Australian Government
Department of Home Affairs

CYBER AND INFRASTRUCTURE SECURITY CENTRE

Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022

Explanatory Document

December 2021

The exposure draft consultation will run between December 2021 and 1 February 2022.

Submissions can be provided to the Cyber and Infrastructure Security Centre (CISC) at the Department of Home Affairs to CI.Reforms@homeaffairs.gov.au until 11:59pm on Tuesday, 1 February 2022.

You can find more information on the exposure draft consultation process on the CISC website at www.cisc.gov.au.

GLOSSARY

Advisory Report – the Parliamentary Joint Committee on Intelligence and Security Advisory Report on the Security Legislation Amendment (Critical Infrastructure) Bill 2020 and Statutory Review of the Security of Critical Infrastructure Act 2018

ASIC – Aviation Security Identification Card

CESAR – Cyber Enhanced Situational and Response

DISP – Defence Industry Security Program

Exposure Draft – the Exposure Draft of the Security Legislation Amendment (Critical Infrastructure Protection) Bill 2021.

Home Affairs – Department of Home Affairs

MNE – Major National Events

MSIC – Maritime Security Identification Card

NHS – National Health Security

PJCIS – Parliamentary Joint Committee on Intelligence and Security

Privacy Act – *Privacy Act 1988*

SOCI Act – *Security of Critical Infrastructure Act 2018*

SLACI Bill 2020 – Security Legislation Amendment (Critical Infrastructure) Bill 2020.

SLACI Bill 2021– Security Legislation Amendment (Critical Infrastructure) Bill 2021.

SLACIP Bill 2022 – Security Legislation Amendment (Critical Infrastructure Protection) Bill 2021.

SECURITY LEGISLATION AMENDMENT (CRITICAL INFRASTRUCTURE PROTECTION) BILL 2022

GENERAL OUTLINE

1. The Australian Government is committed to protecting the essential services all Australians rely on by uplifting the security and resilience of our critical infrastructure. As the threats and risks to Australia's critical infrastructure evolve, so too must our approach to ensuring the ongoing security and resilience of these assets and the essential services they deliver.

2. The critical infrastructure that Australians rely on every day is increasingly interconnected and interdependent, delivering both efficiencies and economic benefits to operations. However, connectivity without proper safeguards creates vulnerabilities that can deliberately or inadvertently cause disruption and result in cascading consequences across our economy, security and sovereignty.

3. Threats ranging from natural hazards (including weather events) to human induced threats (including interference, cyber attacks, espionage, chemical or oil spills, and trusted insiders) all have the potential to significantly disrupt critical infrastructure. Incidents such as compromises of the Australian parliamentary network, university networks and key corporate entities, natural disasters and the impacts of COVID-19 illustrate that threats to the operation of Australia's critical infrastructure assets continue to be significant. Further, the interconnected nature of our critical infrastructure means that compromise of one essential function can have a domino effect that degrades or disrupts others.

4. The consequences of a prolonged and widespread failure in the energy sector, for example, could be catastrophic to our economy, security and sovereignty, as well as the Australian way of life, causing:

    - shortages or destruction of essential medical supplies;
    - instability in the supply of essential food and groceries;
    - impacts to water supply and sanitation;
    - impacts to telecommunications networks that are dependent on electricity;
    - the inability of Australians to communicate easily with family and loved ones;
    - disruptions to transport, traffic management systems and fuel;
    - reduced services or shutdown of the banking, finance and retail sectors; and the inability for businesses and governments to function.

5. While Australia has not suffered a widespread debilitating catastrophic attack on critical infrastructure, we are not immune. Cyber attacks have repeated targeted Australian critical infrastructure for many years now. More recently, the Australian Cyber Security Centre reports that one quarter of reported cyber incidents in 2020/21 were associated with Australia's critical infrastructure or essential services. These cyber incidents have resulted in significant targeting, both domestically and globally, of essential services such as health care, food distribution and energy sectors underscoring the vulnerability of critical infrastructure to significant disruption in essential services, lost revenue and the potential harm or loss of life.

6. Immediately following the 2020 Cyber Security Strategy, the Australian Government began the process of introducing an enhanced regulatory framework, building on existing requirements under the SOCI Act. Following industry consultation, on 10 December 2020, the Australian Government introduced the Security Legislation Amendment (Critical Infrastructure) Bill 2020 (the SLACI Bill 2020). This Bill was subsequently reviewed by the Parliamentary Joint Committee on Intelligence and Security (PJCIS) in its Advisory Report on the Security Legislation Amendment (Critical Infrastructure) Bill 2020 and Statutory Review of the *Security of Critical Infrastructure Act 2018* (the Advisory Report).

7. The Advisory Report recommended the SLACI Bill 2020 be split in two, with the 'urgent elements of the reforms' be 'legislated in the shortest possible time'.

8. The first bill has legislated amendments to the *Security of Critical Infrastructure Act 2018* to incorporate 'government assistance measures' that provide a legislated response to a significant cyber incident, cyber incident reporting obligations, expanding the definition of critical infrastructure to include 11 sectors, and associated definitions and powers. This first bill was passed by Parliament on 22 November 2021 and received Royal Assent on 3 December 2021.

9. This second bill is an Exposure Draft and would amend the *Security of Critical Infrastructure Act 2018* to capture the remaining elements from the SLACI Bill 2020 together with amendments suggested by stakeholders and throughout the Parliamentary Joint Committee on Intelligence and Security review process, including:

    - the Risk Management Program under proposed Part 2A;
    - enhanced cyber security obligations under proposed Part 2C;
    - Systems of National Significance under proposed Part 6A; and
    - information sharing provisions for regulated entities.

10. Should the Parliament legislate this second Bill, it would complete the reforms for an enhanced all hazards security framework delivered under the *Security of Critical Infrastructure Act 2018*. This all hazards framework seeks to uplift security and resilience in all 11 critical infrastructure sectors, providing for better identification and sharing of threats for Australia's critical infrastructure assets, whether industry or government owned and operated. Government will work in partnership with responsible entities of critical infrastructure assets to ensure the new requirements build on and do not duplicate existing regulatory frameworks.

The proposed reforms

Establish, maintain, and comply with a Risk Management Program

11. The Risk Management Program would require owners and operators of critical infrastructure assets to manage the material risk of any hazards occurring, which pose a risk of impacting on the availability, integrity or confidentiality of the critical infrastructure asset. Where possible, the requirements under the Risk Management Program recognise or build on existing regulatory frameworks to minimise the regulatory burden on industry. Indeed, the Government has kept the public interest criteria in the proposed Bill to ensure that cost and the need to switch on the obligation through a rule following formal consultation is maintained. This ensure that if an existing regulation already exceeds the Risk Management Program requirement, there is not a duplicative set of obligations in place.

12. The Exposure Draft sets out the overarching obligations for the Risk Management Program with the more detailed requirements to be contained in rules that have been developed with industry during an extensive consultation process.

Enhanced Cyber Security Obligations for Systems of National Significance

13. The Enhanced Cyber Security Obligations would, if implemented, support a bespoke, outcomes-focused partnership between Government and Australia's most critical assets – declared as systems of national significance'. These obligations would enhance the already mature Government-industry information sharing arrangements to build an aggregated threat picture and provide Government with a comprehensive understanding of the ability of entities responsible for Systems of National Significance to respond appropriately to, or mitigate the impact of, a cyber security incident. Importantly all obligations are exclusively outlined in the proposed bill.

14. Systems of National Significance are proposed to be a significantly smaller subset of critical infrastructure assets that, by virtue of their interdependencies across sectors and cascading consequences of disruption to other critical infrastructure assets and critical infrastructure sectors, are crucial to the nation.

15. Should the Minister for Home Affairs declare a critical infrastructure asset to be a System of National Significance, the Secretary of the Department of Home Affairs may require the responsible entity for a System of National Significance to undertake one or more prescribed cyber security activities. This does not mean that all obligations would apply. They would be considered on a case by case basis following consultation with the System of National Significance. The exclusive and exhaustive list of possible obligations include the development of cyber security incident response plans, cyber security exercises to build cyber preparedness, vulnerability assessments to identify vulnerabilities for remediation, and provision of system information to build Australia's situational awareness. The Exposure Draft explicitly requires the Secretary of the Department of Home Affairs to request the prescribed activity in order to ensure activities have a clear, stated security objective.

16. Through consultation on these reforms, stakeholders have consistently supported greater threat information sharing and partnerships with Government. The Enhanced Cyber Security Obligations would support the bi directional sharing of threat information to provide industry with a more mature understanding of emerging cyber security threats, and the capability to reduce the risks of a significant cyber attack against Australia's most critical assets.

Create a mechanism to declare critical infrastructure assets of the highest criticality as systems of national significance

17. The Exposure Draft sets out a new proposed Part 6A outlining the mechanisms for making a declaration to define critical infrastructure assets that are the most interconnected and interdependent assets, and critical to the security, economy and sovereignty of Australia, as Systems of National Significance, and enabling the requirement for enhanced cyber security obligations.

18. The Minister for Home Affairs would have ability to privately declare a critical infrastructure asset to be a system of national significance, once they have considered the asset's interdependencies with other critical infrastructure assets, and the consequences to Australia's national interest if the asset is significantly impacted.

Other measures

19. The Exposure Draft proposes information sharing provisions to make it easier for regulated entities to share information with their relevant regulator(s).

PART 1—SECTOR AND CRITICAL INFRASTRUCTURE ASSET THRESHOLDS

20. The Exposure Draft contains key sector and asset definitions, which were introduced in the SLACI Bill 2021. These amendments are in response to Recommendation 7 of the PJCIS Advisory Report.

21. These proposed amendments would seek to introduce revised definitions for provisions that have been clearly identified as requiring modification or clarification, as per submissions considered by the PJCIS for the Advisory Report and through significant consultation between the Department of Home Affairs and industry stakeholders.

22. The primary function of these amended definitions is to clarify the responsible entities for critical infrastructure assets, under section 12L of the SOCI Act and as set out in this Exposure Draft. The definition of responsible entity leverages the definition of critical infrastructure asset and enables the Minister for Home Affairs to make rules which determine which obligations in the SOCI Act that would apply to the responsible entity.

23. The responsible entities for these assets would also fall within the definition of 'national security business' in section 8AA of the *Foreign Acquisition and Takeover Regulations 2015*.

24. Assets that fall within the amended critical infrastructure asset definitions below could be subject to the new obligation introduced in this Exposure Draft, the requirement to adopt and maintain a Risk Management Program (Part 2A), in the event that the asset is specified in the rules under section 30AB to require such a program for this class of assets.

25. These assets may also be required to comply with the obligations introduced under the SLACI Bill 2021 to comply with:

    - Mandatory reporting of serious cyber security incidents, in the event that the asset is specified in the rules under section 30BB, and

    - Providing ownership and operational information, in the event that the asset is specified in the rules under section 18A to require this for this class of assets.

COMMUNICATIONS

Critical domain name system definition

26. The Exposure Draft would amend the definition for a critical domain name system to define an asset as a critical domain name system where that asset is critical to the administration of an Australian Domain Name System.

27. The definition would also include a new rule making provisions that would permit the Minister for Home Affairs to create rules that would provide further certainty on what assets are deemed to be 'critical to the administration of an Australian Domain Name System'.

28. This amendment follows consultation with the .au Domain Administration Limited (auDA), the entity responsible for administering the '.au' country code Top Level Domain, and the Department of Infrastructure, Regional Development, Transport and Communications.

DATA STORAGE OR PROCESSING

Data storage or processing service definition

29. The Exposure Draft would amend the definition for a data storage or processing service to provide additional clarity. The amended definition provides additional language around the types of physical assets, such as computing systems and other physical infrastructure, that are used in connection with the sorts of data storage or processing services delivered.

30. This amendment follows consultation with the data storage or processing sector in which industry advised that greater clarity was required for the sector and asset definitions in the Bill.

31. The amended definitions align closely with international definitions and standards, such as the EU's directive on security of network and information systems (the NIS directive) and the National Institute of Standards and Technology agency of the United States Department of Commerce.

32. The amended definition would seek to capture services that

    - Acquire or manage the computing infrastructure required for providing the storage and processing services;
    - Run the storage or processing software that provides the service of storage or processing of computerised data;
    - Makes arrangements to deliver the storage or processing services to consumers through network access.

33. In consultation with the data storage or processing sector, industry has sought clarity around the meaning of 'data processing'. Data processing means the collective set of computerised data actions, such as:

    - **Retention -** the continued possession, use, or control of computerised systems and data
    - **Logging -** the recording of the events occurring and computerised data within an organisation's systems and networks
    - **Generation -** the production or (pro)creation of computerised data and systems.
    - **Transformation** – computerised data that are changed in the form, nature, or appearance of.
    - **Use -** the action of using computerised systems and data or the state of being used for a purpose
    - **Disclosure** - the action of making computerised systems and data known
    - **Sharing -** the action of giving computerised systems and data to another or others
    - **Transmission** - the state that exists when computerised data is being electronically sent from one location to one or more other locations.
    - **Disposal -** the action or process of getting rid of computerised data.

Critical data storage or processing asset definition

34. The Exposure Draft would amend the definition of critical data storage or processing asset to provide additional clarity to industry about the types of entities that will be captured as responsible entities for critical data storage or processing assets. The amended definition removes reference to 'wholly or primarily', to ensure that entities that provide data storage or processing services to Government and critical infrastructure assets are also captured.

35. This amendment follows with the Data Storage or Processing Sector in which industry advised that greater clarity was required for the sector and asset definitions in the Bill.

FINANCIAL SERVICES AND MARKETS

Critical superannuation asset definition

36. The Exposure Draft would amend the definition of critical superannuation asset to include an asset is owned or operated by an RSE Licensee, rather than a registrable superannuation entity, where that RSE Licensee is critical to the security and reliability of the financial services and markets sector.

37. This amendment follows consultation with the Australian Prudential Regulation Authority, which recommended that RSE Licensees, rather than registrable superannuation entities, own and operate critical superannuation assets.

Responsible entity

38. The Exposure Draft would amend the definition for responsible entity to define the responsible entity for a critical superannuation asset to be a Registrable Superannuation Entity Licensee (RSE Licensee). This amendment would ensure that a RSE Licensee that is critical to the security and reliability of the financial services and markets sector is the responsible entity for a critical superannuation asset that it owns and operates.

39. This amendment follows consultation with the Australian Prudential Regulation Authority, which recommended that RSE Licensees, rather than registrable superannuation entities, own and operate critical superannuation assets.

HIGHER EDUCATION AND RESEARCH

Higher education and research sector definition

40. The Exposure Draft would amend the definition for higher education and research sector to the sector of the Australian economy that undertakes a program of research that is supported by the Commonwealth or that is critical to Australia's critical infrastructure, national security or defence.

41. This amendment follows consultation with the University sector, which recommended that this definition be refined to be narrower in scope and provide additional clarity as to the entities and assets that Government consider to be part of this critical infrastructure sector.

ENERGY

Critical energy market operator asset definition

42. The Exposure Draft would amend the definition for a critical energy market operator asset to include an asset that 'is critical to ensuring the security and reliability of an energy market or system'. The amendment ensures that the language is consistent throughout the provision.

PART 2 – DETAILED EXPLANATION OF PROVISIONS

43. A key component of the enhanced critical infrastructure security framework is the creation of a holistic set of Positive Security Obligations for critical infrastructure assets. This Exposure Draft would introduce an additional obligation in the form of a requirement to adopt and maintain a critical infrastructure Risk Management Program. This obligation would only apply in circumstances where the Minister for Home Affairs has made a rule turning the specific obligation on for particular critical infrastructure assets. The rule is subject to mandatory consultation.

44. An uplift in security and resilience across critical infrastructure sectors would mean that all businesses would benefit from strengthened protections to the networks, systems and services we all depend on. The regime would embed preparation, prevention and mitigation activities into the business as usual operation of critical infrastructure assets, providing certainty for businesses across all critical infrastructure sectors by setting clear security standards.

PART 2A - CRITICAL INFRASTRUCTURE RISK MANAGEMENT PROGRAMS

45. During consultations, many stakeholders welcomed the establishment of a clear and consolidated legislative obligation to give industry a sound basis for taking a more comprehensive risk management approach where there was not already an existing regulatory obligation or approach in place. The Exposure Draft would achieve this through the new requirements in Part 2A for critical infrastructure assets to develop and comply with a critical infrastructure Risk Management Program.

46. These proposed amendments are intended to uplift core security practices of critical infrastructure assets by ensuring responsible entities take a holistic and proactive approach toward identifying, preventing and mitigating risks from all hazards.

47. The Exposure Draft sets out the overarching obligations for the Risk Management Programs with the more detailed, principles based requirements to be contained in rules. This approach reflects clear feedback from industry that the responsible entity is best placed to understand the risks to an asset and develop appropriate risk practices Combined, the SOCI Act and the proposed rules would ultimately require responsible entities of critical infrastructure assets to manage security risks by meeting the following principles-based outcomes:

    a. **Identify material risks –** Entities would have a responsibility to take an all-hazards approach when identifying risks that may affect the availability, integrity, reliability and confidentiality of their asset. This would require considering both natural and human induced hazards, which pose a material risk, with the detail outlined in rules that have been designed with industry. This may include understanding how these risks might accumulate throughout the supply chain, understanding the way systems are interacting, and outlining which of these risks may have a significant consequence to core service provision.

    b. **Mitigate risks to prevent incidents –** Entities would be required to understand the identified risks and have appropriate risk mitigations in place to manage those risks so far as is reasonably practicable. Risk mitigation should consider both proactive risk management as well as having processes in place to detect and respond to threats as they are being realised to prevent the risk from eventuating.

    c. **Minimise the impact of realised incidents –** Entities would be required to have robust procedures in place to mitigate, so far as is reasonably practicable, the impacts in the event a

threat has been realised and recover as quickly as possible. This may include ensuring plans are in place for a variety of incidents, such as having back-ups of key systems, adequate stock on hand, redundancies for key inputs, out-of-hours processes and procedures, and the ability to communicate with affected customers.

d. **Effective governance –** Through rules, entities would be required to have appropriate risk management oversight arrangements in place, including evaluation and testing. This would involve strong governance with clear lines of accountability, demonstrated comprehensive planning, and a robust assurance and review process. Compliance would be assessed by the relevant regulator, noting that what is appropriate would be unique to each entity. Regulators would focus on security and resilience outcomes and seek to avoid compliance action wherever possible.

Who would this apply to?

48. Section 30AB would provide a mechanism through which the Minister for Home Affairs may activate the Risk Management Program obligation contained in Part 2A for particular critical infrastructure assets. This would need to be done through making a rule, or where a declaration under section 51 determines that this Part applies to the asset. This 'on-switch' is intended to prevent duplication where arrangements in sectors already exist which impose equivalent obligations to the Risk Management Program. In these circumstances, the SOCI Act obligations would remain dormant with those existing obligations continuing to apply without duplication.

49. As one example, the security and resilience of critical defence industry assets is largely managed through existing frameworks and obligations under the Defence Industry Security Program (DISP). The DISP is a non-regulatory Risk Management Program run by the Department of Defence (Defence) that strengthens security practices in partnership with industry. Existing Defence security mechanisms under the DISP are considered broadly similar and in some cases exceed the Risk Management Program is unlikely to be turned on for the majority of assets in this asset class, absent a significant change in the threat environment or in industry practices.

50. However, the Minister for Home Affairs would retain the power to activate the Risk Management Program should it be considered appropriate and necessary to achieving security outcomes, following consultation with the relevant Minister and should the public interest criteria be met. The Minister would also be required to consult with and consider submissions from proposed responsible entities over a minimum 28 day period.

51. Any rules made under section 30AB to activate the Risk Management Program would be disallowable by Parliament.

52. Acknowledging that bringing business practices into line with these obligations may take time, and that certainty about the requirements to be provided in the rules is necessary before such investments can be made, any rules to apply Part 2A to an asset and provide the requirements for the program would, unless exceptional circumstances exist, have a six month delayed commencement as a minimum to allow an appropriate transition period. Rules may also provide additional time for businesses to bring their practices in line with specific obligations within their Risk Management Program.

Key requirements

Develop a program

53. Section 30AC would provide that if an entity is the responsible entity for one or more critical infrastructure assets, the entity would need to adopt and maintain a critical infrastructure Risk

Management Program in relation to those assets. This requirement would ensure responsible entities develop a nuanced, comprehensive understanding of the threat picture that can affect the availability, confidentiality, reliability and integrity of the relevant critical infrastructure asset.

54. The Risk Management Plan itself would provide a tool for Government to verify whether the risk mitigation approach taken by the responsible entity is appropriate in protecting Australians' access to essential services.

55. While the Rules would provide clarity on what issues would need to be addressed in a risk management plan, Government's intention is that responsible entities would have discretion as to how they construct their Risk Management Program. This recognises industry's expertise and deep knowledge of the unique challenges faced by each critical infrastructure asset.

56. Failure to comply with this provision would attract a maximum civil penalty of 200 penalty units (the value of a penalty unit is currently $222 for offences committed on or after 1 July 2020). The compliance approach though, will always be education and awareness raising as the purpose of these reforms is to ensure that security outcomes are obtained.

Comply with the program

57. Section 30AD would provide that the responsible entity for one or more critical infrastructure assets would need to comply with the critical infrastructure Risk Management Program it has adopted. This provision makes clear that while the process of developing a Risk Management Program is important, the entity would also need to take the necessary steps to implement that program.

58. Failure to comply with this provision would attract a maximum civil penalty of 200 penalty units (the value of a penalty unit is currently $222 for offences committed on or after 1 July 2020).

Review and update the program

59. Sections 30AE and 30AF would provide that the entity is also required to review the program on a regular basis and take all reasonable steps to ensure it is kept up to date. Meaningful uplift of the security and resilience of critical infrastructure would only occur if the Risk Management Programs' articulation of material risks and mitigation strategies remain current. It is therefore vital that responsible entities review their Risk Management Program on a regular basis and take reasonable steps to ensure it is kept up to date. This ensures risk is being continually assessed and managed by the entity rather than taking a set and forget approach to risk management.

60. The Exposure Draft does not define the frequency with which the review required in section 30AE would need to occur, but rather simply would provide that it would need to occur on a regular basis. What is 'regular' for one asset may be different to another asset. This recognises that some assets face a significantly more fluid threat environment than others, and that changing circumstances should be the impetus for review rather than a strict mandated timeframe. Ultimately, this would be a matter for the responsible entity to determine, however the Regulator would work with each sector to provide guidance on its expectations.

61. The Exposure Draft also does not define 'reasonable steps' in section 30AF, as it would depend on the individual circumstances of each entity. It is intended to ensure Risk Management Programs are regularly reviewed and updated in response to evolving technology, business circumstances and changes in the threat environment.

62. Failure to comply with sections 30AE or 30AF would attract a maximum civil penalty of 200 penalty units (the value of a penalty unit is currently $222 for offences committed on or after 1 July 2020).

Content of the program

63. Section 30AH would set out the requirements for a critical infrastructure Risk Management Program. A critical Risk Management Program is a written program that applies to a responsible entity for a critical infrastructure asset and the purpose of which is to do each of the following:

    - 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; and
    - So far as it is reasonably practicable to do so – mitigate the relevant impact of such a hazard on the asset.

64. The critical infrastructure Risk Management Program would need to comply with any requirements set out in the rules, which may be of general application or relate to a particular class of critical infrastructure asset.

65. A hazard in the context of a critical infrastructure Risk Management Program is intended to mean an element, which, alone or in combination with other elements, has the potential to give rise to a material risk. This broad interpretation is needed to reflect the diversity of critical infrastructure assets, which would be subject to the obligation on commencement of the Bill subject to this Exposure Draft, and into the future, and their evolving operating environment. Rather the focus should not be on the source of the hazard but its impact on the functioning of the asset.

66. A relevant impact is defined in section 8G to include the impact of the hazard on the availability, integrity, reliability or confidentiality of the asset, information about the asset, or data or information stored in the asset. Ultimately, this definition ensures responsible entities are considering how a particular hazard affects certain outcomes associated with the asset, whether or not there is a direct or immediate impact on business objectives.

67. What amounts to a material risk would ultimately be a matter for the responsible entity to determine by considering the likelihood of the hazard occurring and relevant impact of the hazard (subsection 30AH(7). The approach to determining what is a 'material risk' is deliberately not prescriptive, in recognition of the many and varied risks faced by critical infrastructure assets and that businesses are best placed to themselves assess what might amount to a material risk. Further detail on this would be contained in rules – see discussion below.

68. Noting these terms, the focus of the critical infrastructure Risk Management Program is identifying and taking steps to minimise or eliminate any material risk arising from a hazard, or mitigating the impact of such a hazard. The requirements have been designed to align with existing business practices which would ordinarily consider the likelihood and consequence attaching to potential hazards business operations.

69. This approach is designed to achieve two key objectives:

    a. Ensure the Risk Management Program **does not** need to consider and take steps to address every potential hazard or risk. The focus is only on **material risks**.

    b. Enable the business **to determine for itself** which risks are material and the appropriate measures to manage those risks.

Risk Management Program rules

70. Part 2A would impose principled-based obligations in recognition of the fact that a Risk Management Program would vary radically between assets and sectors. As such, the process for

developing a Risk Management Program would be supported by consultation with industry and additional guidance provided by Government. The documents would provide requirements and guidance on meeting the obligations.

71. Subsection 30AH(1)(c) specifically requires the critical infrastructure Risk Management Program to comply with any requirements specified in the rules. At a minimum, it is proposed that rules, to be developed with industry, would require responsible entities to consider and address risks in the following four domains:

    a. *Physical security and natural hazards:* This includes risk of harm to people and damage to physical assets. For example, mechanical failures, natural hazards such as floods and cyclones, as well as human induced hazards such as terrorism.

    b. *Cyber and information security hazards:* Malicious cyber activity is one of the most significant threats facing Australian critical infrastructure assets and can range from denial of service attacks, to ransomware and targeted cyber intrusions.

    c. *Personnel security hazards:* This refers to the 'insider threat' or the risk of employees exploiting their legitimate access to an organisations' assets for unauthorised purposes including corporate espionage and sabotage.

    d. *Supply chain hazards:* The reliance on supply chains inherently involves dependencies on other assets, or providing other entities with some level of access to, or control of, your asset or business' deliverables. As is the case for personnel risk, supply chain risks relate to entities exploiting their legitimate access to, or control of, an organisations' assets for unauthorised purposes or otherwise creating a cascading impact to dependent assets.

72. In addition to deeming particular risks as material for the purposes of subsection 30AH(1)(b)(i), the rules may also:

    - mandate the steps responsible entities should be taking through their Risk Management Program to address these risks, including in relation to governance arrangements;
    - recognise existing industry standards and practices are sufficient to meet aspects of the obligation; and
    - de-conflict requirements for entities with assets, which fall within more than one definition of critical infrastructure asset.

73. This approach would ensure Government is able to direct industry action in response to the changing threat environment.

74. Section 30AN makes clear that this may include applying, adopting or incorporating any matter contained in a law of a State or Territory or any matter contained in a standard proposed or approved by Standards Australia.

75. All rules would be developed through extensive consultations, across industry and Government and would outline expectations, and what would be considered a reasonable and proportionate response to meeting the obligations. This is supported by sections 30AL and 30AM which require appropriate consultation to occur prior to the making of any rules.

76. In the event there is an imminent threat that a hazard would have a significant relevant impact on a critical infrastructure asset, a rule may be made without consultation. However, in these circumstances, the Secretary would need to review the operation, effectiveness and implications of

the rules within 60 days of the rules commencing. This review process would need to involve consultation with industry and the findings would need to be tabled in Parliament.

Background checking

77. Trusted insiders are potential, current or former employees or contractors who have legitimate access to information, techniques, technology, assets or premises. Trusted insiders can intentionally or unknowingly assist external parties in conducting activities against the organisation or can commit malicious acts of self-interest. Such action by a trusted insider can undermine or severely impact the availability, integrity, reliability or confidentiality of those assets captured as critical infrastructure assets.

78. Recognising the importance of personnel security, the Exposure Draft would make two key amendments to support industry's ability to understand and manage personnel security risks through background checking.

79. The Exposure Draft would insert new paragraph 8(1)(ba) into the *AusCheck Act 2007* to provide the ability for the AusCheck scheme prescribed in the *AusCheck Regulations 2017* to be amended to enable industry to utilise background checking of an individual if that entity considers that individual to be a critical employee or a member of critical personnel. Please note that this is not a mandatory background check for critical infrastructure. Nor is it to be used as a justification for excessive and unwarranted background checking of staff. The provisions to enable entities to conduct background checking of critical employees or personnel under the critical infrastructure Risk Management Program would be made by rules under new subsection 30AH(4).

80. Currently, the AusCheck Scheme has been established to provide background checking services for the Aviation Security Identification Card (ASIC), Maritime Security Identification Card (MSIC), National Health Security (NHS) check schemes, and in relation to Major National Events (MNE), amongst others.

Annual reporting

81. Section 30AG would provide that where a risk management plan is in place, the responsible entity of that critical infrastructure asset would need to provide a report to the Secretary of Home Affairs, or relevant Commonwealth regulator, within 90 days of the end of the financial year. The report would need to:

    a. state whether or not the program was up to date during the financial year;

    b. if a hazard had a significant relevant impact on one or more of those assets during the relevant period—includes a statement that identifies the hazard; evaluates the effectiveness of the program in mitigating the significant relevant impact of the hazard on the assets concerned; and outlines any variations made to the program as a result of the hazard occurring.

82. A relevant impact is defined in subsection 8G(1) as an impact on the availability, integrity, reliability or confidentiality of the asset. What is significant is likely to vary between assets and across sectors. It would be up to the entity to determine when a relevant impact is significant for the purposes of this reporting obligation, having regard to factors such as the extent of the impact, the vulnerabilities it has exposed and any other factors the entity considers relevant. The Department would provide further guidance to support this particular obligation. It is not intended that entities would be required to report day-to-day incidents; instead the requirement would be to report incidents that have had, or risked having, a significant impact on the entity's ability to conduct its business or deliver its services.

83. This annual report would need to be approved the board, council or other governing body, as the case requires. This is designed to ensure that the most senior levels of an entity are aware of the risk management practices of the entity and personally accountable compliance with this regime.

84. This obligation does not require the responsible entity to provide the full critical infrastructure Risk Management Program to the Secretary, but rather is an assurance process to ensure that it remains up to date and appropriate.

85. Section 30AG also would provide that failure to comply with the annual reporting obligation would attract a maximum penalty of 150 penalty units (the value of a penalty unit is currently $222 for offences committed on or after 1 July 2020).

PART 2C – ENHANCED CYBER SECURITY OBLIGATIONS

86. Critical infrastructure assets and the systems they rely on are increasingly interconnected and interdependent. While Parts 2, 2A, and 2B, discussed above, impose obligations to manage risks to the operation of these assets, a small subset of critical infrastructure assets are of the highest criticality due to their interdependences with other critical assets. A closer partnership is required in relation to these systems of national significance, and the computer infrastructure that underpins them, to build enhanced cyber resilience and preparedness.

87. The Australian Government has introduced the enhanced cyber security obligations to strengthen the cyber preparedness and resilience of entities that operate critical infrastructure assets of the highest criticality (system of national significance). Consultation on the Cyber Security Strategy 2020 supported initiatives to enhance cyber information sharing to build a stronger collective understanding of threats to Australian systems. These obligations enable the Government to establish a bespoke partnership, tailored to individual assets, to not only prepare entities to better manage cyber risks but also improve Australia's situational awareness, particularly as the threat environment worsens.

88. Under Part 6A, the Minister for Home Affairs may declare a critical infrastructure asset to be a system of national significance. Part 2C would provide for a series of enhanced cyber security obligations which may be imposed on the responsible entity for a system of national significance. Responsible entities for Systems of National Significance would not be obligated to comply with each of these enhanced obligations following the Minister's declaration, but rather may be required to do so, from time to time, following a written notice from the Secretary of Home Affairs. This approach reflects the different nature of the obligations provided under this Part, which are aimed at addressing or identifying vulnerabilities and building resilient practices.

89. The Australian Government would continue to build on the strong voluntary engagement and cooperation with critical infrastructure entities that has underpinned the success of the relationship to date. This includes providing voluntary support and guidance. However, there may be instances where entities are unwilling or unable to voluntarily cooperate and the Enhanced Cyber Security Obligations are necessary.

Division 2 of Part 2C – Statutory incident response planning obligations

90. The first of the enhanced cyber security obligations which the Secretary may require the responsible entity for a system of national significance to comply with is the statutory incident response planning obligation. Incident response plans are designed to ensure an entity has established processes and tools to prepare for and respond to cyber security incidents. Incident response plans would provide assurance to Government that entities are sufficiently prepared for cyber security incidents and would assist entities by clearly articulating 'what to do' and 'who to call' in the event of a cyber

security incident. Clear escalation pathways and processes can be crucial to mitigating and minimising the consequences of fast moving cyber incidents.

91. Section 30CB would enable the Secretary of the Department of Home Affairs to determine that the statutory incident response planning obligations apply to the entity, meaning that it would need to adopt and maintain an incident response plan (section 30CD), comply with the plan (section 30CE), and regularly review (section 30CF) and take all reasonable steps to ensure the plan is up to date (section 30CG).

92. Section 30CJ would provide that an incident response plan is a written plan that relates to the system of national significance, for the purposes of planning for responding to cyber security incidents that could have a relevant impact on the system. The plan would need to comply with any requirements specified in the rules, which may include details on procedures to be included in the plan for responding to a particular cyber security incident.

93. Incident response plans would vary from entity to entity. However, common elements of an incident response plan include definitions of the types of systems being used, details of staff member roles and responsibilities, outlines of common cyber incidents and incident response processes to mitigate and remediate a cyber security incident.

94. A copy of the incident response plan would need to provided to the Secretary of Home Affairs, as soon as practicable after it is adopted or varied. This would ensure Government and entities have the necessary information to activate cyber security incident response arrangements at any point in time, particularly in the event of an emergency.

95. A civil penalty of up to 200 penalty units applies for failure to comply with the obligations in this Division (the value of a penalty unit is currently $222 for offences committed on or after 1 July 2020).

Division 3 of Part 2C – Cyber security exercises

96. The second of the enhanced cyber security obligations which the Secretary may require the responsible entity for a system of national significance to comply with is the requirement to undertake a cyber security exercise.

97. Cyber security exercises are an integral part of an entity's cyber security procedures, as they are used to test response preparedness, mitigation and response capabilities. Such exercises enable an entity to develop an understanding of how to address a cyber incident through a scenario that requires the entity to draw upon resources, such as incident response plans, relevant legislation, policies and processes to identify the most appropriate response to a cyber security incident. Cyber security exercises can identify gaps in existing approaches and help streamline processes to ensure more effective and efficient responses to threats as they emerge.

98. During consultation on the Cyber Security Strategy 2020, submissions highlighted the importance of joint cyber security exercises involving industry and government to improve entities' cyber resilience. Noting the interdependencies between critical infrastructure assets, these exercises can be used to develop interoperable response capabilities to prevent a cascading of impacts across sectors.

99. Section 30CM would provide that the Secretary of Home Affairs may, by written notice, require the entity to undertake a cyber security exercise in relation to all types of cyber security incidents, or one or more specified types of cyber security incidents (for example, a denial of service or ransomware attack).

100. The scope of the exercise would be determined based on analysis of threats and incident trends, as well as consideration of the consequential or cascading effects that may occur should the system be impacted by a cyber security incident.

101. A cyber security exercise would be defined in section 30CN to an exercise, the purpose of which is to test the entity's:

- ability to respond appropriately to the cyber security incident/s;
- preparedness to respond appropriately to the cyber security incident/s; and
- ability to mitigate the relevant impacts the cyber security incident/s could have on the system.

102. Cyber security exercises are generally conducted through one of two formats: discussion-based or tabletop exercises, and operational or functional exercises.

103. The Secretary of Home Affairs may also require that the entity allow specified designated officers to observe the cyber security exercise, provide those officers with access to the premises or other assistance and facilities to allow the observation of the exercise, allow them to make reasonably necessary records and give them notice of when the exercise would commence. A designated officer is defined in section 30DQ to be an employee of the Department of Home Affairs or a staff member of the Australian Signals Directorate.

104. Section 30CQ would provide that, on completion of the exercise, the entity is required to prepare an evaluation report relating to the exercise and give a copy of the report to the Secretary. An evaluation report is a written report the purpose of which is to evaluate the entity's:

- ability to respond appropriately to the cyber security incident/s;
- preparedness to respond appropriately to the cyber security incident/s, and
- ability to mitigate the relevant impacts the cyber security incident/s could have on the system.

105. However, if the entity has prepared, or purported to prepare an evaluation report, provided it to the Secretary for Home Affairs and the Secretary has reasonable grounds to believe that the report was not prepared appropriately, the Secretary may require the entity to appoint an external auditor to prepare an evaluation report for the entity. Alternatively, if the entity fails to comply with section 30CQ the Secretary for Home Affairs may require an external evaluation report to be prepared by an external auditor. An external auditor is a specified individual authorised by the Secretary as such for the purposes of the Act.

106. A civil penalty of up to 200 penalty units applies for failure to comply with the obligations in this Division (the value of a penalty unit is currently $222 for offences committed on or after 1 July 2020).

Division 4 of Part 2C – Vulnerability assessments

107. The third element of the enhanced cyber security obligations which the Secretary may require the responsible entity for a system of national significance to comply with is the requirement to undertake a vulnerability assessment.

108. Vulnerability assessments are a routine cyber security practice undertaken to identify vulnerabilities or 'gaps' in systems which expose them to particular types of cyber incidents. These preparatory activities also enable the entity to evaluate the risk of particular vulnerabilities. This

would enable entities that operate Australia's Systems of National Significance to remediate vulnerabilities before they can be exploited by malicious actors. The identification of vulnerabilities in one system may also enable the remediation of similar vulnerabilities across other critical systems.

109. A vulnerability assessment can consist of a documentation-based review of a system's design, a hands-on assessment or automated scanning with software tools. In each case, the goal is to identify security vulnerabilities.

110. Section 30CU would provide that the Secretary of Home Affairs may require the entity to undertake, or cause to be undertaken, a vulnerability assessment in relation to the system and a particular type of cyber security incident, or cyber security incidents generally. The entity can undertake this assessment or may choose to engage the services of a third party to undertake the assessment. Prior to making such a request, the Secretary is required to consult with the entity. This consultation requirement would assist the Secretary to determine the entity's capacity to undertake, or cause to be undertaken, the required vulnerability assessment.

111. If the Secretary of Home Affairs has reasonable grounds to believe that the entity would not be capable of complying with a notice or has not complied with an earlier notice, the Secretary may give a designated officer a written request to undertake the vulnerability assessment and require the entity to provide reasonable access, assistance and facilities to the officer to allow the assessment to be undertaken.

112. If the entity, or a designated officer, undertakes a vulnerability assessment they would need to prepare, or cause to be prepared, a vulnerability assessment report and provide a copy of the report to the Secretary.

113. A civil penalty of up to 200 penalty units applies for failure to comply with the obligations in this Division (the value of a penalty unit is currently $222 for offences committed on or after 1 July 2020).

Division 5 of Part 2C – Access to system information

114. The final of the enhanced cyber security obligations which the Secretary may require the responsible entity for a system of national significance to comply with is the requirement to provide system information.

115. During consultation on the Cyber Security Strategy 2020, stakeholders strongly supported initiatives to improve information sharing to make critical infrastructure more resilient and secure. The provision of system telemetry from Systems of National Significance would support the Government's ability to build a near-real time threat picture through the CESAR capability and share actionable, anonymised information back out to industry. Aggregated system information, overlaid with intelligence and reporting, would also enable the Government to target its limited capabilities to the threats and vulnerabilities of greatest consequence to the nation.

116. System information is information that relates to the operation of the computer needed to operate a system of national significance. This information may assist with determining whether a power under this Act should be exercised in relation to the system of national significance. However, system information cannot include personal information within the meaning of the Privacy Act 1988. For example, system information may be network logs or alerts that provide visibility of the operation and functioning of a broader computer network. The monitoring of this information can be crucial to identifying a compromise of a system and deploying a rapid response to mitigating its potential impacts.

117. Section 30DB would provide that, if the Secretary of Home Affairs believes on reasonable grounds that the responsible entity for the system of national significance is technically capable of

doing so, the Secretary may require the entity to provide the Australian Signals Directorate with periodic reports consisting of specified system information ('a system information periodic reporting notice'). The Secretary may specify the intervals, manner and form in which the information is to be provided, as well as any other information technology requirements relating to the provision of the information. Depending on the information required and the ability for automated provision (such as automated machine-to-machine cyber threat intelligence sharing), these reports may be required to be made at rapid intervals, for example, every minute.

118. Section 30DC would provide that, if the Secretary of Home Affairs believes, on reasonable grounds, that the responsible entity for the system of national significance is technically capable of doing so, the Secretary may require the entity to provide the Australian Signals Directorate with reports consisting of specified system information as soon as practicable after each incidence of a specified event occurring ('a system information event-based reporting notice'). For example, a report may be required every time a particular computer program raises a specified class of alert or error message.

119. In deciding whether to give a system information periodic reporting notice or a system information event-based reporting notice, the Secretary of Home Affairs would have to have regard to the costs that are likely to be incurred by the entity in complying with the notice. To support this consideration as well as the determination of whether the entity is technically capable of providing the report, section 30DD mandates that the Secretary of Home Affairs would need to consult with the entity prior to issuing the notice.

120. If the Secretary of Home Affairs does not believe on reasonable grounds that the entity would be technically capable of preparing reports under sections 30DB or 30DC, section 30DJ would provide that the Secretary may require the entity to install and maintain a specified computer program ('system information software notice'). The computer program may only be specified in the notice if its purpose is to collect and record the required system information and cause the information to be transmitted electronically to the Australian Signals Directorate. The computer program would be provided by the Government and would, for example, operate as a host-based sensor reporting back to the Australian Signals Directorate telemetry information used to monitor the system for malicious behaviour.

121. In deciding whether to give a system information software notice, the Secretary of Home Affairs would need to have regard to the costs that are likely to be incurred by the entity in complying with the notice. To support this consideration, section 30DK mandates that the Secretary of Home Affairs would need to consult with the entity prior to issuing the notice.

122. A civil penalty of up to 200 penalty units applies for failure to comply with the obligations in this Division (the value of a penalty unit is currently $222 for offences committed on or after 1 July 2020).

DIVISION 3 OF PART 4—USE AND DISCLOSURE OF PROTECTED INFORMATION

123. Division 3 of Part 4 sets out a framework for the use and disclosure of protected information.

124. Subsection 43E(1) would provide that an entity may disclose protected information if that information relates to the entity and the information is disclosed to a prescribed person or entity for the purpose of enabling or assisting the person to exercise the person's powers or perform the person's functions or duties.

125. Subsection 43E(2) would provide that an entity may disclose protected information if that information relates to the entity in certain circumstances where the Secretary of Home Affairs has consented in writing to the disclosure.

DIVISION 2 OF PART 6A —DECLARATION OF SYSTEMS OF NATIONAL SIGNIFICANCE BY THE MINISTER

126. Division 2 of Part 6A sets out the process by which the Minister for Home Affairs can declare a critical infrastructure asset to be a system of national significance. Systems of National Significance are a smaller subset of critical infrastructure assets which are of the highest criticality due to their national significance. These are systems that are so integral to the functioning of modern society that their compromise, disruption or destruction would have significant adverse impacts on Australia's economic and social stability, defence and national security.

127. Systems of National Significance are an attractive target for malicious actors, particularly those with the capability and motive to do significant harm to Australia's national interests. Due to these factors and the security vulnerabilities that may emerge if the extent of the asset's criticality were widely known, a declaration under Part 6A is private, and the fact the declaration is made is protected information under the Act.

128. If an asset is declared by the Minister for Home Affairs to be a System of National Significance, the Secretary is empowered to impose the Enhanced Cyber Security Obligations contained in Part 2C on the entity in certain circumstances.

National significance

129. Subsection 52B(1) would provide that the Minister for Home Affairs may declare a particular asset to be a system of national significance if the asset is a critical infrastructure asset and the Minister is satisfied that the asset is of national significance.

130. Subsection 52B(2) would provide that, in determining whether an asset is a System of National Significance the Minister for Home Affairs would need to have regard to the consequences that would arise for the social or economic stability of Australia or its people, the defence of Australia or national security if a hazard were to occur that had a significant relevant impact on the asset, nature and extent of interdependencies between the asset and other critical infrastructure assets that the Minister is aware of, as well as any other matters as the Minister considers relevant.

131. The systems that underpin our critical infrastructure are increasingly interconnected and digital. These interconnections, and convergence of informational technologies and operational technologies, provide economic benefits to owners and operators. System and process data can be drawn and leveraged to improve performance, identify faults and increase productivity. Internet connected systems can be accessed from anywhere in the world, meaning that the unique skills required to rectify faults to these often aged assets can potentially be accessed whenever required. Critical infrastructure is also increasingly interdependent. Energy and communications underpin many other critical infrastructure sectors. Many assets in the communications sector provide a critical function, which relies on electricity. Many critical infrastructure assets in turn rely on the communications sector to undertake their business.

132. However, this interconnectedness and interdependence creates a new set of vulnerabilities. Malicious actors can use these same digitally connected pathways to access, compromise, disrupt and destroy these critical systems. The compromise of one critical infrastructure asset could have first, second and third order consequences which cascade and compromise other critical infrastructure assets and critical infrastructure sectors.

133. The Minister for Home Affairs is only required to consider any interdependency between the asset that is the subject of the declaration and other critical infrastructure assets that the Minister is aware of, which may not capture all actual interdependencies.

Consultation with entities

134. Section 52C sets out the consultation requirements that would need to be undertaken prior to the Minister for Home Affairs making a declaration. Importantly, the Minister would need to provide the responsible entity of the asset with notice of the proposed declaration, including reasons for making the declaration, and invite any representations. The entity would ordinarily be provide 28 days to make any submissions; unless the Minister for Home Affairs is satisfied a shorter period is necessary due to urgent circumstances.

135. Noting that determining the criticality of an asset may rely on classified information, the Minister for Home Affairs is only required to provide reasons for the proposed declaration to the responsible entity for the asset in question to the extent that those reasons would not prejudice security.