# Contents

Glossary of terms ............................................................................................................................................. 5

Purpose of this explanatory document ........................................................................................................ 6

Introduction .......................................................................................................................................................... 6

What is the problem and why is Government action needed? .............................................................................. 9

Part 1—Preliminary ............................................................................................................................................. 15

  Division 1—Preliminary ................................................................................................................................. 15
  Division 2—Definitions ...................................................................................................................................... 17
  Division 3—Constitutional provisions and application of this Bill ................................................................. 32

Part 2—Register of Critical Infrastructure Assets ............................................................................................ 35

  Division 1—Simplified outline of this Part ...................................................................................................... 35
  Division 2—Register of Critical Infrastructure Assets .................................................................................... 36
  Division 3—Obligation to give information and notify of events ..................................................................... 37
  Division 4—Giving of notice or information by agents ................................................................................... 42
  Regulatory burden of the Register of Critical Infrastructure Assets .............................................................. 43

Part 3—Directions by the Minister ................................................................................................................. 46

  Division 1—Simplified outline of this Part ...................................................................................................... 46
  Division 2—Directions by the Minister ........................................................................................................... 47
  Regulatory burden of the directions power ..................................................................................................... 54

Part 4—Gathering and using information ....................................................................................................... 62

  Division 1—Simplified outline of this Part ...................................................................................................... 62
  Division 2—Secretary’s general power to obtain information or documents .................................................. 63
  Division 3—Use and disclosure of protected information ............................................................................... 66
  Subdivision A—Authorised use and disclosure ............................................................................................... 66
  Subdivision B—Offence for unauthorised use or disclosure ......................................................................... 69

Part 5—Enforcement ......................................................................................................................................... 71

  Division 1—Simplified outline of this Part ...................................................................................................... 71
  Division 2—Civil penalties, enforceable undertakings and injunctions .......................................................... 71

Part 6—Declaration of assets by the Minister .................................................................................................. 74

  Division 1—Simplified outline of this Part ...................................................................................................... 74
  Division 2—Declaration of assets by the Minister .......................................................................................... 74

Part 7—Miscellaneous ...................................................................................................................................... 76

  Division 1—Simplified outline of this Part ...................................................................................................... 76
<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAT</td>
<td>Administrative Appeals Tribunal</td>
</tr>
<tr>
<td>AEMO</td>
<td>Australian Energy Market Operator</td>
</tr>
<tr>
<td>ASIO</td>
<td>Australian Security Intelligence Organisation</td>
</tr>
<tr>
<td>ASIO Act</td>
<td>Australian Security Intelligence Organisation Act 1979</td>
</tr>
<tr>
<td>FIRB</td>
<td>Foreign Investment Review Board</td>
</tr>
<tr>
<td>MW</td>
<td>megawatts</td>
</tr>
<tr>
<td>NEM</td>
<td>National Energy Market</td>
</tr>
<tr>
<td>NSI Act</td>
<td>National Security Information (Criminal and Civil Proceedings) Act 2004</td>
</tr>
<tr>
<td>Privacy Act</td>
<td>Privacy Act 1988</td>
</tr>
<tr>
<td>TSSR</td>
<td>Telecommunications sector security reforms contained in the</td>
</tr>
<tr>
<td></td>
<td>Telecommunications and Other Legislation Amendment Act 2017</td>
</tr>
</tbody>
</table>
Purpose of this explanatory document

1. This explanatory document accompanies the exposure draft of the Security of Critical Infrastructure Bill 2017. The Bill is designed to strengthen the Government’s capacity to manage the national security risks of espionage, sabotage and coercion arising from foreign involvement in Australia’s critical infrastructure, with minimal regulatory impact and maintaining Australia’s open investment policy. This document informs and facilitates public consultation by providing context for why the measures are required, its objectives, and proposed operation.

Introduction

2. Critical infrastructure underpins the functioning of Australia’s society and economy and is integral to the prosperity of the nation. It enables the provision of essential services such as food, water, health, energy, communications, transportation and banking. Secure and resilient infrastructure supports productivity and helps to drive the business activity that underpins economic growth. The availability of reliable critical infrastructure promotes market confidence and economic stability, and increases the attractiveness of Australia as a place to invest.

3. The Australian Government (the Government) welcomes foreign involvement in the economy and in Australia’s infrastructure because it plays an important and beneficial role in supporting economic growth, creating employment opportunities, improving consumer choice, and promoting healthy competition, while increasing Australia’s competitiveness in global markets. It can also help improve productivity by enabling the development of much-needed infrastructure, introducing new technology, allowing access to global supply chains and markets, and enhancing Australia’s skills base.

4. However, while recognising the many benefits, foreign involvement 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 or attribute. This can in turn enable them to target activity, in a way that can have subtle effects on the continuity of services to citizens, as well as extreme consequences for other dependant infrastructure or defence assets.

5. Most critical infrastructure in Australia is either privately owned and operated, or run on a commercial basis by government. A disruption to critical infrastructure assets could have a range of serious implications for business, government and the community. The responsibility for ensuring the continuity of operations and the provision of essential services to the Australian economy and community is shared between owners and operators of critical infrastructure, state and territory governments, and the Australian Government.
6. While owners and operators understand and manage many of the risks to the continuity of their operations as a core part of their businesses, the Australian Government is seeking to ensure they have a more detailed understanding of the national security risks posed by foreign involvement in critical infrastructure. The Government wants to ensure effective arrangements are in place to develop and implement mitigation strategies that leverage existing mitigation mechanisms.

7. That is why on 23 January 2017, the Australian Government launched the Critical Infrastructure Centre (the Centre). The Centre works across all levels of government and with critical infrastructure owners and operators to identify and manage the national security risks of espionage, sabotage and coercion in critical infrastructure. The Centre’s key functions include:

- identifying Australia’s most critical infrastructure
- conducting national security risk assessments
- developing risk management strategies, and
- supporting compliance.

8. The Centre works in close consultation with state and territory governments, regulators, and critical infrastructure owners and operators, with an initial focus on the national security risks to four high-risk sectors:

- **Electricity**: Electricity is fundamental to every facet of Australian society, underpinning just about everything in the digital age. A prolonged disruption to Australia’s electricity networks would have a significant impact on communities, businesses and national security capabilities. Some electricity providers also hold large data sets about customers and their electricity usage, which need to be appropriately protected.

- **Water**: A clean and reliable supply of water is essential to all Australians, including other critical infrastructure sectors. A disruption to Australia’s water supply or water treatment facilities could have major consequences for the health of citizens and impact the diverse range of businesses that rely on water—from the cooling towers used at power stations to food processing. Water providers also hold large data sets about customers and their water usage.

- **Ports**: Australia relies heavily on its commercial ports to trade goods with the world, with one third of our GDP facilitated through seaborne trade. Ports support Australia’s prosperity, the supply of liquid fuels, the supply chains for other critical infrastructure, and Defence purposes. Disruption to our most critical ports could have wide-reaching impacts on the economy.

- **Telecommunications**: The Australian telecommunications systems and networks are part of our national critical infrastructure and form the backbone for many other critical infrastructure sectors and services. These networks and systems could be attractive to those who wish to harm Australian interests. On 18 September 2017, the legislation that underpins the Telecommunications Sector Security Reforms (TSSR) received Royal Assent. These reforms introduce obligations on carriers and carriage service providers to do their best to protect networks and facilities from unauthorised access and interference. The Centre will be responsible for leading the implementation of the reforms and will work with industry to assist them to comply with their obligations by the end of the 12-month transition period. The Centre is
currently refining guidance materials to provide greater clarity for organisations on their obligations under the legislation.

9. While the Government continues to take an all-hazards approach to the resilience of Australia’s critical infrastructure, the focus of the Centre is on the national security risks of:

- **Espionage:** Certain critical infrastructure sectors may present opportunities for the collection of information, particularly bulk data, which is not publicly available. Foreign intelligence services will target commercial and government-related organisations for this data. For example, an operator or contractor could monitor data traffic to gather information on behalf of a foreign intelligence service.

- **Sabotage:** A hostile foreign actor could use access gained through investment or commercial involvement in critical infrastructure to conduct a deliberate disruption to supply for strategic or economic gain. For example, the deliberate interruption or destruction of operations at a port could result in economic and reputational damage for the Government.

- **Coercion:** In extreme cases, a foreign actor could use access to, and control of, critical infrastructure to apply coercive power against state, territory or Australian Governments to influence decision-making or policy.
What is the problem and why is Government action needed?

10. The national security risks to critical infrastructure are complex and have continued to evolve over recent years. Rapid technological change has resulted in critical infrastructure assets having increased cyber connectivity, and greater participation in, and reliance on, global supply chains with many services being outsourced and offshored.

11. Australia’s Critical Infrastructure Resilience Strategy (the Strategy) recognises that in most cases, neither business nor government in isolation have access to all the information they need to understand and appropriately mitigate risks. It also recognises that neither business nor government in isolation have the ability to completely influence their operating environments to the extent required to ensure the continuity of essential services. The Strategy, which takes an all-hazards approach, emphasises the need for collaboration between government and industry to ensure that risks to critical infrastructure are appropriately managed.

12. Long-standing government-industry partnerships, such as the Trusted Information Sharing Network for Critical Infrastructure Resilience (TISN), provide an avenue to share information on issues relevant to the resilience of critical infrastructure and the continuity of essential services in the face of all hazards. The Centre aims to build on these partnerships to address the specific national security risks from foreign involvement in critical infrastructure.

Assessing national security risks

13. In assessing the potential risks of sabotage, espionage and coercion from foreign involvement in critical infrastructure assets, the Centre works collaboratively with states, territories and industry to undertake risk assessments on critical assets. Risk assessments involve analysing the:

- threats posed to the sector generally and the specific asset
- vulnerability of that asset, and
- consequences if involvement in that asset was used to conduct espionage, sabotage or coercion.

14. Following a risk assessment, the Centre will, in collaboration with industry and state and territory governments, consider and develop any mitigations that need to be put in place to address the risk.

Lack of information on legal and beneficial ownership

15. The Government has a well-developed understanding of threat, and is generally able to determine consequence. However, the Centre cannot undertake a comprehensive risk assessment without understanding how the asset and sector operates and where there may be vulnerabilities. To determine what vulnerabilities may exist, it is essential to have a detailed understanding of who owns, controls and has access to a particular asset.

16. Wherever possible, the Centre aims to work with owners, operators, and investors to obtain this information. However, critical asset owners often treat this information as commercial-in-confidence and may be reluctant to share with government unless required
to do so. The Centre’s ability to obtain this information has on occasions been limited to existing processes, such as through assessing applications to the FIRB.

17. In the absence of existing mechanisms to obtain this information, Government agencies have difficulty in identifying and understanding beneficial ownership arrangements. Ownership interests are often held in complex corporate structures, spanning multiple jurisdictions, or through trusts, managed funds, or nominee companies. Further, while ownership is an important aspect, the degree of control and access through outsourcing and offshoring arrangements can also be difficult to establish, as they are often detailed in complex contractual arrangements.

18. Finally, critical infrastructure information sources vary from state to state, with regulatory mechanisms often narrowly focused on information required to inform how owners are meeting reliability standards.

**Limited ability to apply appropriate mitigations to address national security risks**

19. Once the Centre has assessed the risks from foreign involvement in an asset, it looks to work collaboratively with the asset owner to develop and implement proportionate mitigations to address the risks. The FIRB process is one existing mechanism through which the Government can implement mitigations. However, this only applies to foreign investments above certain thresholds\(^1\) at the time of the proposed transaction. It is not possible to use it as a mechanism to address risks in outsourcing or offshoring for assets owned by domestic entities or where sales fall outside of the FIRB screening thresholds. As a result, outside of the FIRB process, the Government is not well placed to implement some of the required mitigations to address national security risks.

20. Recognising that critical infrastructure in some sectors is owned or regulated by states and territories, the Government would also look to work with states and territories to leverage existing regulatory regimes wherever possible. However, existing state-based regimes are limited in scope and differ between jurisdictions. In jurisdictions where there are some ministerial powers to require a critical infrastructure owner or operator to do (or not do) a certain thing, these powers are generally only triggered in the case of an emergency event. It is unlikely that such a power could be used to mitigate all possible national security risks, such as an identified risk of espionage.

**Further measures are needed to protect Australia’s critical assets**

21. Existing gaps in the Government’s understanding of the ownership and control of critical infrastructure, and the lack of a mechanism at the federal level to intervene where a significant risk to national security has been identified, limit Government’s ability to understand, manage and respond to national security risks. Disruption of critical infrastructure sectors can have a serious impact on Australia’s national and economic security, both in terms of immediate costs incurred and long-term sector vulnerability.

---

\(^1\) Generally, the threshold for business acquisitions is $252 million, or $1,094 million for investors from certain countries that have free trade agreements with Australia. The threshold for foreign government investors is $0. Different thresholds apply to investments in sensitive sectors, such as media.
22. The more extreme examples of national security risks are unlikely to occur outside a significant shift in regional or global strategic relationships or imminent armed conflict. However, there are substantial risks in the current environment, including from espionage and pre-positioning for sabotage. The Government needs to be able to identify and respond to the full range of national security risks in a way that provides flexibility to respond to changes in the geopolitical landscape as it evolves.

23. The issues outlined above support the need for further measures to ensure that the Government can develop a comprehensive picture of national security risks from foreign involvement in critical infrastructure, and apply appropriate mitigations where necessary. These further measures will ultimately ensure that Australia can effectively manage the risks from foreign involvement in critical infrastructure.

Approach to developing this Bill

24. In February 2017, the Centre released a discussion paper, *Strengthening the National Security of Australia’s Critical Infrastructure*, seeking views on the operations of the Centre and two possible regulatory measures to address the limitations in the existing regulatory regime:

- an asset register to capture and track information about who owns and operates Australia’s most critical assets in the high-risk sectors, and
- a last resort directions power for the Minister to seek information and issue directions to owners and operators of critical assets in the high-risk sectors when a significant national security risk cannot otherwise be mitigated.

25. In March and June 2017, on behalf of the Australian Government, the Centre conducted separate rounds of consultations with officials from state and territory governments and industry to seek views on the proposed regulatory measures. The outcome of these consultations, as well as submissions received on the discussion paper, informed the development of this draft Bill.

26. The Centre welcomes further views and will be hosting briefings and accepting submissions on this draft Bill.

Summary of new law

What does the Bill regulate?

27. The Bill will regulate approximately 100 assets in the highest-risk sectors of ports, electricity and water. If any of these assets were disrupted, they would have a significant impact on Australia’s economic interests and services for large populations. Part 1, Division 2 – Definitions outlines the thresholds for determining which assets will be classed as ‘critical infrastructure’ and who constitutes a reporting entity or an operator, upon whom the obligations under the Bill will fall.

28. Recognising the importance of responding to any changes in the national security risk landscape, the assets, or categories of assets, captured by the legislation can be amended through a legislative instrument rule-making power. The responsible Minister will need to satisfy predetermined criteria before adding further assets.

29. This Bill does not change Australia’s foreign investment framework under the *Foreign Acquisitions and Takeovers Act 1975*. 
What are the obligations for reporting entities under the Register of Critical Infrastructure Assets?

30. This Bill will impose reporting requirements on two sets of entities: direct interest holders and responsible entities.

31. Direct interest holders of a critical infrastructure asset will be required to provide interest and control information in respect of the asset. Responsible entities for a critical infrastructure asset (effectively the main licensed body) will be required to provide operational information, such as system access abilities and operator and outsourcing arrangements.

32. These entities will have six months to report the required information from the commencement of the legislation. Following initial reporting, the entities will then be obligated to notify the Commonwealth Government of any changes to this information within 30 days of the event. The Centre will maintain a secure web portal for entities to easily report information.

33. During consultations, concerns were raised regarding the financial and regulatory burden associated with the reporting measures. The Centre has worked with industry and governments to strike an appropriate regulatory balance. We have assessed that the Register will impose a minimal compliance burden on industry.

34. Part 2 Division 3 – Obligation to give information and notify of events, details the specifics of the obligations.

How will the Last Resort Power be used?

35. The Last Resort Power will allow the Minister to issue a direction to an owner or operator of a critical infrastructure asset to mitigate significant national security risks. Part 3 details the requirements for the use of the Last Resort Power.

36. The Power, as proposed, will only be able to be used in situations where:
   - there is a significant national security risk
   - through collaboration, the reporting entity or operator does not implement mitigations to address the risk, and
   - there are no existing regulatory frameworks that can be used to enforce mitigations.

37. Under the draft legislation, the Minister will be required to be satisfied of certain matters and give consideration to a number of factors before being able to issue a direction, including:
   - giving primary consideration to a mandatory ASIO adverse security assessment, which will consider the risk posed and include a recommendation for action
   - being satisfied that ‘good faith’ negotiations have occurred
   - considering the costs and consequences to services in implementing the mitigation
   - ensuring the direction is a proportionate response to the risk.
38. During consultations, stakeholders requested greater clarity on how the regulatory framework will interact with existing federal, state and territory legislation and regulation to avoid duplication and excessive regulation. The Bill explicitly mandates that the Commonwealth Government must consider the use of existing mechanisms, including state and territory regimes, before issuing a direction under the proposed regime. This includes direct consultation with the relevant state or territory minister.

39. These safeguards will ensure the power is used appropriately and not exercised beyond the remit of specific, significant national security risks that cannot be addressed through other means.

Administration and enforcement

Penalties and offences

40. Non-compliance with the Register obligations and the information-gathering and last resort powers will attract civil penalties, including civil pecuniary penalties, enforceable undertakings and injunctive relief (Part 5 Division 2—Civil penalties, enforceable undertakings and injunctions refers).

41. The only criminal offence in the Bill relates to unauthorised disclosure of protected information obtained under this Act.

Confidentiality of information

42. The Australian Government understands the potentially sensitive commercial information that will be required to be provided under the Register or through the information-gathering power. Any information provided will remain protected and confidential. Access to, and use of, this information is restricted to certain persons and specific purposes (set out in Part 4, Division 3—Use and disclosure of protected information).

Public consultation and key questions

43. The Australian Government welcomes comment on these reforms prior to finalisation and introduction of legislation into Parliament.

44. The Centre will host public briefings in each capital city and will accept submissions on the proposed legislation. To facilitate consideration of the proposed measures, a range of guiding questions are outlined over the page. They can also be found under the relevant sections of this Explanatory Memorandum.

45. Please send written comments by 10 November 2017 to the Attorney-General’s Department at: enquiries@CICentre.gov.au or by mail to: Critical Infrastructure Centre, 3-5 National Cct, BARTON ACT 2913, AUSTRALIA. For further information on the briefing sessions please contact +61 2 6141 3338 or enquiries@CICentre.gov.au.
Questions

1. How can the Australian Government best engage with relevant *entities* to understand and mitigate identified risks?

2. To understand what would be most useful for owners and *operators*, what information would you like to see in best practice guidance provided to manage national security risks?
Part 1—Preliminary

Division 1—Preliminary

Section 1 – Short title

46. This section provides for the short title of the Bill, if enacted, to be the Security of Critical Infrastructure Act 2017.

Section 2 – Commencement

47. This section provides that the Act will come into effect at the date of Proclamation or, if Proclamation does not occur within three months after the Bill receives Royal Assent, then the Bill will commence the day after three months from Royal Assent.

48. Proclamations, which are made by the Governor-General, are the preferred method for providing discretion to fix a commencement date for the Bill.

49. A fixed date, as by Proclamation, or three months after Royal Assent, is appropriate for commencement of this Act to allow stakeholders time to become familiar with their obligations under the Act.

Section 3 – Objects

50. The objects outline the purpose and intention of this Act to provide a risk-based regulatory framework to manage national security risks from foreign involvement in Australia’s critical infrastructure. The national security risks that are the primary focus of the legislation are sabotage, espionage and coercion. This risk-based approach focuses on Australia’s highest-risk critical infrastructure sectors of electricity, ports and waters.

51. With increased privatisation, outsourcing and offshoring of supply chain arrangements, and the shift in Australia’s international investment profile, critical infrastructure is more exposed than ever to sabotage, espionage and coercion. Critical infrastructure underpins the functioning of Australia’s society and economy. Secure and resilient infrastructure ensures the wider community has access to essential services. National security risks such as sabotage, espionage and coercion could cause disruptions to critical infrastructure sectors that have serious impacts on Australia’s national and economic security, both in terms of immediate costs incurred and long-term sector vulnerability.
52. The Act has two key mechanisms to support the management of these national security risks: a Register of Critical Infrastructure Assets and a ministerial ‘last resort’ directions power.

53. The Register will provide a deeper understanding of who owns, controls and has access to the highest-risk assets by requiring interest and control information and operational information to be provided to Government (Part 2, Division 3). While the Government works closely with owners, operators and investors to obtain this information, some stakeholders may be reluctant to share this information unless legally required to do so.

54. The directions power (outlined in Part 3 of the Act) will provide Government with the ability to manage an identified national security risk if other mechanisms cannot be used. Importantly, this directions power is only to be used as a matter of last resort with risks, wherever possible, to be managed through the existing strong and collaborative relationship between government and industry. This includes utilising existing regulatory mechanisms where appropriate. However, the directions power will ensure that risks can be managed where existing mechanisms are not effective.

Section 4 – Simplified outline of this Act

55. While simplified outlines are included in the Act to assist readers to understand the substantive provisions, they are not intended to be comprehensive. It is intended that readers should rely on the substantive provisions.

56. The outline details the following obligations, powers, functions and safeguards:

- Keeping a Register of interest and control information and operational information on critical infrastructure assets, noting that the Register will not be made public (Part 2, Division 2).
- Requiring direct interest holders and responsible entities of critical infrastructure assets to provide interest and control information and operational information to the Register and to notify the Government when there is a change in the information provided (Part 2, Division 3).
- A ministerial directions power to reporting entities and operators of critical infrastructure assets to do or not to a certain thing where a risk to national security has been identified (Part 3, Division 2).
- A power for the Secretary to require reporting entities and operators to provide information or documents relevant to managing national security risks to critical infrastructure (Part 4, Division 2).
- Information obtained under this Act is protected information and can only be disclosed in certain circumstances and for particular purposes (Part 4, Division 3).
- Enforcement measures under this Act include civil penalties, injunctions and enforceable undertakings. There are criminal penalties for disclosure of protected information (Part 5, Division 2).
- The Minister is able to privately declare a particular asset to be critical infrastructure in circumstances where declaration of the asset publicly would pose a risk to national security (Part 6, Division 2).
- A requirement to report annually on the operation of this Act (Part 7, Division 4).
57. Relevant obligations to keep the *Register* up to date and information gathering powers will provide the Government with greater visibility of who owns, operates and is able to influence and control our most critical assets.

58. The ministerial directions power will ensure that in the most significant of cases, where no other mechanisms are available, the Government has the ability to require actions to be taken to manage national security risks.

59. Recognising the nature of the information that will be provided under the Act, there are appropriate safeguards on how that information can be used and further disclosed.

60. Finally, the annual reporting obligations will ensure the Minister provides Parliament and the public with information on the use of the different powers under the Act, ensuring the powers are being used appropriately and subject to the necessary oversight and accountability mechanisms.

### Division 2—Definitions

**Section 5 – Definitions**

61. *ABN* has the same meaning as in the *A New Tax System (Australian Business Number) Act 1999* and is used to identify a business to the Government and the community. An entity’s *ABN* (or other similar business number however described) is required to be reported to the *Register* as part of interest and control information (defined in section 6) in accordance with Part 2, Division 3.

62. *Acquisition of property* has the same meaning as paragraph 51(xxxi) of the *Australian Constitution*. This definition relates specifically to section 33 of the Act, which provides a limitation to use of the Minister’s directions power under section 30. Section 33 provides that the Minister’s directions power at section 30 cannot be used in a way that would result in an acquisition of property as defined under the Constitution. In the event that a direction issued would result in acquisition of property, the direction will only be valid to the extent that it does not result in the acquisition of property.

63. *Adverse security assessment* has the same meaning as subsection 35(1) of the ASIO Act, which means a security assessment conducted by ASIO in respect of a person that contains:

- any opinion or advice, or any qualification of any opinion or advice, or any information, that is or could be prejudicial to the interests of the person, and
- a recommendation that prescribed administrative action be taken or not be taken in respect of the person, being a recommendation the implementation of which would be prejudicial to the interests of the person.

64. An *adverse security assessment* must be provided to the Minister before he or she can issue a direction for a direct interest holder, responsible entity or operator to do, or refrain from doing a certain thing under section 30(2). This is to ensure that the Minister’s directions power is reserved for instances where there is a serious national security risk that warrants ASIO furnishing an *adverse security assessment*. 
65. Under paragraph 30(5)(a), the Minister must give the greatest weight to the adverse security assessment when considering whether to issue a direction under section 30. This is to ensure that mitigating the national security risk is given precedence over other considerations such as costs of complying with the direction or consequences to competition in the relevant industry.

66. Appointed officer for an unincorporated foreign company means the secretary of the company or an officer of the company appointed to hold property on behalf of the company. These individuals are defined for the purpose of understanding who is a direct interest holder under paragraph 8(2)(d). This ensures that the appropriate legal person of an unincorporated foreign company, which can hold property and sue or be sued on behalf of the company (see subparagraph (b)(ii) of the definition of foreign company in the Corporations Act 2001), is required to report interest and control information (defined in section 6) in accordance with Part 2, Division 3.

67. The approved form will be a form that is approved by the Secretary, and it will set out the manner in which direct interest holders and responsible entities are to provide information for the Register in accordance with Part 2, Division 3. While the Act sets out the information to be provided, the approved form will be the practical tool by which to provide this information.

68. Civil penalty provision has the same meaning as subsection 79(2) of the Regulatory Powers Act, which provides that a civil penalty provision establishes an enforceable pecuniary penalty for contravention of provisions that are so described.

69. The following provisions are civil penalty provisions for the purposes of this Act, and are aligned with the key obligations under this Act:

- section 22 – Initial obligation to give interest and control information and/or operational information and notify of events
- section 23 – Ongoing obligations to give interest and control information and/or operational information
- section 32 – Requirement to comply with a direction (under section 30), and
- section 35 – Secretary may obtain information or documents from entities.

70. To encourage compliance, the relevant authority (in this case the Minister or Secretary) can apply to the relevant court for a civil penalty order to seek payment of a pecuniary penalty. Financial penalties are appropriate for this regime to deter non-compliance, having regard to the nature of the obligations, and that they are likely to fall on corporations and other non-natural persons.

71. Commencing day means the day the Act commences in line with section 2. Under section 2, the Act will commence on proclamation by the Governor-General on a specific date, or the day after three months from Royal Assent, whichever occurs first.

72. Given this Act provides the Government with powers to compel direct interest holders, responsible entities and operators of critical infrastructure assets to do certain things and provide certain information to the Government, it is not appropriate to apply the Act from the date of Royal Assent. Rather, stakeholders should be given a period of time to become familiar with the powers and their obligations under the Act.
73. **Critical electricity asset** is defined under section 10, which states that all electricity networks, systems or interconnectors that are used for transmission or distribution of electricity, and electricity generation stations that are critical to ensuring the security and reliability of an electricity network in a state or territory, are **critical electricity assets** for the purposes of this Act. This definition forms part of the definition of **critical infrastructure asset** in section 9, which itself outlines the assets to which this Act applies.

74. **Critical infrastructure asset** is defined at section 9 of the Act and states that a **critical infrastructure asset** is a **critical electricity asset** (section 10), a **critical port** (section 11), a **critical water asset** (in section 5), an asset declared under section 49 to be a **critical infrastructure asset**, or an asset prescribed by the **rules** for the purposes of this paragraph.

75. Detailed information on each of these elements is provided under their respective definitions. However, these assets are captured as they represent the assets and sectors (outside of telecommunications which is being addressed separately through TSSR) that are currently at the highest-risk of sabotage, espionage and coercion.

76. This definition is fundamental to the operation of the Act as it outlines the assets that fall within the scope of the Act and therefore triggers the **entities** that will have reporting obligations. Importantly, this definition also clearly prescribes the assets in relation to which the directions power can only be used.

77. **Critical port** is defined at section 11, and means specific Australian ports that have been gazetted as security regulated ports under section 13 of the MTOFSA. These ports represent the vital ports in Australia for defence purposes, liquid fuel imports and bulk cargo exports. The disruption of any of these ports, and therefore services provided by these ports, would cause significant harm to Australia’s social and economic stability and our ability to ensure our national security. This definition forms part of the definition of **critical infrastructure asset** in section 9, which itself outlines the assets to which this Act applies.

78. **Critical water asset** is defined at section 5 and captures those water utilities that ultimately service at least 100,000 water and/or sewage connections and where there is an entity that holds a licencing agreement with a state or territory regulator to operate the water utility. This captures those critical water utilities, which if disrupted, would significantly impact the operations of large population hubs, economic interests and Government operations. This has been determined by considering:

- **Large population hubs**
  - The Bureau of Meteorology currently uses 100,000 connections as its highest data point to capture the water utilities servicing the major population hubs in Australia.
  - Total residential population serviced – the assets captured by this definition individually service at least 275,000 people. As a collective, these utilities service 80% of Australia’s population.

- **Economic interests**
  - Gross value added – the assets captured contribute approximately 75% of Australia’s gross value added.

- **Critical infrastructure interdependencies** – as the utilities captured service the major population hubs in Australia, their interdependencies include:
data centres—including holders of bulk data and Government data
- hospitals and other health services
- electricity generation assets, and
- telecommunications — the supply of water is important for some telecommunications infrastructure for heating ventilation and air conditioning purposes.

79. This definition forms part of the definition of critical infrastructure asset, which itself outlines the assets to which this Act applies.

80. Direct interest holder in relation to an asset is defined in section 8 and includes any direct interest holder greater than 10% or any other direct interest holder, who is in a position to directly or indirectly influence or control the asset. The direct interest holder, which is a reporting entity under section 5, has the obligation to report interest and control information (defined in section 6) in accordance with Part 2, Division 3.

81. Direct interest holders are defined in the Act as they would be best placed to report on the required interest and control information for the critical infrastructure asset, which is fundamental to the objectives of this Act to better understand who owns and controls our highest-risk critical infrastructure. For the purposes of this Act, a direct interest holder is separately defined from a responsible entity (defined in section 5) as the latter would not ordinarily have access to interest and control information.

82. Entity means an individual, a body corporate, body politic, a trust, a partnership, a superannuation fund, or an unincorporated foreign company. These various structures represent the structures that underpin ownership or operations of critical infrastructure in Australia. To ensure the Act operates to compel these various structures to adhere to obligations under the Act, it is important that they are captured under the definition of entity, which in turn is used as part of the definition of reporting entity. The definition of reporting entity outlines the circumstances in which specific entities will have obligations under this Act, including obligations to provide interest and control information and operational information to the Register in accordance with Part 2, Division 3.

83. Grace period means the six-month period from whenever an asset becomes a critical infrastructure asset for the purposes of the legislation. Subsections (a) and (b) ensure that whether a critical infrastructure asset is identified as such at the commencement of the Act, or sometime in the future (as a result of falling within an existing definition or through additional assets being captured), the direct interest holders and responsible entities for that critical infrastructure asset will have six months to meet its reporting obligations in relation to the Register. This is to allow a sufficient period of time for reporting entities for assets to understand the requirements and collate the necessary information to be provided on the Register.

84. Interest and control information is defined in section 6, which specifies the information that must be provided to the Register. Information required to be reported includes the reporting entity’s legal name, address, ABN, incorporation information, and type and amount of interest held. Information on the direct interest holder’s ability to access networks or systems necessary for the operation or control of the asset is also required to be reported. This information is fundamental to the objectives of this Act which is to better understand who owns and controls our highest-risk critical infrastructure.
85. A **notifiable event** is defined in section 24 and means an event that has the effect of rendering any of the **interest and control information** or **operational information** on the Register incorrect or incomplete. When a notifiable event occurs, reporting entities (direct interest holders and/or responsible entities) will have 30 days (in accordance with subsections 22(3) or 23(2)) to update the Register. This is to ensure that the Register is kept up to date with accurate information.

**Example**

Having already reported its interest and control information to the Register, Interest Holder A sells down its 100% shareholding in Company A to Interest holder B who acquires a 20% interest in Company A. In this example, in accordance with section 23, within 30 days, Interest holder A would now need to report its new shareholding as 80% and Interest Holder B would need to report its 20% shareholding as well as all the information it is required to report as a direct interest holder.

86. **Operational information** is defined in section 7 which specifies the information that a responsible entity must provide to the Register in accordance with Part 2, Division 3. This information is being collected to assist in the Government’s understanding of who is in a position to influence the control and operation of critical infrastructure assets.

87. An **operator** in relation to ports refers specifically to the port facility operators, as defined under the MTOFSA. The port facility operators have operational control of the various facilities that operate at a port, and are often divided by the cargo-type they deal in, such as liquid fuel port facilities, bulk cargo facilities, general cargo facilities, and passenger terminals.

88. For electricity and water assets, the operator is an entity that is authorised to operate the asset (however described), or a part of the asset.

**Example**

Company A holds the licence to operate to a water utility and A has a contract with Company B to operate a treatment facility within that water utility. In this example, Company A would a responsible entity and Company B would be an operator for the purposes of this Act.

89. **Operators** are defined under this Act because they are likely to be in a position to be able to exercise some level of operational control over the day to day running of the asset. Although operators will not be required to provide information for the Register under section 22 and section 23, they will be subject to the information gathering and directions power under Part 4, Division 2.

90. Other entities that may operate at the asset, such as cleaners, maintenance companies, retail operators do not fall with the definition of operators for the purpose of this Act, because they are not operating the asset itself, or a part of the asset.

91. **Port facility** takes its meaning from section 10 of the MTOFSA. Port facility is defined to determine whether an operator, defined in section 5, is a port facility operator (within the
meaning of the MTOFSA) for a critical port. If so, then that would constitute operational information that a responsible entity would need to report for the Register.

92. **Protected information** is defined to capture any information obtained under this Act. Broadly, this refers to information provided as part of Register reporting obligations, or obtained through the information gathering power, or the fact that an asset has been privately declared for the purposes of the Act. Importantly, this definition is used to ensure that information obtained by the Government under the Act is afforded the appropriate protections, given the likely sensitive nature of the information. For example, the type of information that is obtained under the Act may be commercial-in-confidence or sensitive for national security reasons. Accordingly, Part 4, Division 3 provides that protected information may only be disclosed to certain persons and/or for restricted purposes. This will ensure the information is not accessed or used inappropriately.

93. **Register** means the Register of Critical Infrastructure Assets kept by the Secretary under section 18. The Register has been established under this Act to assist the Government to manage national security risks of sabotage, espionage and coercion from foreign involvement in critical infrastructure assets by understanding who owns, controls and has access to specific, high-risk assets. This information will assist the Government to assess the national security risks from foreign involvement in particular critical infrastructure assets.

94. Keeping the Register, and mandating reporting of interest and control information and operational information, will assist the Government to:
   - identify who has ultimate control over critical infrastructure assets
   - understand the risks associated with changes of ownership or control, and
   - develop suitable mitigations to address national security risks wherever they arise.

95. **Regulatory Powers Act** means the Regulatory Powers (Standard Provisions) Act 2014. The purpose of the Regulatory Powers Act is to create standard provisions to deal with, among other things, civil penalties and other such enforcement measures. This Act triggers Parts 4, 6 and 7 of the Regulatory Powers Act that relate to civil penalty provisions, enforceable undertakings and injunctions as the appropriate enforcement measures for this regulatory framework (as established under sections 22, 23, 32 and 35).

96. **Relevant industry** refers to the industries covered by the Act, namely electricity, water, ports and any industry that may be prescribed by rules. Using this term negates the need to outline each of the industries individually in Part 3, Division 2; Part 4, Division 3; and Part 6, Division 2.

97. **Reporting entity** is defined as the entity on which reporting obligations are placed to report operational information and/or interest and control information. Reporting requirements are split between the responsible entity for the asset and/or a direct interest holder in relation to the asset to ensure the entity with access to the relevant information bears the reporting obligations. An entity may be both the responsible entity for an asset and a direct interest holder in relation to the asset. A responsible entity is defined in section 5 as the entity ultimately responsible for the operation of the asset. A direct interest holder is defined in section 8 and incorporates an entity with a direct interest of 10% or any other direct interest holder that is in a position to directly or indirectly control or influence the asset.
98. **Responsible entity** for an asset is the *entity* with ultimate operational responsibility for the asset and has the obligation to report *operational information* (defined in section 7) in accordance with Part 2, Division 3.

99. The definition of *responsible entity* has sector specific meanings:

- for a **critical electricity asset** or a **critical water asset**, the *entity* that holds the licence, approval or authorisation (however described) to operate the asset to provide the service to be delivered by the asset
- for a **critical port**, the port *operator* (within the meaning of the MTOFSA) of the port
- an *entity* specified in a declaration by the Minister under section 49 as the *responsible entity* for a critical infrastructure asset, or
- an *entity* specified by the *rules* as a **critical infrastructure asset** for the purposes of paragraph 9(1)(e).

100. These *entities* have been identified as *responsible entities* as they would be the authorised *operator* of the asset and, as such, ultimately responsible for the asset’s continued operation. Given this, they are best placed to report the required *operational information* in relation to the **critical infrastructure asset** for the *Register*.

101. *Rules* means the *rules* able to be made by the Minister under section 57. Section 57 states that the Minister may, by legislative instrument, make *rules* prescribing matters that are required or permitted by the Act to be prescribed; or matters necessary or convenient to be prescribed for carrying out or giving effect to the Act.

102. An example of a matter that is able to be prescribed by the *rules* is the requirements for an electricity generation station to be critical to ensuring the security and reliability of electricity networks in a particular state or territory.

103. **Security**, other than in section 10, has the same meaning as in section 4 of the ASIO Act. For section 10, **security** has its ordinary meaning. The definition of **security** is a central concept in the exercise of the Minister’s directions power under section 30. The Minister may only provide a written direction to an *entity* if he or she is satisfied that there is a risk of an act or omission in connection with a **critical infrastructure asset** that would be prejudicial to **security**.

104. The concept of **security** is also referenced in the Minister’s rule-making power under paragraph 9(3)(b). Among other things, the Minister can prescribe a **critical infrastructure asset** if he or she is satisfied that there is a risk in relation to an asset that may be prejudicial to **security**.

105. **Sewerage infrastructure** means any infrastructure that is, or is to be, used for collection, treatment, storage, and conveyance of sewage. This definition feeds into the definition of a **critical water asset** to ensure that various systems and functions within a water utility are captured under this Act, and the information gathering and directions powers can be utilised in respect of *operators* of the various parts of a water utility.

106. **Superannuation fund** takes its meaning from section 10 of the Superannuation Industry (Supervision) Act 1993 to include an indefinitely continuing fund that is a provident, benefit, superannuation or retirement fund; or a public sector superannuation scheme.
107. The Act defines this term to clarify that a superannuation fund is captured as a direct interest holder under subsections 8(1) or (2). As a direct interest holder, and where the superannuation fund is a trust, the trustee of the fund would also be a reporting entity under section 5 and would therefore have the obligation to report interest and control information (defined in section 6) under Part 2, Division 3. Where a superannuation fund is not a trust, but otherwise able to hold interests in critical infrastructure assets, Australian law would treat these superannuation funds as a legal person and it would therefore would be a reporting entity and captured by subsection 8(1).

108. Including a definition of superannuation funds recognises that both domestic and foreign superannuation funds have considerable investments in Australia’s critical infrastructure and so must be captured within the provisions of this Act to assist in determining control and operation of critical infrastructure assets.

109. This Act includes the rules, ensuring that the rules are taken to be part of the operation of the Act.

110. Unincorporated foreign company means a body covered by paragraph (b) of the definition of ‘foreign company’ in section 9 of the Corporations Act 2001. This definition is used for the purposes of paragraph 8(2)(d) to capture unincorporated foreign companies as direct interest holders who are required to report interest and control information (defined in section 6) in accordance with Part 2, Division 3. Capturing unincorporated foreign companies is consistent with the object of the Act to improve the transparency of the ownership and control of critical infrastructure.

111. Water infrastructure, although distinct from sewerage infrastructure, also forms part of the definition for critical water asset. This is to ensure that various systems and functions within a water utility are captured under this Act, and the information gathering and directions powers can be utilised in respect of operators of the various parts of a critical water asset.
Section 6 – Meaning of interest and control information

112. Section 18 requires the Secretary to maintain a Register of Critical Infrastructure Assets. This Register must contain a range of information, including interest and control information for critical infrastructure assets. This section defines the interest and control information that must be reported to the Register by the relevant reporting entity under Part 2, Division 3. This information is being collected to assist in the Government’s understanding of foreign ownership and control of critical infrastructure assets, including ultimate beneficial ownership.

113. Section 6 defines the interest and control information in relation to an entity (labelled the first entity) and for each other entity (labelled as the other entity) that is in a position to directly or indirectly influence and control the first entity (also considered to be any ultimate interest holder or beneficial owner). The first entity and the other entity rely on the definition of entity in section 5 to mean an individual, a body corporate, body politic, a trust, a partnership, a superannuation fund, or an unincorporated foreign company.

114. Interest and control information includes the following:

- the legal name of the first entity
- if applicable, the ABN of the first entity, or other similar business number (however described) if the first entity was incorporated, formed or created (however described) outside Australia
- for an entity other than an individual or body politic – the address of the first entity’s head office or principal place of business; and the country in which the first entity was incorporated, formed or created (however described)
- for an entity that is an individual – the residential address of the first entity; the country in which the first entity usually resides; and the country or countries of which the first entity is a citizen, and
- for an entity that is a body politic – the address of the first entity’s head office or principal place of business; and the country in which the first entity was formed or created (however described) as a body politic.

115. Paragraph 6(1)(f) provides that the type of interest (such as a legal, equitable, lease or licence interest) and level of the interest (shareholding) the first entity holds in the asset need to be reported to the Register.

116. Paragraph 6(1)(g) ensures that interest and control information extends to the influence and control that the first entity is in a position to directly or indirectly exercise in relation to the asset. This includes control decisions relating to the running of the asset (for example, voting and veto rights and board appointments), and information on appointments to the body that governs the asset (for example, board members’ full name and citizenship details). Influence and control extends to the ability to:

- materially impact the day-to-day operations of the asset
- influence or determine the business or other management plan for the asset
- influence or determine the appointment of key personnel involved in the day-to-day operation of the asset
- influence or determine major expenditures in relation to the asset or its operations
• influence or determine major contracts or transactions in relation to the asset or its operations, or
• influence or determine indebtedness of any kind in relation to the asset or its operations.

117. Paragraph 6(1)(h) requires information about the ability of a person who has been appointed to the governing body that governs the asset (usually the board of the asset) to directly access networks or systems that are necessary for the operation or control of the asset. This would include board members’ access to industrial control systems and security or corporate systems of the asset. This information aligns with the objects of the Act, which is to ensure there is greater transparency of the ownership and operational control of critical infrastructure in Australia in order to better understand national security risks.

Example
Company A owns a critical water asset. One board member who has experience in industrial control systems takes over the responsibilities of the chief operating officer who has fallen ill and cannot perform their functions for a significant period of time. As this role requires access to the critical water asset’s industrial control systems, this access would require reporting to the Register in accordance with paragraph 6(1)(h).

118. Paragraph 6(1)(i) is a key component of the Act that requires the first entity to report any relevant interest and control information, as described above, about each other entity that is in a position to directly or indirectly influence or control the first entity. For the purposes of the Act, other entity is considered to be any ultimate interest holder or beneficial owner of the first entity. This information forms the crux of the Register to identify who ultimately owns and controls critical infrastructure assets and to assist in identifying any associated risks to national security arising from that ownership or control.

Example
Fifty percent of the shareholdings in Company A, who owns an electricity distribution network in Tasmania, is held by Company X. Company X only has one shareholder, Mr Smith, who is an American citizen and lives at 1 Smith Street, in Auckland, New Zealand. In accordance with paragraph 6(1)(i), Company X would need to report all information covered by paragraphs 6(1)(a) to (e) for itself as well as Mr Smith such as Mr Smith’s shareholding in Company X, which in turn owns 50% of Company A, and that Mr Smith resides at 1 Smith Street, in Auckland, New Zealand but is an American citizen.

119. A rule-making provision is included in paragraph 6(1)(j) in order for the rules to prescribe other interest and control information for this definition. This rule-making provision addresses new and emerging situations where additional interest and control information is required to assess national security risks.

120. Subsection (2) prescribes that the information required under subsection (1) may include personal information (within the meaning of the Privacy Act).
Section 7 – Meaning of operational information

121. Section 18 requires the Secretary to maintain a Register of Critical Infrastructure Assets. This Register must contain a range of information including operational information on captured critical infrastructure assets. This section defines the operational information that must be reported to the Register by the responsible entity under Part 2, Division 3. This information is being collected to assist in the Government’s understanding of foreign control and operation of critical infrastructure assets.

122. Section 7(1) defines operational information to include:

- the location of the asset
- a description of the area the asset services, and
- for each entity that is the responsible entity for, or an operator of, the asset:
  - the name of the entity
  - address of the entity’s head office or principal place of business
  - incorporation details in Australia or another country, and
  - where the entity is incorporated, formed, or created in another country, the name of that country.

123. The responsible entity is defined in section 5 and generally means the entity that holds the licence, approval or authorisation (however described) to operate the asset and the service it delivers. An operator, defined in section 5, means an entity that is authorised to operate the asset (however described), or a part of the asset.

Example

Company A is licensed to operate a critical port. The port has five operators conducting business within the port boundaries, including Operator X who is a New Zealand-incorporated entity. Company A would be the responsible entity for the port asset and would need to report to the Register the location of the port (in New South Wales for example), a description of the industries that the port services (such as liquid fuels, bulk cargo), and the name, address of each operator’s head office (or principal place of business) and incorporation information. Company A would also need to report where each operator is incorporated, which would include outlining that Operator X is incorporated in New Zealand.

124. This section also requires the reporting of the full name and citizenship details of the chief operating officer of the responsible entity. The chief operating officer (however described) usually has ultimate responsibility for the operations of the critical infrastructure asset and would have a detailed understanding of the asset’s operations. In the event that the Secretary undertakes a risk assessment of the asset (see section 54), the chief operating officer would be a primary contact for the Government during the risk assessment process. Information on the name and citizenship details of the chief operating officer also assists in determining the level of foreign control or operation of the asset.

125. Operational information required for the Register also extends to arrangements under which an entity, in this case an operator, operates or controls the asset or a part of the asset (subsection (1)(e)). These arrangements are usually contained in an agreement or
contract for outsourcing or offshoring certain functions or responsibilities. The Government is seeking this information to understand the circumstances in which an entity operates the critical infrastructure asset on behalf of direct interest holder(s) or responsible entity and the degree of foreign control or operation of the asset. Arrangements of particular interest for the Government include the outsourcing or offshoring of industrial control systems and security or corporate systems.

Example

Company A contracts with Company B to operate a regional component of its water infrastructure. To satisfy paragraph 7(1)(e), Company A would need to provide details of the operating arrangement (e.g. through a contractual arrangement) and summarised information on the operator’s functions or responsibilities under the arrangement, such as the operator’s responsibility to maintain water infrastructure or service network control systems. Alternatively, Company A could provide a copy of the contract that outlines the operating arrangement with Company B.

126. Subsection (1)(f) provides the Minister with a rule-making power to prescribe other operational information for this definition. This subsection intends to address situations in which other operational information, often in response to changing circumstances in the relevant industry, may assist in determining who is in a position to influence the control or operation of critical infrastructure.

127. Subsection (2) prescribes that the information required under subsection (1) may include personal information (within the meaning of the Privacy Act).

Section 8 – Meaning of direct interest holder

128. The direct interest holder, which is a reporting entity under section 5, has the obligation to report interest and control information (defined in section 6) in accordance with Part 2, Division 3. An entity is a direct interest holder in relation to an asset if the entity holds:
• a legal or equitable interest of at least 10% in the asset and includes an interest that is jointly held with one or more other entities, or
• a lease of, or an interest in, the asset, that puts the entity in a position to directly or indirectly influence or control the asset.

129. An entity is defined in section 5 to mean either an individual, body corporate, body politic, partnership, trust, superannuation fund, or an unincorporated foreign company.

130. Influence and control extends to the ability to:
• materially impact the day-to-day operations of the asset
• influence or determine the business or other management plan for the asset
• influence or determine the appointment of key personnel involved in the day-to-day operation of the asset
• influence or determine major expenditures in relation to the asset or its operations
• influence or determine major contracts or transactions in relation to the asset or its operations, or
• influence or determine indebtedness of any kind in relation to the asset or its operations.

131. Direct interest holders are obligated to report interest and control information under the Act as they would be best placed to access, or obtain, the required interest and control information for the critical infrastructure asset. For the purposes of this Act, a direct interest holder is separately defined from a responsible entity (defined in section 5) as the latter would not always have access to interest and control information.

132. Subsection (2) clarifies that subsection (1) applies where the entity is a trust, partnership, superannuation fund or an unincorporated foreign company. This subsection is included to ensure that the reporting obligations apply to any direct interest holder regardless of the nature of that interest holder.

Section 9 – Meaning of critical infrastructure asset

133. This legislation contains a range of powers, functions and obligations that only apply in relation to critical infrastructure assets. This section defines a critical infrastructure asset for the purposes of the Act as a critical electricity asset (section 21), a critical port (section 22), a critical water asset (section 5), an asset declared under section 49 to be a critical infrastructure asset, or an asset prescribed by the rules for the purposes of this paragraph.

134. This definition minimises the regulatory burden by ensuring the legislation and its obligations only apply to Australia’s highest-risk critical infrastructure assets. Specifically, the definition limits the Act to those assets, which if destroyed, degraded, or rendered unavailable for an extended period, would have a significant impact on:
• maintaining status quo operations for large population hubs. This includes:
  – material impact, or injury, to people, and
  – the behavioural impact to social norms, including the rule of law
• national economic interests
• government operations – impacting the Government’s ability to provide services to the public or its international partners, and
• Defence capabilities, including the ability to conduct Defence operations.

135. This approach is based on the shared definition for critical infrastructure between the Government, and states and territories, as stated in the Critical Infrastructure Resilience Strategy:

• Those physical facilities, supply chains, information technologies and communication networks which if destroyed, degraded or rendered unavailable for an extended period, would significantly impact the social or economic wellbeing of the nation or economic wellbeing of the nation or affect Australia’s ability to conduct national defence and ensure national security.

136. The water, ports and electricity sectors (in addition to the telecommunications sector, being separately managed through TSSR) have been identified as the highest-risk sectors for the following reasons as well as because their existing regulatory regimes do not directly manage national security risks of sabotage, espionage and coercion.

• **Electricity** – Electricity is fundamental to every facet of Australian society, underpinning just about everything we do in the digital age. A prolonged disruption to Australia’s electricity networks would have a significant impact on communities, businesses and national security capabilities. Some electricity providers also hold large data sets about customers and businesses and their electricity usage, which needs to be appropriately protected. Overseas experience has demonstrated that these networks can be the target of malicious actions.

• **Water** – A clean and reliable supply of water is essential to all Australians, and many of our other critical infrastructure sectors and businesses. A disruption to Australia’s water supply or water treatment facilities could have major consequences for the health of citizens and impact the diverse range of businesses that rely on water—from the cooling towers used at power stations, to food processing. Water providers also hold large data sets about customers and their water usage, which need to be appropriately protected.

• **Ports** – Australia relies heavily on its commercial ports to trade goods with the world, with one third of its GDP is facilitated through seaborne trade. Ports support Australia’s prosperity, the supply of liquid fuels and the supply chains for other critical infrastructure. Disruption to our most critical ports could have wide-reaching impacts on the economy.

137. **National security purposes** – Section 49 provides the Minister with the power to privately declare an asset to be a critical infrastructure asset under the Act, where the asset is critical for security purposes, but where there would be a risk to security if it were publicly known that the asset is a critical infrastructure asset. Where an asset is declared for these purposes, the entities that will have obligations under the Act will be directly notified. It is expected that this will only apply to a limited number of critical infrastructure assets.

138. **Additional assets or classes of assets** – Paragraph 9(1)(e) provides for a rule-making power for the Minister to add new assets to the definition of a critical infrastructure asset. This ensures that as the national security and critical infrastructure environment changes, the Act is able to respond to such changes readily. For example, specific assets, classes of
assets and subsectors and sectors currently not identified as high risk may become higher risk over time due to an increase in the criticality or vulnerability of those assets and/or because the Government becomes aware of new security threats. To limit the Government’s ability to add assets inappropriately, such as going outside the scope of the objects of this Act, the Minister must be satisfied that:

- the asset or class of assets is critical to Australia’s social or economic stability or Australia’s national defence or national security, and
- in respect of that asset or class of assets, there is a risk that may be prejudicial to security (as defined in the ASIO Act).

139. This two limb test ensures that the Act continues to not only focus on the most critical infrastructure assets, but only those assets where there is a risk that may be prejudicial to security. As the addition of new assets is through a legislative instrument, it will be subject to the normal Parliamentary disallowance process.

Section 10 – Meaning of critical electricity asset

140. This section defines which electricity assets are considered to be critical and therefore captured for the purposes of this legislation. Specifically, this section provides that an asset is a critical infrastructure asset if it is an electricity network, system or interconnector used for transmission or distribution of electricity. It also captures electricity generation stations that are critical to ensuring the security and reliability of an electricity system or network in a state or territory.

141. Electricity supply in Australia is dependent on four key components, and given the criticality of each of these components, all four systems are captured within this Act. The four components are:

- **Generation** – generators produce electricity and ensure the system or network is stable. Only the electricity generator stations that are critical to ensuring the security and reliability of the system or network in a state or territory will be captured by the Act. The rules to the Act will specify the basis upon which electricity generation stations are to be captured, the details of which are explained at the end of this document.

- **Transmission** – electricity transmission transmits power from generators to distributors, and to other state transmission networks via interconnectors. The legislation will capture all nine electricity transmission networks in Australia as each of these operate as a natural monopoly and have been identified as high-risk.

- **Distribution** – electricity distributors transform the high voltage electricity from the transmission network, to lower voltages and supply it to their assigned regional service areas and end-users. There are 16 electricity distribution companies in Australia. The legislation will capture all distribution assets as electricity distribution has been identified as high-risk.

- **Interconnectors** – the six interconnectors (dedicated transmission lines) that allow electricity to flow between jurisdictions are essential to maintaining the secure and stable supply of electricity to states and territories. Victoria is the most interconnected state in the NEM, with connections to Tasmania, South Australia and New South Wales. New South Wales is connected to Victoria and Queensland, while Queensland, South Australia and Tasmania are only connected to one region each. The interconnectors for Queensland, South Australia and Tasmania are particularly
important for maintaining system reliability if one of these jurisdictions experiences a shortage in electricity supply.

Section 11– Meaning of critical port

142. The legislation outlines the specific ports that the legislation will apply to. These ports have been specifically listed due by reference to the following factors:

- Relevant for Defence purposes.
- Liquid fuels – liquid fuels facilities that account for 5% of total mass tonnes liquid fuels imports. This captures ports, which if rendered unavailable, would have a significant impact on liquid fuel reserves. Australia is heavily dependent on liquid fuels imports. Our economy, particularly our transport system, is almost wholly dependent on liquid fuels.
- Bulk cargo – critical bulk cargo facilities that account for at least 5% of total mass tonnes of bulk cargo imports and exports. This includes Port of Newcastle, Hay Point and Port Hedland, which collectively represent almost 50% of Australia’s mass tonne throughput. As a result these ports may have a significant impact on the national economy if rendered unavailable.

143. Paragraph 11(u) provides that further ports are able to be captured for the purposes of the legislation by listing in a rule made under section 57. This ensures that the legislation is flexible and is able to adapt to changing circumstances.

Division 3—Constitutional provisions and application of this Bill

Section 12 – Application of this Bill

144. This section clarifies the constitutional heads of power that the Government relies on in establishing this Act and the regulatory framework within it. This section cites the following heads of power and their corresponding provisions within the Australian Constitution:

- the corporations power (section 51 (xx))
- the territories power (section 122)
- the trade and commerce power (section 51(i))
- the defence power (section 51(vi)), and
- the aliens power (section 51(xix))

as the powers upon which this Act relies. This provision, does not, however, limit the Government’s ability to rely on other constitutional heads of power that may be relevant to the operation of the Act. These constitutional heads of power provide the basis upon which the powers, functions and obligations in the Act are placed on each of the entities to which the Act applies.
Section 13 – Extraterritoriality

145. Section 13 confirms that the Act applies within and outside Australia. This covers all territories of Australia, including Australia’s exclusive economic zone, and the continental shelf. It also extends jurisdiction outside Australia.

146. In order for Australia to exercise jurisdiction, such as regulating certain conduct, in relation to matters or actions occurring outside of Australia, it must also have a basis for doing so under international law. This requires a sufficient degree of connection to Australia, which, for example, in respect of foreign operators of critical infrastructure assets with Australia, this nexus would be met. Further, if there was an example of a foreign entity engaging in conduct overseas, but where the conduct affects the security of Australia, this would also provide a sufficient degree of connection to Australia on the basis of the ‘protective’ or ‘security principle’, where security is a key interest of the State.

Section 14 – This Act binds the Crown

147. Subsection 14(1) states that the Act binds the Crown in each of its capacities, which means that the Act applies to the Australian Government as well as the states and territories. As Australia’s critical infrastructure is in large part owned and regulated by states and territories, the Act must apply to the Crown in all its capacities to ensure that the regulatory framework operates effectively.

148. Subsection 14(2) confirms that under this Act, the Crown is not liable to be prosecuted for a criminal offence. The criminal offence under this Act relates specifically to unauthorised disclosure of protected information by a person and will apply to that person in their personal capacity (section 43). However, the Crown is liable for the civil penalties and related remedies under this Act.

Section 15 – Concurrent operation of State and Territory laws

149. To the extent that this Act and any state and territory laws can operate concurrently, this Act does not limit or exclude the operation of a state or territory law. In relation to Australia’s critical infrastructure where states and territories regulate the operations of the critical infrastructure in their respective jurisdictions, this Act does not seek to disrupt or override the operation of such laws.

Section 16 – State constitutional powers

150. The Government acknowledges that ownership and operation of the highest-risk critical infrastructure assets captured under this Act resides primarily with state and territory governments. Section 16 confirms that powers under the Act will not be able to be exercised in a way that impairs the state’s capacity to exercise its constitutional powers. Although this restriction exists by way of the Melbourne Corporation principle, including it in the Act highlights the Government’s acknowledgement of this important principle.
Questions

3. The definition of *critical infrastructure asset* has been developed to only capture the most critical assets and thus minimise the regulatory burden. Are there other critical assets that should be captured, such as gas and data centre assets for example?

4. Does the definition of *reporting entity* adequately capture the scope of *direct interest holders* and *responsible entities* who can influence and control a *critical infrastructure asset*?
Part 2—Register of Critical Infrastructure Assets

Introduction

151. The Government works cooperatively and collaboratively with critical infrastructure owners, operators and regulators to identify national security risks and develop and implement mitigations for those risks. The Government has a well-developed understanding of threat, and is generally able to determine consequence. However, the Centre cannot undertake a comprehensive risk assessment without understanding how the asset and sector operates, and where there may be vulnerabilities. To determine what vulnerabilities may exist, it is essential to have a detailed understanding of who owns, controls and has access to a particular asset. However, the information required to develop this detailed understanding is not captured in a holistic way through any existing mechanisms or registers.

152. The establishment of the Register will assist the Government to gain greater visibility of who owns, controls and has access to our highest-risk critical infrastructure assets, including through Government’s collaborative risk assessments of critical infrastructure assets, particularly the risks of espionage, sabotage and coercion.

Division 1—Simplified outline of this Part

Section 17 – Simplified outline of this Part

153. The simplified outline is to assist readers to understand the substantive provisions, by providing an overview of the provisions within Part 2. Section 17 is not intended to be comprehensive and should not be relied on in place of the substantive provisions within Part 2.

154. This Part contains the provisions that create the Register of Critical Infrastructure Assets and outlines that the Secretary is responsible for administering the Register. The Register is designed to provide a more detailed understanding of who owns and controls critical infrastructure assets. The Register requires reporting entities, who are either direct interest holders or the responsible entity of critical infrastructure assets, to provide
interest and control information and operational information within a certain timeframe following any ‘notifiable event’ (defined in section 24). This information will assist the Government to identify who owns and controls the asset, its board structure, ownership rights of interest holders, and operational, outsourcing and offshoring information.

155. The interest and control information and operational information would form a baseline picture of ownership and control of critical infrastructure assets. This information would be used by the Government to inform risk assessments to identify national security risks for our highest-risk critical infrastructure assets. Where a potential risk has been identified, the Secretary has the power to obtain further information or documents to understand the risk (see Part 4, Division 2) and to issue a direction to a critical infrastructure asset to address a risk to national security (see Part 3, Division 2).

Division 2—Register of Critical Infrastructure Assets

Section 18—Secretary must keep Register

156. The Register is designed to improve the Government’s visibility of who owns, controls and has access to critical infrastructure assets to inform its assessments of assets most at risk from espionage, sabotage and coercion.

157. Section 18 provides that the Secretary is the responsible officer for administering the Register, which involves obtaining, adding, correcting or updating the information provided by reporting entities. The reporting entities have an obligation to give information and notify of events under Part 2, Division 3 of the Act.

158. While the administration of the Register is an important role, the Minister’s authority is not required. It is appropriate for the Secretary to be afforded the administrative responsibility for the Register. The Secretary, in comparison to the Minister, is better equipped to deal with the ongoing administrative requirements of maintaining the Register at the departmental level. The Secretary may also delegate this power in accordance with section 55.

Section 19 – Secretary may add information to Register

159. To ensure that the Register has all the relevant information about a critical infrastructure asset, this section provides the Secretary with the power to add additional information to the Register. The Secretary can add to the Register any operational information (defined in section 7) and interest and control information (defined in section 6) on a critical infrastructure asset.

160. This additional information may be acquired through open sources or as part of risk assessments conducted in consultation with critical infrastructure asset owners and operators, and other stakeholders, including state and territory governments. The additional information will assist Government:

- in understanding the risks to Australia’s critical infrastructure, including through conducting risk assessments, and
- where required, assist with the design and implementation of appropriate strategies to mitigate risks to national security.
Section 20 – Secretary may correct or update information in the Register

161. This section provides the Secretary with the authority to amend the information on the Register to ensure that it is accurate. The accuracy of the Register’s information is important as it will inform risk assessments and decisions taken by the Government on matters relating to mitigating risks to national security.

Section 21 – Register not to be made public

162. The Government recognises that the information on the Register may be commercially sensitive and detrimental to the commercial interests of direct interest holders, responsible entities and operators if the information is made public. To maintain confidentiality, the Act provides that any information provided to the Register falls within the definition of protected information in section 5. Falling within this definition ensures the information is subject to the authorised use and disclosure provisions in Division 3 of Part 4. This Division outlines the rules governing the authorised use, recording and disclosure of protected information. Section 43 provides an offence for the disclosure of protected information, including a penalty of two years imprisonment or 120 penalty units, or both.

163. In addition to the protections afforded by those provisions, this section requires the Secretary to ensure that the Register is not made public. This is designed to provide reporting entities with confidence that their commercially sensitive information will not be made public and only used in accordance with the provisions of the Act.

Division 3—Obligation to give information and notify of events

Section 22 – Initial obligation to give information

164. The purpose of this section is to outline the reporting obligations of the reporting entity for a critical infrastructure asset. The reporting entity, defined in section 5, means either the responsible entity for the asset and/or a direct interest holder in relation to the asset. The responsible entity is defined in section 5 and has sector specific meanings:

- for a critical electricity asset or a critical water asset—the entity that holds the licence, approval or authorisation (however described) to operate the asset to provide the service to be delivered by the asset
- for a critical port—the port operator (within the meaning of the MTOFSA) of the port
- an entity specified in a declaration by the Minister under section 49 as the responsible entity for a critical infrastructure asset, or
- an entity specified by the rules as a critical infrastructure asset for the purposes of paragraph 9(1)(e).

165. A direct interest holder is defined in section 8 as an entity with greater than 10% direct interest in the asset or who otherwise holds an interest that puts the entity in a position to directly or indirectly influence or control the asset.
166. Section 22 requires the **reporting entity** for a **critical infrastructure asset** to provide specified information on the **Register** within the **grace period**. The **grace period** is defined in section 5 as the six month period following an asset becoming a **critical infrastructure asset** to which the Act applies (or six months from commencement for those assets captured by the Act on commencement).

167. Subsection 22(2) sets out the information that each **reporting entity** must provide. Paragraph 22(2)(a) requires the **responsible entity** to provide the **operational information** for that asset. **Operational information** is defined in section 7 as information relating to the **responsible entity** and any other **entity** that is operating the asset or part of the asset on behalf of the **operator**. It specifically includes:

- the location of the asset
- a description of the area that the asset services, and
- for each **entity** that is the **responsible entity** for, or an **operator** of, the asset:
  - the name of the **entity**
  - address of the **entity**'s head office or principal place of business
  - incorporation details in Australia or another country
  - where the **entity** is incorporated, formed, created in another country, the name of that country, and
- details of the arrangement under which an **operator** is operating the asset.

168. Paragraph 22(2)(b) requires each **entity** that is a **direct interest holder** to provide the **interest and control information** in relation to that **entity** and the asset. **Interest and control information** is defined in section 6 and includes:

- the legal name of the first **entity**
- if applicable, the **ABN** of the first **entity**, or other similar business number (however described) if the first **entity** was incorporated, formed or created (however described) outside Australia
- for an **entity** other than an individual or body politic – the address of the first **entity**'s head office or principal place of business; and the country in which the first **entity** was incorporated, formed or created (however described)
- for an **entity** that is an individual – the residential address of the first **entity**; the country in which the first **entity** usually resides; and the country or countries of which the first **entity** is a citizen
- for an **entity** that is a body politic – the address of the first **entity**'s head office or principal place of business; and the country in which the first **entity** was formed or created (however described) as a body politic
- the type of interest (such as a legal, equitable, lease or licence interest) and level of the interest (shareholding) the first **entity** holds in the asset
- details on the influence and control that the first **entity** is in a position to directly or indirectly exercise in relation to the asset, such as voting rights and board appointments, and information on appointments to the body that governs the asset, and
details on any relevant interest and control information, as described above, about each other entity that is in a position to directly or indirectly influence or control the first entity. For the purposes of the Act, other entity is considered to be any ultimate interest holder or beneficial owner of the first entity.

169. The information to be captured on the Register is targeted at the information required by government to better understand who owns, controls and is in a position to influence the operation of our most critical infrastructure.

170. The information captured, specifically the interest and control information, will provide a picture of the extent of foreign involvement in the critical infrastructure asset. The reporting thresholds are consistent with the practices of the FIRB to identify material ownership interests. Ownership interests are often held in complex corporate structures, spanning multiple jurisdictions, or through trusts, managed funds or nominee companies. The requirement to provide information on who is ultimately in a position to control the asset is designed to ensure that those interests are not hidden in complex corporate structures. The direct interest holder will bear the responsibility of reporting these ultimate interests on the Register. Reporting who makes decisions, how they are made, the extent that decisions derive from specific shareholdings, and the circumstances in which shareholders are able to veto board decisions (indicators of direct and indirect control) will also be crucial to inform Government’s understanding of where risks may emanate from.

171. Further, while ownership is an important aspect, the degree of control and access through outsourcing and offshoring arrangements can also be difficult to establish, as they are often detailed in complex contractual arrangements. The operational information required to be provided by the responsible entity will provide Government with a greater understanding of the extent of foreign involvement in the critical infrastructure assets operation and control arrangements.

172. The details for the Register have been designed to balance the information required by Government to have a better understanding of who owns, controls and has access to critical infrastructure, with minimising the reporting requirements being placed on industry. Where the information provided suggests further investigation is required, the other powers of the Act will be utilised, including the power to request information (section 35) and the power to conduct a risk assessment (section 54).

173. Subsection 22(2) also outlines that where an eligible entity fails to comply with the obligations to provide information for the Register, it will attract 25 civil penalty points. This penalty is a proportionate response based on the infringement and is designed to deter non-compliance.

174. Subsection 22(3) sets out that the information must be provided in the approved form and no later than the end of the grace period or the end of 30 days after the entity becomes a reporting entity for the asset. The use of an approved form simplifies the process for providing the information and ensures there is consistency to the information that is provided for the Register. The 30-day timeframe ensures that reporting entities have an appropriate amount of time to understand and meet their obligations, while also providing Government with up-to-date interest and control information and operational information.
Section 23 – Ongoing obligation to give information

175. To ensure that the Register is kept up to date, section 23 outlines the ongoing obligations of reporting entities to give information. Specifically, subsection 23(1) outlines that the section, and therefore the ongoing obligation applies to a reporting entity if a notifiable event occurs in relation to the asset at any point after an entity has given information for the Register, even if that event falls within the grace period.

176. A notifiable event is defined in section 34 to mean any event that renders the information already provided for the Register to be incorrect or incomplete.

177. Subsection 23(2) outlines the obligations for a reporting entity where a notifiable event occurs. It outlines that the reporting entity must provide the Secretary with notice of the event and the information required to be provided in relation to that event in the approved form and within 30 days. The use of an approved form simplifies the process for providing the information and ensures there is consistency to the information that is provided for the Register. The 30-day timeline ensures that Government always has access to the most up-to-date information on Australia’s highest-risk critical infrastructure assets.

178. Subsection 23(2) also outlines that where a reporting entity fails to comply with the obligations of section 23, it will be liable to a civil penalty up to 25 penalty points. This penalty is a proportionate response based on the infringement and is designed to deter non-compliance to ensure the Register is accurate.

Subsections 23(3) and (4) and section 24 – Meaning of notifiable event

179. Subsection 23(3) contains a table which clearly outlines the information required to be given for each type of notifiable event covered by section 24.

180. Under section 24, there are two types of notifiable events which have different effects depending on the relevant reporting entity.

Event 1 – the event has the effect that the operational information or interest and control information becomes incomplete or incorrect.

181. In this event, items 1 and 2 in the table in subsection 23(3) outline the relevant reporting entities and the information they are required to provide. Where the information that becomes incomplete or incorrect is operational information, item 1 in the table requires the entity that is the responsible entity immediately after the event to provide any operational information that is required to correct or complete the operational information previously obtained by the Secretary.

Example

Company X, which owns a critical water asset, decides to change the operating arrangement for its water treatment facilities. In a new operating arrangement, Company X contracts with Company A to operate its treatment facilities. The operating arrangement results in Company A being one of the operators for Company X’s water asset. In accordance with paragraph 24(a)(i), Company X would need to report operational information about Company A to the Register as the existing operational information on the Register in incorrect.
182. Where the information that becomes incomplete or incorrect is interest and control information, item 2 in the table requires the entity, which is the direct interest holder to which the information relates, to provide any interest and control information in relation to that entity that is necessary to correct or complete the interest and control information previously obtained by the Secretary.

Example

Company X, which owns a critical port, is itself 51% owned by Company Y. Company Y is wholly-owned by Mr John Smith. Mr Smith decides to sell his 100% interest in Company Y to Mr Bill Williams. In accordance with paragraph 24(a)(ii), Company X as a direct interest holder in the critical port, would need to update its interest and control information on the Register to note that Mr Williams has a 100% interest in Company Y.

Event 2 – the event is an entity becoming a reporting entity for the asset, or a reporting entity for the asset becoming an entity to which this Act applies.

183. This event covers two potential scenarios. Under paragraph 24(b), a notifiable event is one where an entity becomes a reporting entity. This would include where an entity acquires a greater than 10% direct interest in the asset. Under paragraph 24(c), a notifiable event is one where a reporting entity becomes an entity to which the Act applies. This would include circumstances where an entity that does not fall within the definition of entity in section 5 changes its structure, for example, by becoming an incorporated body.

184. Items 3 and 4 in the table in subsection 23(3) outline the relevant reporting entities and the information they are required to provide for these events. Where the event relates to the responsible entity for the asset, item 3 in the table requires the responsible entity to give the operational information in relation to the asset.

Example

Company X, which owns an electricity distribution asset, decides against renewing its arrangement with the current asset operator. In a new arrangement, Company X engages Company A to be the entity that will hold the license to operate its electricity distribution asset. The licence arrangement results in Company A being the responsible entity for the electricity distribution asset. In accordance with paragraph 24(b), Company A would need to report its operational information to the Register.

185. Where the event relates to a direct interest holder, item 4 in the table requires the direct interest holder to provide the interest and control information in relation to that entity.
Example
Company X, which wholly owns an electricity generation asset within the meaning of paragraph 10(1)(b), decides to sell 25% of the asset to Company Y. Company Y is a new direct interest holder in the asset and therefore becomes a reporting entity for the purposes of the Act. As such, in accordance with subsection 24(b), it would need to report its interest and control information to the Register.

186. Subsection 23(4) clarifies the circumstances where an update to the Register is not required. This is where two events occur within the same 30 days and the second event has the effect of rending the information in relation to the first event incorrect. In these circumstances, the information relating to the first event is not required to be reported for the Register. For example, if the responsible entity changed twice within 30 days, if it had not already been reported when it changed for the second time, there would be no need to report the first change in the responsible entity.

Section 25 – Rules may exempt from requirement to give notice or information

187. The purpose of this section is to enable classes of entities or specified entities to be exempted from giving notice or information. Section 25 provides that the rules may provide that this Division, or specified provisions of this Division, do not apply in relation to:

- any entity
- specified classes of entities, or
- specified entities

either generally or in the circumstances prescribed by the rules.

Example
The Minister may use this rule-making power to prescribe that electricity transmission assets are no longer required to provide information for the purposes of the Register and as such are not bound by the obligations in section 23. In these circumstances, they will still be critical infrastructure assets for the purposes of the Act (and therefore still subject to a direction issued under section 30), but would not be obligated to update interest and control information or operational information on the Register.

Division 4—Giving of notice or information by agents

Section 26 – Requirement for executors and administrators to give notice or information for individuals who die

188. The purpose of this section is to ensure that the Register information is kept up to date in the event that an individual who is a reporting entity, dies. This section provides that if an individual, who is required by sections 22 or 23 to give notice and interest and control
information and/or operational information, dies before giving the notice and information, the executor or administrator of the individual’s estate must give the notice and information in accordance with that section. This ensures the accuracy of the information on the Register in circumstances where an individual is unable to fulfil their obligations.

Section 27 – Requirement for corporate liquidators to give notice or information

189. The purpose of this section is to ensure that the Register is kept up to date in the event of a corporate liquidation. This section provides that if a corporation required by sections 22 or 23 to give notice and information for the Register:

- is placed into voluntary administration, liquidation or receivership before giving the notice or information, and
- is no longer in a position to give the notice and information,

190. the voluntary administrator, liquidator or receiver of the corporation must give the notice or information in accordance with that section. This ensures the accuracy of the information on the Register even if a corporation, as a reporting entity, is unable to fulfil their obligation. This is particularly important to ensure Government has visibility of who has control of, and therefore is making decisions in relation to, the asset throughout the liquidation process.

Section 28 – Agents may give notice or information

191. The purpose of this section is to allow an agent to give notice or report information on an entity’s behalf. This section provides that where an entity is required by sections 22 or 23 to give notice or information, they are taken to have complied with the requirement if someone else gives the notice or information, in accordance with that section, on the entity’s behalf. This reduces the regulatory burden on reporting entities as it allows for a person such as a lawyer to act on the reporting entity’s behalf to meet information reporting obligations of the Register. It would also allow an agent to report all information in relation to an asset on behalf of all reporting entities for that asset.

Regulatory burden of the Register of Critical Infrastructure Assets

192. The regulatory burden of the Register’s reporting obligations would vary depending on the sector in which the critical infrastructure asset operates. Recognising this, and drawing on open source and other information available to Government, the regulatory burden is based on the following typical assumptions:

- Electricity generation, transmission and distribution assets each have two direct interest holders (a majority & minority holder) in addition to its responsible entity. Each direct interest holder has one ‘other entity’ on which it needs to report (see paragraph 6(1)(i)).
- Each port has two direct interest holders (a majority & minority holder) in addition to its responsible entity. Each direct interest holder has one ‘other entity’ on which it needs to report.
• Each water asset has two **direct interest holders** in addition to its **responsible entity** and two **operators**. The **direct interest holder** has no ‘other entity’.

• Each **direct interest holder** spends 2.5 hours providing the initial **interest and control information** and then 2.5 hours updating **interest and control information** when required.
  - The average period that a **direct interest holder** holds its interest in an asset is 4.3 years. Therefore, in the ten-year costing timeframe, reporting a change in a **direct interest holder** is assumed to happen 2.3 times.
  - The average period in which an ‘other entity’ holds an interest in a **direct interest holder** is 2.5 years. Therefore, in the 10 year costing timeframe, reporting a change in details of an ‘other entity’ is assumed to happen four times.
  - **Interest and control information** includes **direct interest holders’** details, name and citizenship details of board members, ownership thresholds and voting rights for board members, and access rights and privileges to operational systems and corporate network for board members.

• Each **responsible entity** spends 1.25 hours spent providing the initial **operational information** and then 1.25 hours to updating **operational information** when required.
  - On average, an electricity, water or port asset has 10.8 board members, with board members’ average tenure of 8.5 years. Therefore, in the ten-year costing timeframe, reporting a change in details of board members is assumed to happen 1.2 times.
  - One chief operating officer per asset, with average tenure of 7 years. Therefore, in the ten-year costing timeframe, reporting a change in the details of the chief operating officer is assumed to happen 1.4 times.
  - **Operational information** includes asset **operator** information, description of the regulated/licenced area of the asset, and name and citizenship details of the chief operating officer.
  - A **direct interest holder** may also be the **responsible entity** who reports operational information in the time taken above.

• Total costs are averaged out over a 10-year period.

193. Total annual once-off reporting costs of the required information for captured assets in the water, ports and electricity generation, transmission and distribution sectors is $9,544, or $110 per critical asset.

194. The annual cost of ongoing reporting of changes in the required information for assets in the three sectors is $13,383, or $155 per captured critical asset. These costs are averaged over a 10 year period.
### Average annual regulatory costs (from business as usual)

<table>
<thead>
<tr>
<th>Change in costs</th>
<th>Total change in cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>Electricity generation</td>
<td>$5,392</td>
</tr>
<tr>
<td>Electricity transmission/distribution</td>
<td>$8,368</td>
</tr>
<tr>
<td>Ports</td>
<td>$5,668</td>
</tr>
<tr>
<td>Water</td>
<td>$3,497</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>$22,927</strong></td>
</tr>
</tbody>
</table>

### Questions

5. Are there any barriers to companies providing the information required for the Register?

6. Are the costings and the underlying assumptions accurate or reflective of the costs that would be involved to meet the Register reporting obligations? Can you provide further quantification of the likely costs?
Part 3—Directions by the Minister

195. The Government is responsible for protecting Australia’s national security. With national security risks constantly evolving, it is the Government’s responsibility to work with the states, territories and industry, who own, operate and regulate our critical infrastructure to collaboratively develop a better understanding of how to best mitigate risks to national security. This collaborative approach is essential to better understand existing risk management controls, and to develop targeted mitigation strategies that leverage existing regimes where possible.

196. While the Centre will work collaboratively with reporting entities and operators to mitigate national security concerns, there are circumstances where the Government may need to take action if a reporting entity or operator does not cooperate to manage an identified national security risk.

197. This Part provides the Minister with the power to issue a direction to a reporting entity or operator to require them to take action to mitigate significant national security risks.

Division 1—Simplified outline of this Part

Section 29 – Simplified outline of this Part

198. The simplified outline is to assist readers to understand the substantive provisions, by providing an overview of the provisions within Part 3. Section 29 is not intended to be comprehensive and should not be relied on in place of the substantive provisions within Part 3.

199. The main feature of Part 3 is the Minister’s directions power, which is designed to only be able to be used in rare circumstances, where it is the only option available to manage a significant national security risk. This Part sets out the threshold for use of the power, the features of the power, and the safeguards to ensure the power is used proportionately and appropriately.

200. Noting that this Act is premised on cooperative engagement and collaboration, this power will only be used as a last resort. Government agencies will continue to engage in a cooperative manner with reporting entities and operators of critical infrastructure assets to manage national security risks. However, if national security risks cannot be managed on this basis, or through existing regulatory mechanisms, the Minister will be able to manage the risk by issuing a formal direction.

201. Alternatively, there may be circumstances in which a reporting entity for, or operator of, the critical infrastructure asset would prefer the certainty of a formal direction. For example, implementing security measures may increase the cost of a particular business decision where other options may be more commercially attractive. Fiduciary duties to shareholders can operate as a disincentive to invest in measures for the purpose of protecting national security interests. Additionally, a formal direction may also be taken into account by other regulators that govern what business costs may be passed on to consumers.
Division 2—Directions by the Minister

Section 30 – Direction if risk prejudicial to security

202. Part 3, Division 2 provides the Minister with the power to issue a direction to manage national security risks where this cannot be done on a cooperative basis, or through existing regulatory frameworks.

203. Subsection 30(1) outlines the basis upon which the Minister can exercise the directions power. The Minister needs to be satisfied of three elements:

- in connection with the operation of a critical infrastructure asset or the delivery of a service by a critical infrastructure asset
- there is a risk of an act or omission, and
- that risk would be prejudicial to security (within the meaning of the ASIO Act).

In connection with

204. This element ensures that the use of the direction is limited to manage risks that are connected to operations and services delivered by a critical infrastructure asset. This means that the power can only be used to manage risks in connection to a critical infrastructure asset that falls within the definition at section 9.

205. The use of ‘in connection with’ ensures the power is only used in respect of risks that arise from a connection with the delivery of a service by that asset or the asset’s operations (for example, a malicious insider). This does not mean that a direction cannot be used to manage vulnerabilities that may be acted on by third parties, however, the risk identified to trigger the use of this power, would still need to meet the ‘in connection with’ test.

206. For example, the Minister may issue a direction for an entity to implement extra cyber security measures to guard against data theft or unauthorised access to the asset’s control network through a legitimate connection to the asset. However, the direction may also incidentally protect against risks of external attacks as well, such as from an independent hacker.

207. ‘Operation’ and ‘delivery of service’ are broad terms, and are expected to be interpreted as such. Within a critical infrastructure asset, there are several parts that make up the operation of the asset or contribute to the delivery of service for that asset. This directions power can only be utilised where it can be shown that the ‘risk’ (discussed below) is in connection with the operation of delivery of service (i.e. the delivery of electricity). For example, board operations, management of systems data and operations controls would be ‘connected’ with the operation of, or delivery of a service by, a critical infrastructure asset.

208. The intention of the Act is to manage risks posed by malicious insiders, including foreign state actors, where, through their legitimate connection to the operations and delivery of service of a critical infrastructure asset, a risk exists, and that risk is prejudicial to security.
Example
Entity A is involved in the operation of Business X, and separately, a critical infrastructure asset. Entity A is the subject of an adverse security assessment in respect of its operation of Business X, with no risk identified to the critical infrastructure asset. The threshold for the exercise of the directions power is unlikely to be met.

Risks of an act or omission

209. To issue a direction, the Minister needs to be satisfied that there is a risk of any act or omission. This essentially means that there is a risk of an entity doing an active thing that would be prejudicial to security; or alternatively, a risk of an entity not doing something that would be prejudicial to security. These terms ensure that both active and passive risks are captured.

210. A practical example of an act would be where a person uses their legitimate access to a control system to conduct targeted acts of sabotage. This is an active risk because the risk requires positive action. Whereas an example of an omission would be the risk of failing to operate an electricity grid or failing to appropriately secure data. In these latter examples, the risk is not in relation to an act, but rather the failure to act, which is categorised here as an omission.

Prejudicial to security

211. The third limb is that the Minister must be satisfied that the identified risk of an act or omission (that exists in connection with the operation or delivery of service of a critical infrastructure asset) is, or would be, prejudicial to security. The term ‘prejudicial’ is given the same meaning as ‘activities prejudicial to security’, which is defined within the Attorney-General’s Guidelines in relation to the performance by the Australian Security Intelligence Organisation of its function of obtaining, correlating, evaluating and communicating intelligence relevant to security (including politically motivated violence), to mean activities relevant to security and which can reasonably be considered capable of causing damage or harm to Australia, the Australian people, or Australian interests, or to foreign countries to which Australia has responsibilities.

212. Security is given the same meaning as section 4 of the ASIO Act, which refers to the protection of the Australian Government, states, territories and the people of Australia from espionage, sabotage, attacks on Australia’s defence system, or acts of foreign interference, as well as the protection of Australia’s border integrity.

213. This limb ensures that the Minister’s directions power is properly limited to circumstances where he or she is satisfied that the risk that exists can reasonably cause harm to Australia, Australian people or Australian interests by prejudicing the ability to protect Australia from the specific matters of security that are listed within the definition of security. This element of the threshold ensures that the act or omission that leads to a risk must be of a significant enough magnitude before a direction can be issued. To demonstrate the risk is prejudicial to security, consideration would be given to the specific threat posed, as well as the vulnerability and consequence of that risk. For example, there may be a high-level threat posed to the operations of a particular critical infrastructure asset, but due to the
protections in place, there are minimal vulnerabilities. As such, in this scenario, no significant national security risk exists.

214. For example, in a case where data is stolen from an offshore data storage centre, the third limb would require demonstration that the risk of stealing data from offshore storage would prejudice the protection of Australia from one or more of the heads of security. That is, it would need to prejudice the protection of Australia from, for example, sabotage, to the extent that it could reasonably be considered capable of causing damage or harm to Australia, the Australian people, or Australian interests, or to foreign countries to which Australia has responsibilities. In this case, the data could relate to the operation of a particular critical infrastructure asset. The theft of this data and access to that information may provide a malicious actor with the knowledge required to conduct an act of sabotage, which could have the effect of causing damage or harm to Australia.

Issuing a direction

215. When the Minister is satisfied that the circumstances in subsection 30(1) exist, subsection 30(2) provides the specific power for the Minister to issue a written direction requiring a reporting entity (defined in section 5 as a direct interest holder or responsible entity), or operator of a critical infrastructure asset to do, or refrain from doing, an act or thing within a period of time specified in the direction. This ensures that, depending on the nature of the identified risk, the Minister is able to issue the direction to the entity best placed to take steps to manage the risk. As part of the direction, the Minister will provide the timeframe within which the entity must comply with the direction.

216. An example of a direction may be that the Minister directs a critical infrastructure asset operator to move currently stored offshore corporate and operating data to a more secure data storage provider. The direction will provide a specific timeframe within which the entity must comply. A further example of a direction is the Minister may direct a critical infrastructure asset owner to not outsource operations of its core network to certain providers. This direction may specify that the condition exists in perpetuity. Alternatively, the Minister may specify in the direction that the entity must consult the Government before entering into future outsourcing arrangements.

217. Given the range of national security risks that could arise, the directions power is designed to provide the Minister with the necessary scope to issue a direction that can sufficiently manage the risk. Recognising the breadth of the power, there are significant safeguards built into the use of the power at subsections 30(3), 30(4) and 31 to ensure that any direction issued is limited to the minimum required to manage the risk.

218. In addition to the factors upon which the Minister must be satisfied (subsection 30(1)), subsection 30(3) specifies further conditions that must be considered before the Minister can issue a direction. First, under paragraph 30(3)(a), the Minister must not give the direction unless satisfied that the direction is ‘reasonably necessary’ for the purposes of eliminating or reducing the risk at subsection 30(1). This is a proportionality test, and ensures the direction is limited to what is reasonably necessary to eliminate or reduce the national security risk identified, and importantly, does not require the entity to do, or refrain from doing, anything that is not necessary to address the specific risk.

219. Paragraph 30(3)(b) states that before issuing a direction, the Minister must be satisfied that reasonable good faith attempts have been made to reduce or eliminate the national security risk between relevant Government agencies and the direct interest holder,
**responsible entity** or **operator**. This requirement places an obligation on Government agencies to engage directly in good faith, wherever possible, with the affected **entity** to:

- ensure the **entity** is alert to, and understands:
  - the risk, and
  - the consequences of not managing the risk, and
- develop and implement appropriate measures that mitigate the risk to security and no more.

220. While not under the same specific obligation to negotiate in good faith as Government, the expectation would be that the affected **entity** will have similarly engaged in good faith to address the identified security risks.

221. Good faith in this context is intended to impose a requirement that engagement is genuine and solutions-focussed and that all reasonable options for addressing the risk are considered by both parties. This provision reinforces the objective of the Act, which is to facilitate a cooperative and collaborative government and industry partnership to manage national security risks in relation to **critical infrastructure assets**.

222. Paragraph 30(3)(c) requires the Minister to be given an **adverse security assessment** before issuing a direction. The **adverse security assessment** will set out in writing ASIO’s advice in respect of the exercise of the directions power by the Minister. An **adverse security assessment** is defined in section 35 of the ASIO Act and means a security assessment made by ASIO in respect of a person (including a company) that:

- any opinion or advice, or any qualification of any opinion or advice, or any information, that is, or could be, prejudicial to the interests of the person; and
- a recommendation that prescribed administrative action be taken, or not be taken, in respect of the person, being a recommendation the implementation of which would be prejudicial to the interests of the person.

223. The recommendation that must be attached to an **adverse security assessment** provides certainty that the risk to **security** identified is significant enough for ASIO to recommend specific action.

224. Further to the meaning of an **adverse security assessment** at section 35 of the ASIO Act, there is additional guidance on the characteristics of ASIO security assessments in the 2010 **ASIO Act Security Assessment Determination No.2**. This provides that security assessments should take into account three factors:

- the prescribed administrative action and the type of assessment (for example, what action is required and whether the assessment is an **adverse security assessment** that makes a recommendation for particular action)
- the assessment subject (who or what is the assessment about). An assessment of the subject would likely take into account the subject’s activities, associations, attitudes, and background, among other things, and
- consequences to **security** (**security** as defined under the ASIO Act). This requires consideration of the potential consequences to security if the prescribed administrative action is or is not taken.
In accordance with the accountability provisions contained within Part IV of the ASIO Act, the relevant *entity* may seek merits review of the *adverse security assessment* at the Administrative Appeals Tribunal. The Minister is required to provide a copy of the security assessment to the relevant *entity* within 14 days of receiving the assessment. The *adverse security assessment* must be accompanied by an unclassified statement of grounds setting out the information ASIO has relied on and a written notice informing the relevant *entity* of its right to apply to the AAT for merits review of the security assessment.

While subsection 30(3) sets out the matters that the Minister must be satisfied of before issuing a direction, subsection 30(4) sets out a range of further matters to which the Minister must have regard before issuing a direction. Having regard in this context means that those matters inform the substance of the direction.

Paragraph 30(4)(a) provides that the Minister must have regard to the *adverse security assessment* provided under paragraph 30(3)(c). While recognising the importance of the other factors in subsection 30(4), paragraph 30(5)(a) requires the Minister to give the greatest weight to the *adverse security assessment*. This ensures the significance of the security risk is given precedence over the other considerations outlined below.

Paragraph 30(4)(b) provides that the Minister must have regard to the use of any existing mechanisms, including regulatory systems at the federal, state and territory levels to eliminate or reduce the identified risk. For example, where the Government identifies mitigations to eliminate or reduce the national security risk, and this mitigation can be implemented through another federal regime or under a state or territory framework, such as a licencing regime, then the Government will work collaboratively with the bodies responsible for these regimes to implement the mitigation, before considering the use of the directions power under this Act. This is because in most cases, as the owners and regulators of *critical infrastructure assets*, states and territories would be best placed to manage the risk through their existing regulatory frameworks.

This provision reinforces the Government’s intention to continue to engage collaboratively to manage national security risks. This will avoid duplicating existing regimes where possible and takes advantage of the states’ and territories’ ability to leverage existing regulatory frameworks.

However, the Government is aware that there may be circumstances where the existing state-based regulatory regime is limited, and unable to be used to apply an identified mitigation. In these circumstances, following consultation with relevant states or other Government agencies, a formal direction may be the necessary course of action.

Paragraphs 30(4)(c) to (e) reinforce the intention that the directions power is to be used in a proportionate way, which takes into consideration the specific risk, the practical options for mitigating that risk, and the implications of those options. The factors the Minister must consider at paragraphs 30(4)(c) to (e) are the potential cost implications for an *entity* for complying with a direction, and the potential consequences that the direction may have on competition and customers of, or services provided by, the *relevant industry* of the *critical infrastructure asset*. Having regard to these factors will guard against imposing directions that would address security risks, but have an unnecessarily crippling effect on the *entity*, the *relevant industry* or impede market innovation and competition. The Government notes that the availability of reliable critical infrastructure promotes market confidence, and increases the attractiveness of Australia as an investment destination.
Critical Infrastructure Centre

232. Paragraph 30(4)(f) provides that the Minister must have regard to representations made by the entity under subsection 31(3). This ensures that as part of procedural fairness, the Minister gives due regard to the representations made by the relevant entity before issuing a direction.

233. Paragraph 30(5)(b) clarifies that the matters listed in subsection 30(4) are not intended to limit or prescribe the matters to which the Minister can have regard when exercising the power. This ensures that if there are other relevant factors specific to the consideration of a direction, they can also be taken into account by the Minister in determining whether to issue a direction. However, if they are, paragraph 30(5)(a) still requires the greatest weight to be given to the adverse security assessment.

Section 31 – Consultation before giving direction

234. To ensure that the directions power is exercised in a manner that complies with procedural fairness requirements, mandatory consultation requirements are part of the process before issuing a direction. This reinforces the Government’s intention to promote a collaborative approach to managing national security risks from foreign involvement in critical infrastructure assets and confirms that the directions power is a measure of last resort.

235. Subsection 31(1) recognises that states and territories as owners, operators and/or regulators of critical infrastructure assets share the responsibility with the Government to manage national security risks. States and territories are often best placed to mitigate national security risks through their existing regulatory frameworks. To reinforce the Government’s intention that this Act strengthens and formalises a collaborative approach to managing national security risks, subsection 31(1) provides that the Minister consult with the relevant state or territory minister before issuing a direction. This provision ensures the relevant minister has been directly consulted and is able to provide a formal state view on the proposed risk, how it could or should be addressed, including through a possible direction, and the impacts of such a direction.

236. Subsections 31(2) and (3) impose mandatory consultation with the entity that would be issued a direction. Under these subsections, the Minister is required to write to the entity and notify them of his or her intention to issue a direction, set out the terms of the proposed direction, and provide the entity the opportunity to make written representations about the proposed direction. Importantly, this requirement does not negate the requirement for earlier good faith negotiation with the entity to manage the security risk.
237. Paragraph 31(3)(a) outlines the minimum 28-day timeframe in which the Minister can require the relevant entity to provide written representations. The provision does not prevent the Minister from providing the relevant entity longer than 28 days in which to make representations. However, paragraph 31(3)(b) provides that a shorter timeframe can be stipulated where there are urgent circumstances requiring action to be taken within the 28-day timeframe. These provisions balance the need to properly engage with, and provide an opportunity for the affected entity to make representations, with the need to address the national security risks in a timely manner.

238. While this provision provides the entity with the ability to make representations, it does not limit what representations can be made (other than requiring the representations to be in writing). The relevant entity should set out in their representations any reasons as to why they do or do not agree with the proposed direction. This might include, but is not limited to, disagreement that the identified risk exists or disagreement with the mitigations specified in the Minister’s proposed direction (in part or in full). The entity could also make representations on other mechanisms that could be used to mitigate the risk. Given the Minister is required to consider factors such as the potential cost and impact on the entity and consumers, it will also be desirable for representations to address these matters.

239. Subsection 31(4) clarifies that section 31 does not restrict the Minister from consulting other persons. For example, given the nature and potential impacts of a direction, it may be appropriate that the Minister consult with other Commonwealth ministers, such as the Minister for Foreign Affairs and Trade where there are international sensitivities, the Prime Minister and the minister responsible for the relevant industry.

Section 32 – Requirement to comply with direction

240. An entity is required to comply with a direction issued to them by the Minister under this Act. Non-compliance with the Minister’s direction will attract a pecuniary penalty of 250 civil penalty units for each day of non-compliance as prescribed in subsection 93(2) of the Regulatory Powers Act. Enforceable undertakings and injunctions as prescribed in the Regulatory Powers Act are also available as enforcement measures to compel compliance with a direction under this Act.

241. These enforcement measures, particularly the number of penalty units, are commensurate with non-compliance measures for similar directions powers under the TSSR and reflect the significance of the national security risks that would be left unmitigated if a direction was not complied with.

Section 33 – Exception—acquisition of property

242. Section 33 provides that any direction issued by the Minister under subsection 30(2) cannot result in an acquisition of property as defined under the Constitution (which also gives rise to an obligation to compensate a property owner). An entity is exempt from complying with the Minister’s direction to the extent that the outcome of compliance results in the Government acquiring property. If an entity wishes to rely on this exemption, the entity has the burden of presenting evidence to substantiate this claim.
Regulatory burden of the directions power

243. The regulatory costs of issuing a last resort direction would vary widely depending on the scope of the direction and the individual circumstances of the entity subject to the direction. However, to ensure the directions power operates effectively and is appropriately targeted, Government is interested in the views of stakeholders on the cost impacts of possible directions.

244. To assist in providing indicative costs, four different scenarios have been modelled. Two tables have been provided for each scenario. The first table for each scenario draws on the following assumptions to provide a regulatory impact across all critical infrastructure assets:

- across the four scenarios, it is assumed that a direction will only be used once every three years
- each scenario has been assigned an equal probability of 25%
- within each scenario, the 25% probability is split between the 12 entity types (small, medium, large by electricity (generation), electricity (transmission/distribution), ports, and water), and
- a medium and a large entity is twice as likely to be issued a direction than a small entity.

245. The second table for each scenario provides the one-off cost for each asset type if the direction was issued in relation to that asset.

246. The costings provided have been developed using information available to Government, and drawing from open source information. The total annual expected regulatory burden, averaged out over each scenario, sector and entity size based on the assumptions above (including using the power once every three years) and across a 10 year costing timeframe, is $9.38 million.

Scenario 1: Direction to move and store all data in an Australian Signals Directorate (ASD) certified cloud services provider, assuming the company currently stores all its corporate and operating data offshore.

247. Table 1(a) provides that the annual compliance burden for captured asset owners and operators in the electricity, water and ports sectors is $396,655.

248. The following activities and assumptions have contributed to calculating the annual compliance burden:

- Costs of breaking contract with current data storage provider.
  - The 12 entity types and sizes are classified on the complexity of their data holdings (low to very high) and amount of data held (very small to very large). For example, a very small data holding is 10TB, a small data holding is 60TB.
- Costs associated with procurement activities for a new data storage provider.
  - Before the direction, the entity stored its data with a non-ASD approved data storage provider. A procurement cost of $375,000 is assumed.
- Costs for data mitigation.
- It could reasonably take approximately 8 x FTE 12 months to migrate 10TB of data (very high complexity data).

- Ongoing data storage service costs.
  - Non-ASD approved storage provider cost of $15.26 per TB/month. ASD approved storage provider cost of $74.11 per TB/month to use the new provider’s data centre.
  - A multiplier based on the amount of data held.

- Independent compliance audit.
  - Assumed cost of approximately $60,000 with a frequency of 0.3 per year.

### Table 1(a) – Average annual regulatory costs (from business as usual)

<table>
<thead>
<tr>
<th>Change in costs ($Z)</th>
<th>Entity size</th>
<th>Costs to entity</th>
<th>Total sector change in cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>Electricity generation</td>
<td>Small</td>
<td>$2,673</td>
<td>$26,575</td>
</tr>
<tr>
<td></td>
<td>Medium</td>
<td>$8,424</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Large</td>
<td>$15,477</td>
<td></td>
</tr>
<tr>
<td>Electricity transmission/distribution</td>
<td>Small</td>
<td>$23,838</td>
<td>$223,691</td>
</tr>
<tr>
<td></td>
<td>Medium</td>
<td>$74,608</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Large</td>
<td>$125,244</td>
<td></td>
</tr>
<tr>
<td>Ports</td>
<td>Small</td>
<td>$4,481</td>
<td>$49,105</td>
</tr>
<tr>
<td></td>
<td>Medium</td>
<td>$16,123</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Large</td>
<td>$28,500</td>
<td></td>
</tr>
<tr>
<td>Water</td>
<td>Small</td>
<td>$9,514</td>
<td>$97,282</td>
</tr>
<tr>
<td></td>
<td>Medium</td>
<td>$31,987</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Large</td>
<td>$55,781</td>
<td></td>
</tr>
<tr>
<td>Total, by sector</td>
<td></td>
<td></td>
<td>$396,655</td>
</tr>
</tbody>
</table>

### Table 1(b) – One-off costs for scenario 1

<table>
<thead>
<tr>
<th>Electricity generation</th>
<th>Small</th>
<th>$64,155.41</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Medium</td>
<td>$101,098.18</td>
</tr>
<tr>
<td></td>
<td>Large</td>
<td>$185,728.34</td>
</tr>
<tr>
<td>Electricity transmission/distribution</td>
<td>Small</td>
<td>$572,126.04</td>
</tr>
<tr>
<td></td>
<td>Medium</td>
<td>$895,304.88</td>
</tr>
<tr>
<td></td>
<td>Large</td>
<td>$1,502,931.32</td>
</tr>
<tr>
<td>Ports</td>
<td>Small</td>
<td>$107,554.86</td>
</tr>
</tbody>
</table>
Table 1(b) – One-off costs for scenario 1

<table>
<thead>
<tr>
<th></th>
<th>Medium</th>
<th>Large</th>
</tr>
</thead>
<tbody>
<tr>
<td>Water</td>
<td>$193,476.35</td>
<td>$342,009.93</td>
</tr>
<tr>
<td></td>
<td>$228,342.43</td>
<td>$669,372.69</td>
</tr>
</tbody>
</table>

Scenario 2: Direction requiring a business to limit any offshore access to its industrial control systems unless approved by Government. In this scenario, it is assumed there is already significant offshore access.

249. Table 2(a) outlines that the annual compliance burden for captured asset owners and operators in the electricity, water and ports sectors is $67,955.

250. The following activities and assumptions have contributed to calculating the annual compliance burden:

- Costs of monitoring offshore access for SCADA issues.
  - 60 SCADA incidents requiring offshore vendor access each year. Based on 30 SCADA incidents a month, 15 of which are resolved in-house, 10 of which are escalated to the local integrator (not requiring offshore access), and five are escalated to the offshore vendor each month. 3.75 hours spent monitoring offshore vendor access to the SCADA system.
  - One SCADA software update each year requiring offshore vendor access. Based on four SCADA software updates a year. Two hours spent monitoring offshore vendor access for a SCADA software update.

- Costs of preparing an assessment of the issue.
  - Frequency of 60 a year, given 60 SCADA issues requiring offshore vendor access. Two IT specialists spend 3.75 hours each preparing an assessment of the issue before escalating to the SCADA vendor.

- Organising communications with the vendor.
  - Frequency of 61 a year, given 60 SCADA issues, and one SCADA software update requiring offshore vendor access. One IT specialist spends 0.25 hours organising a time to open the portal with the provider.

- Developing a protocol for offshore access.
  - Protocol development time increases with complexity of SCADA system, and thus, with larger business size. Frequency of 0.1 a year, given protocol would only need to be developed once. Two IT specialists spend one week working on protocol development, given protocol for vendor SCADA access should already be defined, so new protocol relates to any change in interaction between provider and entity due to limited SCADA access.

- Cost of external audit.
  - Assumed cost of approximately $60,000 with a frequency of 0.3 per year.
### Table 1(a) – Average annual regulatory costs (from business as usual)

<table>
<thead>
<tr>
<th>Change in costs ($Z)</th>
<th>Entity size</th>
<th>Costs to entity</th>
<th>Total sector change in cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>Electricity generation</td>
<td>Small</td>
<td>$2,338</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Medium</td>
<td>$4,425</td>
<td>$11,022</td>
</tr>
<tr>
<td></td>
<td>Large</td>
<td>$4,258</td>
<td></td>
</tr>
<tr>
<td>Electricity transmission/distribution</td>
<td>Small</td>
<td>$5,413</td>
<td>$25,061</td>
</tr>
<tr>
<td></td>
<td>Medium</td>
<td>$10,074</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Large</td>
<td>$9,572</td>
<td></td>
</tr>
<tr>
<td>Ports</td>
<td>Small</td>
<td>$2,953</td>
<td>$13,830</td>
</tr>
<tr>
<td></td>
<td>Medium</td>
<td>$5,555</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Large</td>
<td>$5,321</td>
<td></td>
</tr>
<tr>
<td>Water</td>
<td>Small</td>
<td>$3,876</td>
<td>$18,041</td>
</tr>
<tr>
<td></td>
<td>Medium</td>
<td>$7,250</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Large</td>
<td>$6,915</td>
<td></td>
</tr>
<tr>
<td>Total, by sector</td>
<td></td>
<td></td>
<td>$67,955</td>
</tr>
</tbody>
</table>

### Table 2(b) – One-off costs for scenario 2

<table>
<thead>
<tr>
<th>Entity size</th>
<th>Small</th>
<th>Medium</th>
<th>Large</th>
</tr>
</thead>
<tbody>
<tr>
<td>Electricity generation</td>
<td>$56,118.85</td>
<td>$53,107.13</td>
<td>$51,099.32</td>
</tr>
<tr>
<td>Electricity transmission/distribution</td>
<td>$129,932.78</td>
<td>$120,897.62</td>
<td>$114,874.18</td>
</tr>
<tr>
<td>Ports</td>
<td>$70,881.64</td>
<td>$66,665.23</td>
<td>$63,854.29</td>
</tr>
<tr>
<td>Water</td>
<td>$93,025.82</td>
<td>$87,002.38</td>
<td>$82,986.75</td>
</tr>
</tbody>
</table>
Scenario 3: Direction preventing a business from outsourcing the operations of its core network to certain low-cost, less secure providers.

251. Table 3(a) outlines that the annual compliance burden for captured asset owners and operators in the electricity, water and ports sectors is $3.82 million.

252. The following activities and assumptions have contributed to calculating the annual compliance burden:

- Costs of breaking contract with current SCADA provider.
  - Assuming the entity has 1.5 years remaining in its three year contract and the annual maintenance fee is 15% of the SCADA set up cost from a low-quality provider (high-quality provider cost premium of 20%).
  - High-quality SCADA cost of $50,000,000. Low-quality SCADA cost of $41,666,667.
  - Low-quality SCADA annual maintenance cost of $6,250,000. Thus, contract break cost for the 10 year costing timeframe is $6,250,000 x 1.5 years.

- Costs associated with procurement for new SCADA system.
  - A procurement cost of $500,000 is assumed.

- Costs of new SCADA system – initial setup and ongoing maintenance (software updates).
  - $50,000,000 cost for a new SCADA system. The regulatory burden is calculated as the cost difference in maintenance costs between a low-quality ($6,250,000) and high-quality SCADA provider ($7,500,000).

- External audit.
  - Assumed cost of approximately $60,000 with a frequency of 0.3 per year.

<table>
<thead>
<tr>
<th>Table 3(a) – Average annual regulatory costs (from business as usual)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Change in costs ($Z)</strong></td>
</tr>
<tr>
<td>--------------------------</td>
</tr>
<tr>
<td>Electricity generation</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Electricity transmission/distribution</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Ports</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Water</td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>
### Table 3(a) – Average annual regulatory costs (from business as usual)

<table>
<thead>
<tr>
<th></th>
<th>Large</th>
<th>$604,607</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total, by sector</td>
<td></td>
<td>$3,823,940</td>
</tr>
</tbody>
</table>

### Table 3(b) – One-off costs for scenario 3

<table>
<thead>
<tr>
<th></th>
<th>Small</th>
<th>$786,541.04</th>
</tr>
</thead>
<tbody>
<tr>
<td>Electricity generation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Medium</td>
<td>$2,224,041.04</td>
<td></td>
</tr>
<tr>
<td>Large</td>
<td>$3,661,541.04</td>
<td></td>
</tr>
<tr>
<td>Electricity transmission/distribution</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Small</td>
<td>$2,224,041.04</td>
<td></td>
</tr>
<tr>
<td>Medium</td>
<td>$6,536,541.04</td>
<td></td>
</tr>
<tr>
<td>Large</td>
<td>$10,849,041.04</td>
<td></td>
</tr>
<tr>
<td>Ports</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Small</td>
<td>$1,074,041.04</td>
<td></td>
</tr>
<tr>
<td>Medium</td>
<td>$3,086,541.04</td>
<td></td>
</tr>
<tr>
<td>Large</td>
<td>$5,099,041.04</td>
<td></td>
</tr>
<tr>
<td>Water</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Small</td>
<td>$1,505,291.04</td>
<td></td>
</tr>
<tr>
<td>Medium</td>
<td>$4,380,291.04</td>
<td></td>
</tr>
<tr>
<td>Large</td>
<td>$7,255,291.04</td>
<td></td>
</tr>
</tbody>
</table>

**Scenario 4:** *Direction preventing a business from sourcing core operational systems technology from certain low-cost, less secure providers.*

253. Table 4(a) outlines that the annual compliance burden for captured asset owners and operators in the electricity, water and ports sectors is $5.09 million.

254. The following activities and assumptions have contributed to calculating the annual compliance burden:

- **Cost of breaking contract with current communications infrastructure provider.**
  - Current low-quality provider managed network service fee of $55 per month per intelligent device. 5000 intelligent devices assumed for the asset.
  - Thus, the contract break cost is (5000 x $55)/2 = $137,500 once-off.

- **Cost associated with procurement activities for new communications infrastructure provider.**
  - $300,000 for cost of procuring a new managed network service provider (to maintain intelligent devices).

- **Ongoing cost difference between old and new communications infrastructure provider.**
- High-quality cost is assumed at $100 a month per device, low-quality cost is $55 a month per device.
- Thus, annual cost difference is $45 x 5000 x 12.

- Costs associated with procurement activities for new communications infrastructure material (intelligent devices).
  - $250,000 for cost of procuring new intelligent devices.

- Cost of intelligent devices.
  - $20,000 cost for a new intelligent device for a large electricity (transmission/distribution) company.
  - 17,000 intelligent devices for a large electricity (transmission/distribution) company, assuming an intelligent device on every street of a large city.

- Costs to train staff in new intelligent devices.
  - 50 staff requiring one week of training for a large electricity (transmission/distribution) company.

- Cost of Independent compliance audit.
  - Assumed cost of approximately $60,000 with a frequency of 0.3 per year.

### Table 4(a) – Average annual regulatory costs (from business as usual)

<table>
<thead>
<tr>
<th>Change in costs ($Z)</th>
<th>Entity size</th>
<th>Costs to entity</th>
<th>Total sector change in cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>Electricity generation</td>
<td>Small</td>
<td>$4,082</td>
<td>$153,367</td>
</tr>
<tr>
<td></td>
<td>Medium</td>
<td>$32,061</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Large</td>
<td>$117,223</td>
<td></td>
</tr>
<tr>
<td>Electricity transmission/distribution</td>
<td>Small</td>
<td>$285,278</td>
<td>$4,544,843</td>
</tr>
<tr>
<td></td>
<td>Medium</td>
<td>$1,421,043</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Large</td>
<td>$2,838,521</td>
<td></td>
</tr>
<tr>
<td>Ports</td>
<td>Small</td>
<td>$3,122</td>
<td>$28,048</td>
</tr>
<tr>
<td></td>
<td>Medium</td>
<td>$9,636</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Large</td>
<td>$15,289</td>
<td></td>
</tr>
<tr>
<td>Water</td>
<td>Small</td>
<td>$24,605</td>
<td>$371,789</td>
</tr>
<tr>
<td></td>
<td>Medium</td>
<td>$117,055</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Large</td>
<td>$230,128</td>
<td></td>
</tr>
<tr>
<td>Total, by sector</td>
<td></td>
<td></td>
<td>$5,098,048</td>
</tr>
</tbody>
</table>
Table 4(b) – One-off costs for scenario 4

<table>
<thead>
<tr>
<th>Service</th>
<th>Category</th>
<th>Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>Electricity generation</td>
<td>Small</td>
<td>$97,969.62</td>
</tr>
<tr>
<td></td>
<td>Medium</td>
<td>$384,737.48</td>
</tr>
<tr>
<td></td>
<td>Large</td>
<td>$1,406,683.92</td>
</tr>
<tr>
<td>Electricity transmission/distribution</td>
<td>Small</td>
<td>$6,846,683.92</td>
</tr>
<tr>
<td></td>
<td>Medium</td>
<td>$17,052,523.23</td>
</tr>
<tr>
<td></td>
<td>Large</td>
<td>$34,062,255.42</td>
</tr>
<tr>
<td>Ports</td>
<td>Small</td>
<td>$74,928.54</td>
</tr>
<tr>
<td></td>
<td>Medium</td>
<td>$115,634.79</td>
</tr>
<tr>
<td></td>
<td>Large</td>
<td>$183,478.54</td>
</tr>
<tr>
<td>Water</td>
<td>Small</td>
<td>$590,541.04</td>
</tr>
<tr>
<td></td>
<td>Medium</td>
<td>$1,404,666.04</td>
</tr>
<tr>
<td></td>
<td>Large</td>
<td>$2,761,541.04</td>
</tr>
</tbody>
</table>

Questions

7. Are there any barriers for reporting entities and operators to engage cooperatively with the Australian Government to implement mitigations to address identified national security risks?
   - Would the level of cooperation change if there are significant cost implications for the business?

8. Do the safeguards in the Bill provide industry with sufficient confidence that the directions power is a true last resort that can only be exercised when risks cannot be managed through cooperation or existing regulatory mechanisms?

9. Are the costings and the underlying assumptions accurate or reflective of the costs that would be involved in complying with the potential directions proposed in this document? Can you provide further quantification of the likely costs?
Part 4—Gathering and using information

255. The Government’s ability to identify, manage and respond to national security risks is dependent on having access to information on who owns, controls and has access to, or is in a position to influence, the operation of critical infrastructure assets. While the Government works closely with owners, operators and investors to obtain this information, some stakeholders may be reluctant or restrained from providing this information. This Act provides the Secretary with an information-gathering power which compels the provision of information or documents.

256. The power is to be exercised in circumstances where a reporting entity or operator is restrained from sharing information for contractual or other legal issues, or otherwise refuses to cooperate.

257. The compulsion element has the effect of authorising the disclosure of personal information under the Privacy Act (i.e. the disclosure is authorised by law) and offers a statutory protection for breach of confidentiality provisions in contracts.

Division 1—Simplified outline of this Part

Section 34 – Simplified outline of this Part

258. The simplified outline is to assist readers to understand the substantive provisions, by providing an overview of the provisions within Part 4. Section 34 is not intended to be comprehensive and should not be relied on in place of the substantive provisions.

259. The main feature of Part 4 is the Secretary’s power to require reporting entities and operators of critical infrastructure to provide information or documents where the Secretary reasonably believes that such information or documents are relevant or may assist in the exercise of duties, functions and powers under the Act.

260. The matters to which the Secretary must have regard before issuing a notice for information, as well as administrative measures relating to complying with the notice, and penalties for non-compliance are contained in the Part.

261. The information provided to the Secretary is protected information under the Act. Use and disclosure of protected information is restricted in line with provisions at Part 4, Division 3.

262. To ensure an entity complies with a notice issued by the Secretary, the Act provides broad protections for individuals against criminal or civil proceedings if the information is self-incriminating.
Division 2—Secretary’s general power to obtain information or documents

Section 35 & 38 – Secretary may obtain information or documents from entities, and self-incrimination

263. Subsection 35(1) empowers the Secretary to request certain information from reporting entities (direct interest holders, responsible entities) and operators of critical infrastructure assets. The section limits the use of the information gathering powers to the following, in line with the purpose and objects of the Act:

- where the information or document is relevant to exercising a power, or the performance of a duty or function under the Act, or
- where the information or document may assist in determining whether a power under this Act should be exercised in relation to the asset.

264. Paragraph 35(1)(a) refers to information or documents that may be relevant to:

- the Secretary’s duty and function to keep a Register under section 18
- the Minister’s power to issue a direction under subsection 30(2), or
- the Secretary’s power to undertake an assessment of a critical infrastructure asset to determine if there is a national security risk under section 54.

265. Under section 18, the Secretary is required to keep a Register of Critical Infrastructure Assets containing certain information. Further, Part 2 of this Act requires reporting entities to provide interest and control information and operational information to assist the Government to understand and assess national security risks.

266. To ensure the Secretary is able to meet these obligations, this provision will enable the Secretary to issue a notice to obtain information or documents to assess compliance with the reporting obligations for the Register, which will ensure that the information provided by reporting entities is correct and up to date.

267. Additionally, in line with the objects of the Act and section 54 (undertaking an assessment of a critical infrastructure asset), the information gathering power in this paragraph will allow further information to be sought, where that information is required to gain a clearer national security risk picture in respect of the critical infrastructure asset.

268. Similarly, paragraph 35(1)(b) would apply if the Secretary required further information relevant to determining whether to exercise a power under this Act. For example, this power could be used to obtain further information about the way a critical infrastructure asset operator manages an aspect of the asset’s operations to assist the Minister in making a decision on whether to issue a direction. It could also be used to assist with the performance of the Secretary’s power under section 54 to conduct a national security risk assessment of a critical infrastructure asset.

269. The information gathering power has been drafted with reference to the Administrative Review Council’s twenty best practice principles for implementing and exercising information gathering powers in its 2008 report, Coercive Information Gathering Powers of Government Agencies. In particular, the information gathering power is limited
to obtaining information or documents that are directly relevant to the purposes of the legislation, as stated in the objects of the Act, as well as the functions, duties, powers and purposes prescribed in the Act.

270. In circumstances where the section applies (as set out in subsection 35(1)), subsection 35(2) provides that the Secretary may require, by notice in writing, the entity to provide information or a document that meets the requirements in subsection 35(1). The notice may require the documents or information to be provided directly, or through the provision of copies of documents, rather than original versions of requested documents. The notice must also clearly set out the period within which the documents or information must be provided and the manner in which it has to be provided (including the ways outlined above).

271. Recognising the potential impost on business of complying with such a notice, subsection 35(3) requires the Secretary to consider the potential costs to an entity in complying with the notice. The Secretary may also have regard to other matters, including the time required to comply and other impacts on the business. In practice, Government agencies will engage with the relevant entity prior to issuing a notice to try and obtain the information voluntarily and, if necessary, discuss the terms of the notice. This will ensure that wherever possible the notice directly targets the information sought and does not create unnecessary expense or burden on the entity. However, in circumstances where it is not feasible or necessary to engage the entity or operator prior to issuing the notice, a failure to engage or consult will not affect the validity of the notice as it is not a pre-condition for issuing the notice.

272. Subsection 35(4) provides that an entity issued with a notice under subsection (2) to produce information or documents must comply with that notice. Subsection 35(4) is a civil penalty provision that is enforceable under Part 4 of the Regulatory Powers Act (civil penalty provisions); Part 6 of the Act (enforceable undertakings); and Part 7 of the Act (injunctions). Non-compliance with the Minister’s notice will attract a pecuniary penalty of 250 civil penalty units for each day of non-compliance as prescribed in subsection 93(2) of the Regulatory Powers Act.

273. This penalty is commensurate with the non-compliance measure for a similar information gathering power under the TSSR. The penalty also reflects the significance of obtaining information relevant to assessing a national security risk to a critical infrastructure asset, noting that the critical infrastructure assets captured under this Act represent the highest-risk water, electricity and ports assets.

274. Furthermore, under section 38, a notice must be complied with even if it exposes the person (an individual or a body corporate) to criminal or civil liability. This has been modelled on the Evidence Act 1995, which abolishes the privilege against self-incrimination for bodies corporate, including where the body corporate is required to answer a question, give information or produce a document under a law of the Commonwealth. The common law privilege against self-incrimination only extends to natural persons, not to bodies corporate.

275. However, subsection 38(2) provides broad protections for individuals against criminal or civil proceedings if the information is self-incriminating. It clarifies that the documents or information cannot be used in evidence in any criminal or civil proceedings against the individual with the exception of Commonwealth criminal proceedings for providing false or misleading information or documents or civil proceedings to recover a penalty for non-
critical infrastructure Centre

compliance with the exercise of the information gathering power itself. This does not prevent the information or document being used if obtained through other means unrelated to this Act.

276. Subsection 35(5) sets out the requirements for a notice issued by the Secretary under subsection 35(2). Subsections 35(2) and 35(5) have the effect of requiring the Secretary to make any request for information and documents in writing, specifying the information or document required and the timeframe in which the information or document is required. In line with the Coercive Information Gathering Powers of Government Agencies Report 2008, subsection 35(5) also requires the notice to outline the effect of certain provisions relating to non-compliance with the notice and offences under the Criminal Code for providing false or misleading information. This ensures that the entity understands the consequences of failure to comply with a notice issued under section 35, including the criminal consequences for providing misleading or false information.

277. Given the potential sensitivity of information required to be provided to the Secretary under section 35, the Act sets out provisions for how and when information obtained under the Act can be used, retained and further disclosed to other persons (Part 4, Division 3).

278. Subsection 35(6) provides that if an entity provides copies of documents in compliance with a requirement under paragraph 35(2)(c), the entity is entitled to be paid reasonable compensation by the Government.

Section 36 – Copies of documents

279. Section 36 recognises that the documents or information that may be sought might also be required by the business. As such, this section provides flexibility as to how the Secretary may consider documents that have been requested. Subsection 36(1) enables the Secretary to inspect a document produced under section 35 and make and retain copies as necessary. Confidentiality of retained documents would be protected information under provisions governing the use and disclosure of documents and information held for official purposes. Subsection 36(2) also enables the Secretary to retain any copies of documents that are produced under paragraph 35(2)(c). This recognises that the Secretary should be able to retain those copies for the purposes for which they were requested noting the entity providing the copies will still retain the originals.

Section 37 – Retention of documents

280. Under section 37, the Secretary may retain possession of copies of documents obtained under section 35 for as long as he or she deems necessary. This would enable the document to be used for the purpose for which it was obtained, as well as for any other purpose authorised under Part 4, Division 3.

281. In circumstances where a document is retained, subsection 37(2) requires the Secretary to provide a certified copy of the original documents to the person who is entitled to possess the document that was produced pursuant to the notice. Additionally, under subsection 37(4), until such time as the certified copy is produced the Secretary must provide reasonable access to inspect and make copies of the document.
282. Finally, subsection 37(3) confirms that the certified copy of the document, if received in a court or tribunal, is to be dealt with as if it were the original document.

Division 3—Use and disclosure of protected information

283. Division 3 sets out how protected information obtained under this Act may be shared and disclosed. All information obtained under the Act, such as information provided for the Register or obtained through the Secretary’s power under section 35, is protected information. It is a criminal offence to use or disclose protected information other than as authorised by this Division.

Subdivision A—Authorised use and disclosure

Section 39 – Authorised use and disclosure—performing functions, etc

284. Section 39 provides that a person may make a record, use or disclose protected information if it is for the purposes of performing the person’s functions, duties or powers under this Act. A person may also make a record, use or disclose the protected information if it is for the purpose of ensuring compliance with a provision in this Act. Some examples include:

• Information obtained under the Secretary’s information gathering power for the purposes of a national security risk identified may be used to determine whether information on the Register is up to date.
• Information on the Register may be required by Government agencies for assessing a national security risk and determining whether to issue a direction.

• The information may be required to be shared with a relevant entity or person such as a state or territory Minister for the purpose of consulting them on the possible issuing of a direction.

Section 40 – Authorised use and disclosure—other person’s functions, etc

285. While the information obtained under this Act is specifically collected for national security purposes, the information may be relevant to the exercise of other powers or purposes related to a critical infrastructure asset or relevant industry. Section 40 authorises the Secretary to disclose protected information in circumstances where the information would assist the person to whom it is being disclosed to exercise their powers, functions or duties.

286. Subsections 40(1) and (2) combined enable protected information to be disclosed to:

• a Commonwealth minister, the head of an agency or an officer or an employee of that agency administered by the Minister and/or a member of staff of a minister who is responsible for any of the following:
  - national security – for the purposes of informing and understanding the national security environment and the development of policies related to national security
  - foreign investment in Australia – for the purposes of informing and understanding foreign investment by providing relevant information such as sources of foreign investment, types of assets attracting investment and the level of investment
  - taxation policy – for the purposes of informing taxation policies particularly related to ensuring entities and operators meet taxation obligations
  - industry policy – for the purposes of informing wider industry policies and objectives
  - promoting investment in Australia – for the purposes of informing policies related to promoting foreign investment in Australia by providing relevant information such as sources of foreign investment, assets attracting investment and the level of investment
  - defence – for the purposes of informing defence activities, and
  - regulation or oversight of any relevant industry for the critical infrastructure asset – for the purposes of ensuring those industries have access to information relevant to the overall resilience of their sector.

287. Subsection 40(1) combined with paragraphs 40(2)(b), (c) and (d) allows the sharing of information obtained under this Act with states and territories. This is in keeping with the Act’s objective to promote a collaborative and cooperative approach to managing national security risks.

288. The Act specifically enables information to be disclosed to a state or territory minister responsible for oversight of the relevant industry for that particular critical infrastructure asset; that minister’s staff; agencies or departments administered by that minister; and officers or employees of such agencies or departments.
289. The information obtained under the Act may have broader policy implications for states and territories, particularly in relation to maintaining the security and resilience of critical infrastructure assets. This acknowledges that the states and territories, as owners and regulators of critical infrastructure assets share the responsibility with the Government to manage national security risks.

290. Disclosure is made at the discretion of the Secretary, and must be for the purpose of enabling or assisting the person to exercise their powers, functions or duties. Authorising disclosures in these circumstances strikes a balance between recognising that the protected information may be sensitive, with reinforcing the collaborative approach to managing national security risks.

Section 41 – Authorised disclosure relating to law enforcement

291. Section 41 provides that the Secretary may disclose protected information to an enforcement body (within the meaning of the Privacy Act) if the Secretary believes it is reasonably necessary for one or more enforcement related activities (within the meaning of that Act) conducted by or on behalf of the enforcement body.

292. The definition of ‘enforcement body’ in the Privacy Act includes the Australian Federal Police, a police force or service of a state or territory, the Office of the Director of Public Prosecutions or a similar body established under a law of a state or territory, the Australian Criminal Intelligence Commission, the Australian Prudential Regulation Authority, and the Australian Securities and Investment Commission. The definition of ‘enforcement related activity’ in the Privacy Act includes (among other activities) the prevention, detection, investigation, prosecution or punishment of criminal offences or breaches of a law imposing a penalty or sanction; the conduct of surveillance activities; intelligence gathering activities or monitoring activities and the protection of public revenue. Allowing disclosure in these circumstances is consistent with the object of this Act to manage national security risks relating to critical infrastructure.

293. An authorised disclosure in these circumstances is at the discretion of the Secretary. It is not a mandatory requirement.

Section 42 – Secondary use and disclosure of protected information

294. Persons who have been provided information under section 40 may further disclose protected information if it is for the purposes for which they initially received the information. For example, the Secretary may disclose protected information relating to a critical water asset to a state minister responsible for water, for the purpose of discharging his duty as minister responsible for that sector. If the relevant state minister is provided information for these purposes, then he or she may further disclose the information to other persons (for example, officers in a local council that has responsibilities in relation to the critical water asset), but only where that disclosure is connected to the oversight of that sector.
Subdivision B—Offence for unauthorised use or disclosure

Section 43 – Offence for unauthorised use or disclosure of protected information

295. This section makes it an offence for a person to record, disclose or otherwise use protected information unless the making of the record, disclosure, or use is authorised by Subdivision A or an exception applies.

296. Information provided under the Register obligations or obtained through the information gathering power, in respect of the highest-risk sectors of critical infrastructure, is likely to be sensitive in nature. Aggregation of the information will also increase its sensitivity and value. To appropriately deter unauthorised disclosure, noting the very real national security risks that such a disclosure may pose, it is appropriate that criminal offences apply. Imposing a criminal offence of imprisonment for two years, 120 penalty units or both is in keeping with similar regimes that obtain sensitive industry information.

297. Subsection 43(2) notes that section 15.1 of the Criminal Code will apply to an offence against subsection 43(1). Section 15.1 of the Criminal Code imposes extended geographical jurisdiction – Category A. This means the offence will extend to Australian citizens regardless of where in the world they are when they engage in conduct that contravenes subsection 43(1).

Section 44 – Exceptions to offence for unauthorised use or disclosure

298. Section 44 provides a range of appropriate defences to an offence of unauthorised disclosure of protected information. These defences are where the disclosure is:

- authorised under a Commonwealth law (excluding authorised disclosures under Subdivision A or subsection 49(3))
- authorised under a state or territory law prescribed in the rules;
- disclosed in good faith in attempting to comply with provisions relating to authorised disclosure under Subdivision A or subsection 49(3), or
- to a person to whom the protected information relates, or with their express or implied consent.

299. Recognising the severity of a criminal sanction as the highest form of punishment or deterrence, these exceptions ensure that the criminal penalty does not extend to situations where there is no criminal culpability, such as in complying with another law, or disclosing the information with the consent of the person to whom the information relates.

300. Given the exceptions act as a legal defence, the evidential burden of these matters lies with the defendant. This is prescribed under section 13.3(3) of the Criminal Code, which states that a defendant who wishes to rely on any exception, exemption, excuse, qualification or justification provided by the law creating an offence bears an evidential burden in relation to that matter. An ‘evidential burden’ in relation to a matter means the burden of adducing or pointing to evidence that suggests a reasonable possibility that the matter exists or does not exist.
Section 45 – No requirement to provide information

301. Section 45 clarifies that a person cannot be required to provide *protected information* to a court, tribunal or other authority that can require the production of documents or testimony, except where it is necessary to do so for the purpose of giving effect to this Act. This provision protects the sensitivity of the information from being revealed in court proceedings that are not in relation to the operations of this Act.
Part 5—Enforcement

302. This Part outlines the enforcement measures available to the Government if the civil penalty provisions within this Act are contravened.

303. The Government intends to promote cooperative and collaborative working relationships with reporting entities and operators to obtain interest and control information and operational information and proportionately manage national security risks. However, in the event that such an approach fails, the Government will be able to enforce compliance through the civil penalty provisions in this Act. While the enforcement measures are civil, not criminal in nature, the Government considers this appropriate when considering the potential nature of the breaches envisaged. For example, where the breach is in relation to providing information to the Register, or a failure to comply with a direction, financial penalties under a civil penalty order, or an injunction to require performance, are sufficient penalties to deter contravention and achieve the objects of this Act.

Division 1—Simplified outline of this Part

46 Simplified outline of this Part

304. The simplified outline is to assist readers to understand the substantive provisions, by providing an overview of the provisions in Part 5. Section 46 is not intended to be comprehensive and should not be relied on in place of the substantive provisions in Part 5. It outlines that civil penalty orders may be sought for contravening aspects of the Act, undertakings may be accepted and enforced, and injunctions may be used to restrain action, through triggering the application of certain parts of the Regulatory Powers Act.

Division 2—Civil penalties, enforceable undertakings and injunctions

47 Civil penalties, enforceable undertakings and injunctions

305. Part 5, Division 2 contains the enforcement measures that can be used in circumstances where there has been a contravention of a civil penalty provision in this Act. Under
subsection 47(1), the Minister or Secretary has the discretion of seeking one or a combination of the following enforcement measures, through an application to a relevant court:

- **Civil penalty provision** – enforceable under Part 4, Regulatory Powers Act. The Minister or Secretary would be able to seek a civil penalty order from the relevant court for the person to pay the Government a pecuniary penalty in line with the civil penalty units assigned to the civil penalty provision.

- Enforceable undertakings – enforceable under Part 6, Regulatory Powers Act. An enforceable undertaking allows the Minister or Secretary to accept an undertaking relating to compliance with a civil penalty provision. The Minister or Secretary can then seek an order from a relevant court to direct compliance with the undertaking, seek any financial benefit from the failure to comply with the undertaking to be surrendered; or seek an order for damages.

- Injunctions – enforceable under Part 7, Regulatory Powers Act. Depending on the contravention, the Minister or Secretary may apply to a court seeking one of the following injunction orders:
  - Restraining injunction – to restrain a person from engaging in conduct (where the person has engaged, is engaging, or is proposing to engage, in conduct) that would be in contravention of a civil penalty provision.
  - Performance injunction – to compel a person who has refused or failed to do a thing that is required under a civil penalty provision to do that thing.
  - Interim injunction – to be issued as an interim measure to either restrain a person from engaging in conduct; or requiring a person to do a thing, while the court determines whether to issue a restraining or performance injunction.

306. These enforcement measures afford the Minister or Secretary the flexibility to determine the most appropriate course of action, allowing consideration of the contravention, and its impact on achieving the objects of this Act. For example, the Minister is likely to issue a performance injunction if an entity is unwilling to abide with a direction from the Minister to do or not do a thing under subsection 30(2) of the Act. In these cases, the true last resort nature of the directions power reiterates the importance of a reporting entity or an operator, of a critical infrastructure asset complying with any direction that is issued to mitigate a national security risk. Accordingly, ensuring performance in line with the direction would be the paramount objective, and this can be facilitated through an injunction measure. The pecuniary penalties that can be enforced under enforceable undertakings and civil penalty orders will act to deter and punish an entity from contravening a civil penalty provision.

307. The Minister or Secretary may seek an enforcement measure if an entity that is a reporting entity of a critical infrastructure asset contravenes one of the following provisions of this Act:

- subsection 22(2) – which requires the reporting entity to initially register interest and control information and/or operational information through the approved form.
- subsection 23(2) – which requires the reporting entity to update interest and control information and operational information through the approved form if the information initially provided to the Secretary is out of date or incorrect because of a notifiable event.
308. The Minister or Secretary may seek an enforcement measure if an **entity** that is a **reporting entity** or **operator** of a **critical infrastructure asset** contravenes one of the following provisions of this Act:

- subsection 30(2) – which requires a **reporting entity**, or an **operator** of, a **critical infrastructure asset** to comply with a direction issued to them by the Minister.

- subsection 35(2) – which provides that an **entity** that is a **reporting entity** for, or **operator** of, a **critical infrastructure asset** may be issued with a notice to produce information or documents, and it must comply with that notice.

309. Subsections 47(2) and (3) prescribes the Minister and Secretary as the authorised applicants and authorised person for the purposes of the **civil penalty provisions** in this Act in line with powers provided in Parts 4, 6 and 7 of the Regulatory Powers Act. This means that seeking an enforcement measure under this Act will require an application to the relevant court by the Minister or Secretary. These two authorities are appropriate, given that they are the two persons that have duties, powers or functions under this Act.

310. Subsection 55(1) provides that the Secretary may, by written instrument, delegate his or her powers, functions or duties under this Act to an SES employee, or an acting SES employee in the Department. This means that, with the written authority of the Secretary, an SES employee or an acting SES employee may institute proceedings in a relevant court seeking an enforcement measure under this Act.

311. Subsection 47(4) prescribes the ‘relevant courts’ in which the Minister or Secretary may make an application seeking an order for an enforcement measure to be applied. The relevant courts are:

- the Federal Court of Australia
- the Federal Circuit Court of Australia, or
- a state or territory court that has jurisdiction in relation to matters arising under this Act.

312. Prescribing these courts as the ‘relevant courts’ is in keeping with the Attorney-General’s Department’s policy that jurisdiction should, wherever possible, be conferred as widely as appropriate to ensure that disputes can be resolved in the lowest level of court, and allows the workload resulting from new legislation to be distributed fairly. There is not a justifiable reason in this instance for limiting the jurisdiction of this Act to a particular court.

313. Noting that some court proceedings that may be initiated under this Act will deal with information that is sensitive for national security purposes, this information can be protected through the common law of public interest immunity or under the NSI Act.

314. Subsection 47(5) provides that under this Act, the operation of Parts 4, 6 and 7 of the Regulatory Powers Act, extend outside Australia. Given the operation of this Act triggers the Regulatory Powers Act, it is important to ensure consistency of jurisdiction across all the provisions under this Act. This Act has extended application outside Australia, as provided at 13, therefore the effect of 47(5) is to ensure the enforcement measures triggered in Parts 4, 6 and 7 of the Regulatory Powers Act have the same application.
Part 6—Declaration of assets by the Minister

315. This Act applies to critical infrastructure assets captured by the definition in section 9. Paragraph 9(1)(d) explicitly provides that an asset can be privately declared under section 49 to be a critical infrastructure asset. This Part provides the basis upon which such a declaration can be made.

Division 1—Simplified outline of this Part

Section 48 – Simplified outline of this Part

316. The simplified outline is to assist readers to understand the substantive provisions by providing an overview of the provisions within Part 6. Section 48 is not intended to be comprehensive and should not be relied on in place of the substantive provisions within Part 6.

317. The main feature of Part 6 is power for the Minister to privately declare a particular asset to be a critical infrastructure asset for the purposes of this Act. Importantly, if an asset is declared, it then falls within the operation of the Act. However, as this is a private declaration, this Part requires the Minister to notify each reporting entity for a declared asset so they are aware of their reporting obligations.

Division 2—Declaration of assets by the Minister

Section 49 – Declaration of assets by the Minister

318. Subsection 49(1) outlines the basis upon which the Minister can privately declare an asset to be a critical infrastructure asset for the purposes of the Act.

319. The first limb is that the asset is not otherwise a critical infrastructure asset. This refers to the other limbs of the definition of critical infrastructure asset in section 5, being a critical electricity asset, as defined in section 10; a critical port as defined in section 11; a critical water asset as defined in section 5; or an asset prescribed by the rules.

320. The second limb is that the asset relates to a relevant industry. Relevant industry is defined in section 5 as electricity, water and ports industries, as well as any industry prescribed by the rules. This limb ensures that the Minister can only declare an asset as a critical infrastructure asset if it is directly relevant to an industry already regarded by the Act to be a high-risk sector. It also provides certainty to assets outside of those sectors that this power cannot be used to make a declaration that will affect them.

321. The third limb is that the Minister must be satisfied that the asset is critical infrastructure that affects national security and there would be a risk to national security if it were publicly known that the asset is critical infrastructure that affects national security.
322. This limb is the most important component of the test and sets the parameters within which a declaration can be made. It limits declarations to circumstances where there would be significant national security risks if were publicly known that the critical infrastructure asset affects national security.

323. For example, an electricity generation asset could be supplying electricity to an asset that is essential for a national security purpose, but that asset’s connection to a national security purpose is not known publicly. In these circumstances, it is important that the Act applies to the asset so that the interest and control information and operational information is captured on the Register and the directions power is able to be used. However, this section will ensure that there is not public visibility of the link between the critical infrastructure asset and national security.

324. Subsection 49(2) requires the declaration to specify the entity that is the responsible entity for the asset. An entity is defined in section 5 and refers to the entity with ultimate operational responsibility for the asset.

325. Subsection 49(3) requires the Minister to notify each reporting entity for the asset of the declaration in writing within 30 days of making the declaration. This Act imposes obligations on reporting entities in relation to an asset to provide a range of information. This subsection ensures that reporting entities in relation to a declared asset are aware of their obligations. Direct interest holders (defined in section 8) for the declared asset will be required to report their interest and control information (as defined in section 6) and the responsible entity (as specified in the declaration as a result of subsection 49(2)) will be required to report operational information (defined in section 7) for the asset.

326. Importantly, the grace period of six months will apply from the date on which the asset is declared. This ensures the reporting entities have sufficient time to understand and comply with their obligations in relation to the Register.

327. The notification to reporting entities under subsection 49(3) may also outline other obligations to which the reporting entities may be subject to under the Act, such as an information gathering request (section 35) or a direction issued under section 30.

328. The Minister’s declaration of an asset is also protected information as per paragraph (b) of that definition in section 5. As such, the unauthorised disclosure of the fact that an asset is declared, or any information obtained under this Act related to the asset will be an offence and attract the relevant penalties in accordance with the relevant penalty provisions. This ensures that information obtained by the Government under this Act is afforded the appropriate protections, given the sensitivities of the information and the criticality of the asset for security.

329. Subsection 49(4) provides that a declaration under subsection (1) is not a legislative instrument. The declaration under subsection 49(1) does not fall within the meaning of a legislative instrument under subsection 8(1) of the Legislation Act 2003 as it does not determine or alter the law set out in the Act. Rather, it determines particular cases and circumstances in which the law will apply. The inclusion of subsection 49(4) is to assist readers and avoid doubt in this respect.
Part 7—Miscellaneous

Division 1—Simplified outline of this Part

Section 50 – Simplified outline of this Part

330. The simplified outline is to assist readers to understand the substantive provisions, by providing an overview of the provisions within Part 7. Section 50 is not intended to be comprehensive and should not be relied on in place of the substantive provisions within Part 7.

331. Part 7 details the reporting requirements on the operation of this Act. The Secretary will be required to give the Minister a report each financial year for presentation to the Parliament. This Part also details other matters which are important to the functioning of this Act including the delegation of powers and rules.

Division 2—Treatment of certain entities

Section 51 – Treatment of partnerships

332. This section sets out how the Act applies to partnerships, including apportioning legal liability for offences and civil penalty provisions under this Act. This is required because partnerships themselves do not have a separate legal identity.

333. Subsection 51(1) provides that the Act applies to a partnership as if it were an entity, but with the changes set out in this section. Under paragraph 8(2)(b), an entity is a direct interest holder in relation to an asset if the entity is a partnership where one or more partners hold the interest on behalf of the partnership.

334. Subsection 51(2) provides that an obligation that would otherwise be imposed on the partnership by this Act is imposed on each partner instead, but may be discharged by any of the partners. This section provides clarity as to how a partnership is to meet its obligations under this Act (the obligations may be discharged by any of the partners).

335. Subsection 51(3) provides that an offence against this Act that would otherwise have been committed by the partnership (for example, disclosure of protected information) is taken to have been committed by each partner in the partnership, at the time the offence was committed, who:

- did the relevant act or made the relevant omission; or
- aided, abetted, counselled or procured the relevant act or omission; or
- was in any way knowingly concerned in, or party to, the relevant act or omission (whether directly or indirectly, and whether by any act or omission of the partner).

336. This provision imposes joint liability on partners by ensuring that an offence committed by one or more partners of a partnership is an offence committed by all other partners of the partnership to the extent that they were directly engaged in, or otherwise involved in or aware of, the conduct.
Subsection 51(4) extends the application of the section to the contravention of a civil penalty provision in a corresponding way to the way in which it applies to an offence. This provision imposes joint liability on partners by ensuring that where a civil penalty provision is incurred by one or more partners of a partnership (for example, not complying with a direction issued under section 30), the civil penalty provision is incurred by all other partners of the partnership.

Subsection 51(5) outlines that for the purposes of this Act, a change in the composition of a partnership does not affect the continuity of the partnership. This section ensures that where a new partner is admitted, or partner retires or dies, the Act considers that the partnership continues unaffected.

Section 52 – Treatment of trusts and superannuation funds that are trusts

This section sets out how the Act applies to trusts and superannuation funds, including apportioning liability for offences and civil penalty provisions against this Act. Subsection 52(1) provides that the Act applies to a trust or a superannuation fund that is a trust as if it were an entity, but with the changes set out in this section. Under paragraph 8(2)(a), an entity is a direct interest holder in relation to an asset if the entity is a trust where one or more trustees hold the interest on behalf of the beneficiaries of the trust. Similarly, under paragraph 8(2)(c), an entity is a direct interest holder in relation to an asset if the entity is a superannuation fund that is a trust where one or more trustees hold the interest on behalf of the beneficiaries of the superannuation fund. A superannuation fund is defined in section 5 as having the same meaning given by section 10 of the Superannuation Industry (Supervision) Act 1993.

Subsection 52(3) provides that if the trust or superannuation fund has two or more trustees:

- an obligation that would otherwise be imposed on the trust or superannuation fund by this Act is imposed on each trustee instead, but may be discharged by any of the trustees, and

- an offence against this Act that would otherwise have been committed by the trust or superannuation fund is taken to have been committed by each trustee of the trust or superannuation fund, at the time the offence was committed, who:

  - did the relevant act or made the relevant omission; or
  - aided, abetted, counselled or procured the relevant act or omission; or
  - was in any way knowingly concerned in, or party to, the relevant act or omission (whether directly or indirectly and whether by any act or omission of the trustee).

Subsections 52(2) and (3) ensure that the provisions of this Act are placed on the trustee or trustees of a trust or superannuation fund as a legal person, as a trust or superannuation fund themselves do not have a separate legal identity. In circumstances of two or more trustees, joint liability is imposed on trustees by ensuring that an offence committed by one or more trustees of a trust or superannuation fund is committed by all other trustees of that trust or superannuation fund to the extent that they were directly engaged in, or otherwise involved in, or aware of, the conduct. This ensures that there is clarity as to the individual who bears the responsibility to comply with obligations under the Act and also who is subject to an offence or penalty provision if the Act is contravened in any way.
342. Subsection 52(4) extends the application of the section to the contravention of a civil penalty provision in a corresponding way to the way in which it applies to an offence. This provision ensures that where a civil penalty provision is incurred by one or more trustees of a trust or superannuation fund, the civil penalty provision is incurred by each trustee of the trust or superannuation fund.

Section 53 – Treatment of unincorporated foreign companies

343. The purpose of this section is to set out how the Act applies to unincorporated foreign companies, including apportioning legal liability for offences and civil penalties against this Act. Subsection 53(1) provides that the Act applies to an unincorporated foreign company as if it were an entity, but with the changes set out in this section. Under subsection 8(2)(d), an entity is a direct interest holder in relation to an asset if the entity is an unincorporated foreign company with one or more appointed officers who hold the interest on behalf of the company. An unincorporated foreign company is defined in section 5 as a body covered by paragraph (b) of the definition of foreign company in section 9 of the Corporations Act 2001. An appointed officer is also defined in section 5 to include the secretary of the company, or an officer of the company appointed to hold property on behalf of the company.

344. Subsection 53(2) provides that an obligation that would otherwise be imposed on the unincorporated foreign company by this Act is imposed on each appointed officer for the company instead. It also clarifies that any of the appointed officers are able to discharge their obligations. This section ensures that the provisions of this Act are placed on the appointed officer as a legal person, as unincorporated foreign companies themselves do not have a separate legal identity.

345. Subsection 53(3) provides that an offence against this Act that would otherwise have been committed by the unincorporated foreign company is taken to have been committed by each appointed officer for the company, at the time the offence was committed, who:

- did the relevant act or made the relevant omission, or
- aided, abetted, counselled or procured the relevant act or omission, or
- was in any way knowingly concerned in, or party to, the relevant act or omission (whether directly or indirectly and whether by any act or omission of the appointed officer).

346. This provision imposes joint liability on each appointed officer of the unincorporated foreign company by ensuring that an offence committed by one or more appointed officers is an offence committed by all other appointed officers of the unincorporated foreign company to the extent that they were directly engaged in, or otherwise involved in or aware of, the conduct. This ensures that there is clarity as to the individual who bears the responsibility to comply with obligations under the Act, and also who is subject to an offence or penalty provision if the Act is contravened in any way.

347. Section 53(4) extends the application of the section to the contravention of a civil penalty provision in a corresponding way to the way in which it applies to an offence. This provision imposes joint liability on appointed officers of an unincorporated foreign company ensuring that a civil penalty provision is incurred by all other appointed officers of the unincorporated foreign company.
Division 3—Matters relating to Secretary’s powers

Section 54 – Additional power of the Secretary

348. Section 3 outlines the object of this Act, which is to provide a framework for managing national security risks relating to critical infrastructure. In line with this overarching objective, section 54 provides the Secretary with the power to undertake an assessment of a critical infrastructure asset to determine if there is a national security risk.

349. This power is in addition to, and does not limit, any of the other powers or functions under this Act. In particular, this section complements the other provisions in the Act in ensuring that information obtained for the Register, or in response to an information gathering request, are able to be used by the Secretary in conducting a risk assessment. This will inform whether there are mitigations required for a particular asset, in turn informing decision-making on the use of the Minister’s directions power (Part 3, Division 2).

350. Importantly, while not explicit in the provision, in line with the objects in section 3, any risk assessment conducted by the Secretary would be conducted in collaboration with the asset’s owners and operators, as well as relevant state and territory agencies and regulators.

Section 55 – Delegation of Secretary’s powers

351. Subsection 55(1) allows the Secretary to delegate his or her powers, functions or duties under this Act to an Senior Executive Service (SES) employee, or an acting SES employee, in the department. The Secretary’s powers, functions and duties under this Act are:

- to keep a Register of Critical Infrastructure Assets
- information-gathering power, and
- authority to institute enforcement proceedings for non-compliance with obligations under the Act.

352. Allowing the Secretary to delegate these matters to an SES officer provides for more timely and effective action under the Act, noting that access to the Secretary may be compromised by other matters. For example, it may be more appropriate that an SES officer of the department be responsible for the day-to-day management of the Register.

353. Subsection 55(2) outlines that any officer performing functions under a delegation is compelled to only act as authorised by that delegation. This ensures the powers or functions authorised by SES officers cannot go beyond the scope of the Act.

Division 4—Periodic reports and rules

Section 56 – Periodic report

354. Part 7, Division 4 details the Secretary’s reporting obligation to the Minister on the operation of this Act. The periodic reporting will ensure the Government reports to Parliament (and therefore publicly) on the operation of this Act, including details of how many times the powers in the Act have been used in the financial year.
355. Subsection 51(1) requires the Secretary to report to the Minister each financial year on the operation of the Act. Subsection 56(1) requires this report to be presented to Parliament.

356. Subsection 56(2) outlines the matters which must be dealt with in the report. These include:

- the number of notifications in respect of the Register obligations to provide interest and control information and operational information (Division 3 of Part 2)
- the use of the Minister’s directions power at subsection 30(2)
- the use of the Secretary’s information gathering power at section 35
- any enforcement action taken relating to failures to comply with obligations under the Act, and
- the number of assets declared as critical infrastructure assets under section 49.

357. This annual overview on the operation of the Act provides accountability and transparency of the Act’s application to critical infrastructure assets, including how often the powers are used.

358. Despite subsection 56(2) listing the matters that must be in the report, this does not prevent or limit the matters that can be dealt with in the report.

359. Subsection 56(3) provides that the report must not include any personal information within the meaning of the Privacy Act, which provides personal information to be information or an opinion about an identified individual, or an individual who is reasonably identifiable.

Section 57 – Rules

360. Section 57 provides the general rule-making power in the Act. Providing for a general instrument-making power under an Act is a long-standing practice. This is to allow certain matters, as prescribed under the Act, to be provided for in subordinate legislation where appropriate.

361. The authority to make such rules is vested with the Minister, and relates to matters that are required or permitted by the Act to be prescribed in rules, or where such rules are necessary or convenient to give effect to the Act. Rules form part of the Act in line with the definition of this Act in section 5.

362. There are general principles that govern what matters are best dealt with in an Act as opposed to rules. The types of matters that, by way of policy, should not be prescribed in rules are clarified in section 57(2) and include creating an offence, imposing a tax, and directly amending the text of the Act.

363. There are a range of provisions in the Act that specifically provide for rules to be made, including:

- details about what is meant by interest and control information (paragraph 6(1)(j))
- details about what is meant by operational information (paragraph 7(1)(f))
- prescribing assets for the purposes of the definition of critical infrastructure asset (paragraph 9(1)(e)), and
• the requirements for an electricity generation station to be critical (subsection 10(2)).

364. These matters (and others in the Act) have been determined to be suitable to be dealt with through the making of a rule because they are matters that may require amendment over time, and are not of sufficient importance to have to be dealt with through amendments to the Act.
Security of Critical Infrastructure Rules

365. Section 57 of the Act provides that the Minister may, by legislative instrument, make rules prescribing matters that are required, or permitted to be prescribed, by the rules, or necessary or convenient to be prescribed for carrying out, or giving effect to, the Act. Subsection 57(2) clarifies that the rules may not, however, create an offence or civil penalty, provide arrest, detention, entry, search or seizure powers, impose a tax, set an appropriation amount from the Consolidated Revenue Fund under an appropriation in this Act, or directly amend the text of the Act.

366. Subsection 10(2) of the Act provides that for the purposes of paragraph 10(1)(b), the rules may prescribe requirements for an electricity generation station to be critical to ensuring the security and reliability of electricity networks in a particular state or territory. This matter is prescribed in rules rather than the Act to take account of changing technologies and shifts in the energy market that may change which generators are critical to the security and reliability of electricity networks. This subsection allows the Government to make any necessary amendments in a timely manner.

Rule 1 – Name

367. This rule provides that the title of the rules is the Security of Critical Infrastructure Rules 2017.

Rule 2 – Commencement

368. This rule provides for the whole of this instrument to commence on either the day after this instrument is registered, or the day after the Security of Critical Infrastructure Act 2017 commences, whichever is later.

369. Given the Security of Critical Infrastructure Act 2017 is the authorising Act for the rules, the rules cannot come into effect until the Act has commenced. Accordingly, this rule confirms that if these rules are registered before the Act commences, the rules will not be taken to have commenced until the Act has come into effect. If the Act commences and these rules have not been registered, then the rules will come into effect the day after it is registered.

Rule 3 – Authority

370. These rules are made and authorised under the Security of Critical Infrastructure Act 2017.

Rule 4 – Definitions

371. Act means the Security of Critical Infrastructure Act 2017, being the Act that enables the rules to be made, and noting that section 5 of the Security of Critical Infrastructure Act 2017 provides that references to ‘this Act’ include the rules.

372. Synchronous electricity generator means a generator that produces electricity via a rotating shaft with a stator and rotor that is directly connected to the electricity system or network.
by electromagnetic coupling at a speed equivalent to the frequency of the electricity system or network.

373. While this is a technical definition, synchronous generators are most commonly coal, gas and hydroelectric generators. Synchronous generators are important for frequency control and system strength in electricity networks. Electricity network reliability depends on carefully balanced supply and demand to control power system frequency. If frequency deviates from a specified range, consumer and generation equipment can malfunction or be damaged.

374. *System restart ancillary service* is given its meaning at subsection 5(2), which is discussed further below where Rule 5 is explained.

**Rule 5 – Requirements for electricity generation stations**

375. Paragraph 5(1)(a) states that an electricity generator station that provides a system restart ancillary service is a generator station that is considered to be critical to ensuring the security and reliability of electricity networks to a particular state or territory. *System restart ancillary service* is defined in Subsection 5(2).

376. Paragraph 5(1)(b) states that a synchronous electricity generator (defined in Rule 4 above) that has an installed capacity of at least the amount specified in the table for each state or territory is captured under the Act. The thresholds are:

- New South Wales – 1400MW
- Victoria – 1200MW
- Queensland – 1300MW
- Western Australia – 600MW
- South Australia – 600MW
- Tasmania – 700MW, and
- Northern Territory – 300MW.

377. These jurisdictional thresholds are supported by the AEMO and are consistent with the MW capacities held in reserve for each jurisdiction within the system (i.e. the system is designed to be able to withstand the loss of this level of MW capacity). Accordingly, the loss of input above these thresholds could cause critical instability in the system, resulting in security and reliability issues, or cascading failures leading to widespread blackouts.

378. Subsection 5(2) provides a definition of a system restart ancillary service to be an electricity generation station that is able to start without an external power supply and to connect and provide energy to an electricity system or network for the transmission of electricity. This service is provided by selected and contracted electricity generators. They provide an option for AEMO to restart generators in the electricity network and ultimately commence restoration of load. System restart may be possible in the absence of these contracted generators, but cannot be relied on.