond to and recover from a breach in the arrangements; and

(f) to minimise or eliminate a material risk of, or mitigate, a relevant impact of a natural hazard on the asset.

(3) In this subsection:

(a) for subsection 30AKA(1) of the Act—in deciding whether to adopt a program; and

(b) for subsection 30AKA(3) of the Act—in reviewing the program in accordance with section 30AE; and

(c) for subsection 30AKA(5) of the Act—in deciding whether to vary the program

an entity must have regard to:

(d) whether the asset's critical sites are described in the program;

(e) whether the physical security hazards, the occurrence of which could have a relevant impact on a critical site, are described in the program;

(f) whether the security arrangements for the asset are described in the program;

(g) whether the natural hazards, the occurrence of which could have a relevant impact on the asset, are described in the program.

EXPOSURE DRAFT

EXPLANATORY STATEMENT

Issued by authority of the Minister for Home Affairs

Security of Critical Infrastructure Act 2018

Security of Critical Infrastructure (Critical infrastructure risk management program) Rules (LIN 22/018) 2022

1 The instrument, Departmental reference LIN 22/018, is made under section 61 of the *Security of Critical Infrastructure Act 2018* (the Act).

2 The instrument commences on the day after registration and is a legislative instrument for the *Legislation Act 2003* (the Legislation Act).

Purpose

3 Part 2A of the *Security of Critical Infrastructure Act 2018* (the Act) provides that the responsible entity for one or more critical infrastructure assets must have, and comply with, a critical infrastructure risk management program (a program). As outlined in paragraph 30AH(1)(b) of the Act, the purpose of a program is to:

- identify each hazard where there is a material risk that the occurrence of the hazard could have a relevant impact on the asset;
- so far as it is reasonably practicable to do so—minimise or eliminate any material risk of such a hazard occurring;
- so far as it is reasonably practicable to do so—mitigate the relevant impact of such a hazard on the asset.

4 Subsection 30AB(1) of the Act provides that Part 2A of the Act applies to a critical infrastructure asset if the asset is specified in the rules or, if a critical infrastructure asset is the subject of a declaration under section 51 of the Act, that declaration determines Part 2A applies to the asset.

5 Part 2 of the instrument sets out the requirements for paragraph 30AH(1)(c) of the Act that an entity must establish and maintain in the entity's program. Part 2 of the instrument also sets matters that must be considered by a responsible entity when adopting, reviewing and varying their critical infrastructure risk management program for section 30AKA of the Act.

6 In specifying the requirements in the rules, and in accordance with subsection 30AH(6), the Minister will have regard to:

- any existing regulatory system of the Commonwealth, a State or a Territory that imposes obligations on responsible entities (paragraph (a));
- the costs that are likely to be incurred by responsible entities in complying with the rules (paragraph (b));

- the reasonableness and proportionality of the requirements in the rules in relation to the purposes referred to in paragraph 30AH(1)(b) (paragraph (c)).

- such other matters (if any) as the Minister considers relevant (paragraph (d)).

Consultation

7 The Department of Home Affairs (the Department) engaged industry stakeholders from across sectors in a consultation process to design the rules underpinning the risk management program.

8 Under subsection 30AL(2) of the Act, the Minister must cause to be published a notice on the Department's website a draft of the proposed rules under section 30AH and invite submissions to the Minister. The Minister must also give a copy of the notice to each State and Territory First Minister. The Minister must consider any submissions received within the period specified in the notice.

9 A regulatory impact statement (RIS) is also being conducted in relation to the instrument. Whilst that document cannot be finalised until the Bill is passed and the rules can be made, a draft RIS informed by extensive consultation with stakeholders has been developed to identify the regulatory impact of these reforms. The RIS weighs the regulatory costs of the RMP rules against the damage to the economy if business underinvests in security and allows breaches to occur. The RIS clearly identifies that the regulatory costs of complying with the critical infrastructure risk management program obligation, as specified in rules, is minimal when compared to the damage to the economy if businesses underinvest in security and allow breaches to occur.

10 The RIS highlights that existing regulatory frameworks and market forces are insufficient to protect critical infrastructure against all hazard threats in a consistent and coordinated manner across critical infrastructure assets. Moreover, the likely benefits of the critical infrastructure risk management program obligation will be at least (and are expected to be more than) the costs of the regulation. This is primarily because the frequency and severity of all-hazard risks for critical infrastructure assets are growing and this increasing severity and frequency of incidents, particularly in the context of growing cybersecurity incidents, represents a risk to the whole economy.

11 Detailed economic analysis of costing figures received through the RIS indicates that the potential cost of the required security uplift would be significantly outweighed by the net benefits to the economy as a whole.

Details of the instrument

12 Details of the instrument are set out in **Attachment A**

Parliamentary scrutiny etc.

13 The instrument is subject to disallowance under section 42 of the Legislation Act and the final explanatory statement for the instrument will contain a Statement of Compatibility with Human Rights in accordance with the *Parliamentary Scrutiny (Human Rights) Act 2011*.

14 The instrument will be made by the Minister for Home Affairs in accordance with the requirements of section 30AL.

Attachment A

Details of the *Security of Critical Infrastructure (Critical infrastructure risk management program) Rules (LIN 22/018) 2022*

Section 1 Name

This section provides that the name of the instrument is the *Security of Critical Infrastructure (Risk management program) Rules 2022* (the instrument).

Section 2 Commencement

This section provides that the instrument commences on the day after registration on the Federal Register of Legislation.

Who will the rules apply to?

As outlined in the Explanatory Memorandum to the Security Legislation Amendment (Critical Infrastructure) Bill 2022 (the Explanatory Memorandum), it is proposed that the Part 2A of the Act will, shortly after commencement of the SLACIP Bill, apply to:

- critical electricity assets;
- critical energy market operator assets;
- critical gas assets;
- critical liquid fuels assets;
- critical water and sewerage assets;
- critical financial market infrastructure assets that are a critical payment system (other critical financial market infrastructure assets will not be captured);
- critical data storage or processing assets;
- critical hospital assets;
- critical domain name system assets; and
- critical broadcasting assets.

As also outlined in the Explanatory Memorandum, it is proposed that Part 2A of the Act will additionally apply to critical freight services assets, critical freight infrastructure assets and critical food and grocery assets. Given current supply chain impacts arising from the COVID-19 pandemic, the critical infrastructure risk management obligation will be delayed until at least 1 January 2023.

This will be facilitated by rules made under proposed section 30AB of the SOCI Act (the section 30AB rule), which are proposed to provide that the abovementioned assets will be assets to which Part 2A applies:

- if the asset is a critical infrastructure asset on or before the commencement of the section 30AB rule—six months after the rule commences; or

- if the asset becomes a critical infrastructure asset after the commencement of the section 30AB rule—six months after the asset becomes a critical infrastructure asset.

This means that the requirements and matters that must be regarded specified in this instrument will not need to be complied with until this date, except for the requirement in subsection 6(2) of the instrument for specified cyber security frameworks, for which an additional 12 months is provided before the responsible entity needs to be compliant.

Section 3 Definitions

This section sets out definitions of terms used in the instrument.

Section 4 Material risk

Section 5 of the instrument sets out that, under subsection 30AH(8) of the Act, a 'material risk' is taken to include any risk of the following impacts:

- an impairment of the asset that may prejudice the social or economic stability of Australia or its people, the defence of Australia or the national security of Australia (paragraph (a));

- any hazard that would cause the stoppage or major slowdown of the asset's functioning for an unmanageable period (paragraph (b));

- the substantive loss of access to or deliberate or accidental manipulation of a component of the asset (paragraph (c));

- interference with the asset's operating technology or information communication technology essential to the functioning of the asset (paragraph (d));

- the relevant impact on the asset resulting from the storage, transmission or processing of sensitive operational information outside Australia (paragraph (e)) – the term *sensitive operational information* is further defined in section 3;

- the relevant impact on the asset resulting from remote access to operational control or operational monitoring systems of the asset (paragraph (f));

- any other material risks as identified by the entity that affect the functioning of the asset (paragraph (g)).

Part 2 Requirements etc. for a critical infrastructure risk management program

Section 5 General

Subsection 5(1) of the instrument specifies general requirements that an entity must comply with when establishing and maintaining a critical infrastructure risk management program under paragraph 30AH(1)(c) of the Act. The requirements are that the program contains:

- a process or system for identifying the operational context of each Part 2A asset for which an entity is responsible (paragraph (a));
- a principles-based risk identification process used to identify risks to the entity's Part 2A assets (paragraph (b));
- a risk management process or system that includes, for each material risk, a process or system to consider the risk and minimise or eliminate the risk (paragraph (c));
- a process for reviewing the risk management program so that it remains compliant with the requirement to review the program in section 30AE of the Act (subparagraph (d)(i));
- a process for keeping the risk management program up to date so that it remains compliant with requirement to keep the program up to date under section 30AF of the Act (subparagraph (d)(ii)).

Subsection 5(2) of the instrument specifies that, in deciding to adopt, review or vary a risk management program, for section 30AKA of the Act an entity must have regard to the matters mentioned in paragraphs (d) to (i).

Describing outcomes and interdependencies

Paragraphs 5(2)(d) and (e) of the instrument provide that the entity must have regard to:

- whether the program describes the outcomes of the process or system under section 5(1)(a) for identifying the operational context of their Part 2A assets (paragraph (d)); and
- whether the program describes any interdependencies between their Part 2A assets critical and other critical infrastructure assets (paragraph (e)).

The purpose of paragraphs 5(2)(d) and (e) is to ensure that the program sets out the entity's process for identifying risk relating to critical infrastructure assets for which it is responsible. This includes matters such as how the program will function on a daily basis, the kinds of relevant impacts that are most applicable to those assets, and interaction with other critical infrastructure assets.

Positions responsible for risk management

Paragraph 5(2)(f) of the instrument provides that the entity must have regard to whether the program the program identifies:

- each position within the entity that is responsible for developing and implementing the program (subparagraph (i));

- each position within the entity that is responsible for developing and implementing the minimisation, elimination or mitigation, as referred to in subparagraph 5(1)(c)(ii) of the instrument (subparagraphs (ii)-(iii));

- each position within the entity responsible for reviewing the program or keeping the program up to date, as referred to in paragraph 5(1)(c) of the instrument (subparagraph (iv));

Under paragraph 5(2)(g), the entity must have regard to whether the program include contact details of the positions referred to in paragraph 5(2)(f).

The purpose of paragraphs 5(2)(f) and (g) is to ensure that details of the positions (and their contact details) responsible for developing and implementing a program, and eliminating or mitigating risks, are set out in the program.

Risk management methodology

Paragraph 5(2)(h) of the instrument provides that the entity must have regard to whether the program describes a reasonable risk management methodology or principles of a reasonable risk management methodology.

The purpose of this provision is to ensure that the program contains a risk management methodology, or principles of risk management methodology. This will be an overview of the process of risk management methodology that the entity uses. Generally it should cover how risks should be identified, the methods that should be used, the people who should be involved and other methodological issues.

Review of the program

Paragraph 5(2)(i) of the instrument provides that the entity must have regard to whether the program describes the circumstances in which the entity will review the program (even if not required to do so by section 30AE of the Act). Section 30AE of the Act requires a responsible entity for a critical infrastructure asset to review its program on a regular basis.

The purpose of paragraph 5(2)(i) is to ensure that the program describes how the entity will regularly review its program in accordance with section 30AE of the Act.

Section 6 Cyber and information security

Section 6 of the instrument sets out the cyber and information security hazard requirements that an entity's risk management program must comply with under the Act.

Subsection 6(1) provides that subsections (2) and (3) specify requirements for paragraph 30AH(1)(c) of the Act.

Subsection 6(2) requires that the entity must establish and maintain a process or system in the entity's critical infrastructure risk management program:

- to minimise or eliminate a material risk of a hazard that could have a relevant impact on the cyber and information security of the asset (paragraph (a)); and

- to mitigate the relevant impact of a hazard on the cyber and information security of the asset (paragraph (b)).

The purpose of subsection 6(2) is to require an entity's program to have the required level of preparedness to mitigate cyber security threats to their critical infrastructure assets.

Subsection 6(3) provides that, within 12 months of the compliance day, an entity must comply with either subsection 6(4) or 6(5).

Paragraph 6(4)(a) of the instrument requires that the entity's program must comply with one of the frameworks contained in the documents as listed in the table as in force from time to time. Paragraph 7(4)(b) requires that if there is a condition mentioned in the item associated with the document, the entity must also comply with the condition. The documents listed in the table are as follows:

- Australian Standard *AS ISO/IEC 27001:2015* (item 1);
- the *Essential Eight Maturity Model*, published by the Australian Signals Directorate, with the condition that the entity is required to meet maturity level one (item 2);
- *Framework for Improving Critical Infrastructure Cybersecurity* published by the National Institute of Standards and Technology of the United States of America (item 3);
- *Cybersecurity Capability Maturity Model* published by the Department of Energy of the United States of America, with the condition that the entity is required to meet Maturity Indicator Level 1 (item 4); and
- *The 2020-21 AESCSF Framework Core* published by Australian Energy Market Operator Limited (ACN 072 010 327), with the requirement that the entity is required to meet Security Profile 1 (item 5).

A note to this provision indicates that:

- the document listed in item 1 of the table, as an Australian Standard, can be incorporated as in force from time to time as provided for in subsection 30AN(3) of the Act; and
- the other documents (items 2-5) are defined to be 'relevant documents' in subsection 30ANA(2) of the Act, and therefore can be incorporated as in force from time to time as provided for in subsection 30ANA(1).

Under subsection 6(5), an entity must alternatively comply with a framework that is equivalent to a framework mentioned in a document mentioned in subsection 6(4). The purpose of this provision is to provide industry with the necessary flexibility to comply with their statutory obligations by recognising alternative cyber security frameworks that achieve the desired uplift in security and resilience of the entity's Part 2A asset.

Subsection 6(6) sets out a matters an entity must have regard to when adopting, reviewing or varying a critical infrastructure risk management program for section 30AKA of the Act. Under this provision, the entity must have regard to whether the cyber and information security risks, the occurrence of which could have a relevant impact on the asset, are described in the program. 'Cyber and information security risk' is defined in section 3 of the instrument.

The matter that the entity must have regard to is whether the cyber and information security risks, the occurrence of which could have a relevant impact on the asset, are described in the program.

Section 7 Personnel hazards

Subsection 7(1) of the instrument provides that subsection 7(2) specifies the personnel hazard requirements that a critical infrastructure risk management program must comply with under paragraph 30AH(1)(c) of the Act.

Subsection 7(2) provides that an entity must establish and maintain a process or system in the entity's program:

- to identify the entity's critical workers (paragraph (a)). 'Critical worker' is defined in section 3 of the instrument;
- to assess, on an ongoing basis, the suitability of a critical worker to have access to the critical components of the asset (paragraph (b));
- to minimise or eliminate material risks that negligent employees and malicious insiders may cause to the functioning of the asset (paragraph (c));
- to minimise or eliminate material risks arising from the off-boarding process for outgoing employees and contractors (paragraph (d)).

Subsection 7(3) provides that the process or system for considering the suitability of a critical worker to have access to critical components of an asset may be a background check under the AusCheck scheme.

Subsection 7(4) provides requirements for a background check of a critical worker under subsection 8(3). The requirements are that the background check must:

- provide that such a background check must include assessment of information relating to one or more of the matters mentioned in paragraphs 5(a), (b), (c) or (d) of the *AusCheck Act 2007* (AusCheck Act)—relating respectively to a criminal history check, an ASIO security assessment, an immigration status check and an identity check (paragraph (a));
- provide that if a background check includes a criminal history check pursuant to paragraph 5(a) of the AusCheck Act—the criteria must be assessed against criteria that will be set out in the instrument at a later date (paragraph (b)); and
- if the background check includes an identity check pursuant to paragraph 5(d) of the AusCheck Act—provide for how that check will be conducted, as an electronic identity verification check, in person identity verification check, or both (paragraph (c)).

A note to this provision for the purpose of the exposure draft indicates that subsections (3) and (4) have been included in the instrument to indicate how background checks under the AusCheck scheme will be enabled. The specific operation of the AusCheck scheme, including the criteria against which the background check will be conducted and the associated amendments required for the *AusCheck Regulations 2017* to enable such background checks, will be the subject of further consultation before being finalised

Subsection 7(5) sets out the matters an entity must have regard to when adopting, reviewing or varying a critical infrastructure risk management program for section 30AKA of the Act.

Under this provision, the entity must have regard to:

- whether the program lists the entity's critical workers (paragraph (d)); and
- whether the personnel risks, the occurrence of which could have a relevant impact on the asset, are described in the program (paragraph (e)).

Section 8 Supply chain

Section 8 sets out the supply chain hazard requirements that an entity's critical infrastructure risk management program must comply with under paragraph 30AH(1)(c) of the Act (see subsection (1)).

Subsection 8(2) provides that an entity must establish and maintain in its program a process or system used to minimise or eliminate the material risk of, or mitigate, the relevant impact of:

- unauthorised access, interference or exploitation of the asset's supply chain (paragraph (a));
- misuse of privileged access to the asset by any provider in the supply chain (paragraph (b));
- disruption and sanctions of the asset due to an issue in the supply chain (paragraph (c));
- threats to people, assets, equipment, products, services, distribution and intellectual property within supply chains (paragraph (d));
- high risk vendors (paragraph (e)); and
- any failure or lowered capacity of other assets and entities in the entity's supply chain (paragraph (f)).

The purpose of subsection 8(2) is to ensure that an entity's program contains necessary detail regarding the steps they are taking to secure the supply chains necessary for the operational continuity of their critical infrastructure asset, as well as the practices they are implementing to continually monitor and enhance their supply chain security.

Section 9 Physical security hazards and natural hazards

Section 9 of the instrument sets out the physical and natural hazard requirements that an entity's critical infrastructure risk management program must comply with under paragraph 30AH(1)(c) of the Act (see subsection (1)).

Subsection 9(2) provides that an entity must establish and maintain a process or system in the entity's program:

- to identify the parts of the asset that are critical to the functioning of the asset (the critical sites) (paragraph (a)); and
- to minimise or eliminate a material risk of, or mitigate, a relevant impact of a physical hazard on a critical site (paragraph (b)); and
- to respond to incidents where unauthorised access to a critical site occurs (paragraph (c)); and

- to control access to critical sites, including restricting access to only those individuals who are critical workers or accompanied visitors (paragraph (d)); and

- to test that security arrangements for the asset are effective and appropriate to detect, delay, deter, respond to and recover from a breach in the arrangements (paragraph (e)); and

- to minimise or eliminate a material risk of, or mitigate, a relevant impact of a natural hazard on the asset (paragraph (f)).

The purpose of subsection 9(2) is to ensure that an entity's program contains necessary detail regarding their processes for managing and mitigating a variety of physical and natural hazards to their critical infrastructure assets, as well as recovery procedures for circumstances where a natural hazard disrupts the business operations of the asset.

Subsection 9(3) sets out the matters an entity must have regard to when adopting, reviewing or varying a critical infrastructure risk management program for section 30AKA of the Act.

The matters that the entity must have regard to are:

- whether the asset's critical sites are described in the program (paragraph (d));

- whether the physical hazards, the occurrence of which could have a relevant impact on a critical site, are described in the program (paragraph (e));

- whether the security arrangements for the asset are described in the program (paragraph (f));

- whether the natural hazards, the occurrence of which could have a relevant impact on the asset, are described in the program (paragraph (g)).

Attachment B - Comparison of provisions between SLACI 2020 and SLACIP 2022

Original SLACI Bill 2020	Exposure Draft of the SLACP Bill 2022	SLACIP Bill 2022 as introduced
Definitions		
Critical education asset Introduced the definition as a university that is owned or operated by an entity that is registered in the Australian university category of the National Register of Higher Education Providers ("University").	***Critical education asset*** No changes. *Rationale* **Recommendation 7** of the PJCIS Report, paragraph 3.49, first dot point requested that any definitions introduced by SLACI 2021 that require modification, clarification or reconsideration as to scope be amended by SLACIP 2022. No changes were identified as required to this definition.	***Critical education asset*** Narrows the scope of the definition to assets owned by an entity that operates a University, and where those assets are used in connection with research for national security, defence or critical infrastructure and where funded by the Commonwealth. *Rationale* The Department received feedback from the higher education and research sector to amend the existing asset definition to ensure that only ***critical*** elements of universities were captured.
Higher education and research sector Introduced the definition as involving: • a higher education provider, or • undertaking research that is supported financially by the Commonwealth or relevant to a critical infrastructure sector.	**Higher education and research sector** Significantly narrowed the scope of the definition to programs of research that are: • supported financially by the Commonwealth, or • is critical to a critical infrastructure sector, national security or the defence of Australia. *Rationale* These amendments contributed to implementing **Recommendation 7** of the PJCIS Report as a definition that has been clearly identified as requiring modification. The higher education and research sector, in their submissions and during hearings, advised that the sector definition was too broad and required a narrowing of scope and additional clarity.	**Higher education and research sector** Narrows the scope of the definition even further to programs of research that are both: • supported financially by the Commonwealth, **and** • are critical to a critical infrastructure sector, national security or the defence of Australia. *Rationale* The Department received additional feedback from the higher education and research sector on the proposed definition to further narrow the scope of the definition.

Original SLACI Bill 2020	Exposure Draft of the SLACP Bill 2022	SLACIP Bill 2022 as introduced
Data storage or processing service/asset Introduced the asset definition. The *data storage or processing service* definition is a key element of the *data storage or processing asset* definition. These two definitions work together to fully define the assets that are captured within the data storage or processing sector.	***Data storage or processing service/asset*** Amended the definition to: • Remove the requirement that the service be 'wholly or primarily' provided based on certain criteria to ensure that the definition is sufficiently broad • excludes telecommunications assets that may be incidentally captured due to potential overlap between the asset definitions to avoid unintended duplication of regulation *Rationale* These amendments contributed to implementing **Recommendation 7** of the PJCIS Report as a definition that has been clearly identified as requiring modification. The data storage or processing sector, in their submissions and during hearings, advised that the sector definition was unclear, may overlap with other asset definitions and required additional clarity.	***Data storage or processing service/asset*** Amends the definition to: • Re-introduce the requirement that the service be wholly or primarily provided on the basis of certain criteria, to narrow the scope of the definition • further excludes assets to any critical infrastructure asset, not just telecommunications assets, that may be incidentally captured by the asset definition • duplicating the 'business critical data' requirement to Government data to narrow the definition, and • adds a rulemaking power to ensure the service definition can remain current in the rapidly evolving sector. *Rationale* The Department received additional feedback from the data storage or processing sector to further narrow the scope of the definition and to provide additional clarity to industry. Many of these amendments, including adding the 'business critical data' requirement for Government data and re-introducing the 'wholly or primarily' requirement, are made as a direct implementation of industry feedback.

Original SLACI Bill 2020	Exposure Draft of the SLACP Bill 2022	SLACIP Bill 2022 as introduced
Critical superannuation asset Introduced the asset definition. Introduced the responsible entity for the asset as a *registrable superannuation entity*.	***Critical superannuation asset*** Amended the responsible entity for the asset to the RSE Licensee. *Rationale* These amendments contributed to implementing **Recommendation 7** of the PJCIS Report as a definition that has been clearly identified as requiring modification. The Department received feedback from a superannuation entity that advised the RSE Licensee was the more appropriate responsible entity for this class of asset.	***Critical superannuation asset*** No changes.
Critical gas asset No changes to the original SOCI Act definition.	***Critical gas asset*** No changes. *Rationale* No changes were identified, at this stage, as required to this definition.	***Critical gas asset*** Amends the definition of 'gas transmission pipeline' from the original SOCI Act to include a control rooms and similar to ensure that entities can be required to look at all points of vulnerability, not just physical threats to the pipeline. *Rationale* This amendment was identified internally as requiring modification.

Original SLACI Bill 2020	Exposure Draft of the SLACP Bill 2022	SLACIP Bill 2022 as introduced
Critical domain name system Introduced the asset definition. Identified the asset as a *critical domain name system* where it is, among other things, used in connection with the administration of an Australian domain name system.	***Critical domain name system*** Inserted a rule making power to further define the specific assets that are critical to the administration of an Australian Domain Name system. *Rationale* These amendments contributed to implementing **Recommendation 7** of the PJCIS Report as a definition that has been clearly identified as requiring modification. The Department received feedback from auDA that further clarity was required on this definition. Due to the complexity of the systems involved, a rule making power was identified as the clearest way to future-proof the definition. The Department will continue to consult with auDA through the development of any rules.	***Critical domain name system*** No changes.
Critical food and grocery asset Introduced the asset definition. Identified the asset where it is a network that is, among other things, used for the distribution or supply of food or groceries.	***Critical food and grocery asset*** No changes. *Rationale* No changes were identified as required to this definition.	***Critical food and grocery asset*** Significantly narrows the scope of the definition to a network that is, among other things, used for the distribution or supply of **essential** food and groceries. *Rationale* The Department received feedback that the asset definition should only capture the elements of distribution or supply networks that involve **essential** food and groceries, rather than all food and groceries.

Original SLACI Bill 2020	Exposure Draft of the SLACP Bill 2022	SLACIP Bill 2022 as introduced
Critical telecommunications asset Identified the asset as: • a telecommunications network that is owned or operated by a carrier and used to supply a carriage service, or • a telecommunications network **or any other asset** that is owned or operated by a **carriage service provider** and used in connection with the supply or a carriage service.	***Critical telecommunications asset*** No changes. *Rationale* Submissions from the telecommunications sector identified concerns with the breadth of the definition. Due to the forthcoming PJCIS review into the TSSR and the lack of intention to 'switch on' any obligations under the SOCI Act, no changes were identified as required to this definition.	***Critical telecommunications asset*** Significantly narrows the scope of the definition to: • a telecommunications network that is owned or operated by a carrier or carriage service provider, and used to supply a carriage service provider, or • **a facility** owned or operated by a carrier or carriage service provider, and used to supply a carriage service. *Rationale* The Department received significant feedback from the telecommunications sector, as well as other sectors, to narrow the scope of the definition.
Direct interest holder No amendments were proposed to the SOCI Act definition of *direct interest holder*.	***Direct interest holder*** No changes. *Rationale* While changes were identified as required, consultation was ongoing with relevant Commonwealth line agencies to ensure correct implementation of any amendments.	***Direct interest holder*** These amendments: • correct the moneylender exemption so that there is less legal risk that the exemption doesn't operate as intended. • insert a new exemption for custodial or depository services in line with moneylenders • inserts a new rule making power to specify additional types of entities that are exempt from the definition. *Rationale* These amendments ensure that businesses that may technically hold a legal interest in a critical infrastructure asset, but do not have any actual

Original SLACI Bill 2020	Exposure Draft of the SLACP Bill 2022	SLACIP Bill 2022 as introduced
		influence or control over that asset are not captured by the definition. The Department received feedback from the financial services and markets sector that: • the moneylender exemption may not work, and • additional exemptions were required for the same reason that the moneylender exemption was introduced in the first place.

Original SLACI Bill 2020	Exposure Draft of the SLACP Bill 2022	SLACIP Bill 2022 as introduced
Risk management program		
Risk management program (Part 2A) Introduced the risk management program regime.	**Risk management program (Part 2A)** Amended Part 2A to lower the requirement for "possible" mitigation of hazards to "practicable" mitigation of hazards, which was identified as a more reasonable standard. *Rationale* These amendments contribute to implementing **Recommendation 8** of the PJCIS Report by responding to extensive consultation with all critical infrastructure sectors. Most of this feedback was implemented through the development of rules that will underpin the Risk Management Program.	**Risk management program (Part 2A)** The amendments to Part 2A include: • recognition of the Digital Transformation Agency's (DTA) Hosting Certification Framework (HCF)—new Part 2AA which sets out the certified entity's minimal reporting requirements, instead of the regular Part 2A requirements • a capacity for the Minister to recognise other existing risk mitigation frameworks in the same manner as the DTA's HCF • a list of standards and risk management frameworks that are considered 'relevant documents', including international standards, and may be used for the purposes of an entity's risk management program • more clarity on which background checks under the AusCheck Act regime can be leveraged and amending language so rules do not 'require' background checks in specified circumstances. *Rationale* The Department received significant feedback from industry to provide additional clarity and certainty to industry on the requirements under the program. These amendments respond to this feedback by clarifying that existing standards, particularly international standards, are recognised. Further, the DTA's HCF amendments respond directly to feedback from the data storage or processing sector.

Original SLACI Bill 2020	Exposure Draft of the SLACP Bill 2022	SLACIP Bill 2022 as introduced
Enhanced Cyber Security Obligations for systems of national significance		
Enhanced cyber security obligations Introduced the enhanced cyber security obligations regime.	**Enhanced cyber security obligations** No changes.	**Enhanced cyber security obligations** When making a decision to impose enhanced cyber security obligations on an entity, the amendments insert requirements for the Secretary to consider a number of factors before making the decision, including: • the likely cost to the affected entity of complying with the obligations • the reasonableness and proportionality of the decision, and • any other matter the Secretary considers relevant. *Rationale* These amendments respond to both Government and industry feedback to insert additional administrative safeguards for decisions made to impose cyber security obligations.

Original SLACI Bill 2020	Exposure Draft of the SLACP Bill 2022	SLACIP Bill 2022 as introduced
Protected information: secrecy and disclosure		
Information sharing and authorised disclosure The original amendments to the protected information provisions only expanded the definition of protected information to the information that was generated under Part 2A (risk management programs), Part 2C (enhanced cyber security obligations), Part 3A (responding to serious cyber security incidents) and Part 6A (declarations of systems of national significance).	**Information sharing and authorised disclosure** These amendments introduce a variety of new circumstances where the disclosure of protected information will be authorised, including: • for the purpose of disclosing information about the entity to its relevant Commonwealth, State or Territory government regulator for the purposes of enabling or assisting the regulator to exercise their powers or functions • enabling entities to disclose specified less sensitive protected information to any recipient • enabling entities to disclose specified more sensitive protected information that relates to the entity when the Secretary provides written consent. • These amendments also adjust the exceptions to the offence of unauthorised disclosure of protected information, including: • to remove the ability for an entity to disclose its own information for any reason • to permit disclosure to an Ombudsman official. *Rationale* These amendments contribute to implementing **Recommendation 7, para 3.49, dot point 6** of the PJCIS Report. One of the key concerns raised by State and Territory jurisdictions were barriers to sharing protected information, especially for entities to share the information for securing funding from relevant State or Territory regulators.	**Information sharing and authorised disclosure** These amendments introduce a variety of new circumstances where the disclosure of protected information will be authorised, including: • the Secretary may disclose protected information to a Commonwealth Ombudsman official • the Secretary may disclose protected information for the purpose of developing amendments or new rules to the SOCI Act. *Rationale* These amendments are based on feedback as part of the Commonwealth scrutiny process to ensure that adequate provision is made for information sharing with the Commonwealth Ombudsman. Furthermore, these amendments permit the use of protected information to further refine and develop the SOCI Act and rules.

Original SLACI Bill 2020	Exposure Draft of the SLACP Bill 2022	SLACIP Bill 2022 as introduced
Immunities		
Protection from civil liability	**Protection from civil liability** A variety of amendments were introduced to all of the immunity provisions in the legislation to expand the scope of the immunities to a broader class of individuals in a broader class of circumstances. *Rationale* These amendments contribute to implementing **Recommendation 9** of the PJCIS Report. These amendments are in direct response to feedback provided by the Law Council of Australia and the Business Council of Australia, requesting strengthened protection for a broader class of entities that may be required to comply with directions under the SOCI Act.	**Protection from civil liability** No changes.
Other amendments		
	Other amendments included a minor technical amendment to the criminal code to correct a reference to the definition of a 'computer'.	Other amendments included amendments to Parts 2, 2A and 2C to ensure that consultation can extend longer than 28 days at the Minister's discretion. The consultation may still not be shorter than 28 days. *Rationale* These amendments ensure that consultation can extend longer than 28 days if required. This amendment generally responds to the request from all industry sectors for greater consultation on the reforms.