2016 - 2017

THE PARLIAMENT OF THE COMMONWEALTH OF AUSTRALIA

SENATE

SECURITY OF CRITICAL INFRASTRUCTURE BILL 2017

EXPLANATORY MEMORANDUM

(Circulated by authority of the
Attorney-General, Senator the Honourable George Brandis QC)

GLOSSARY

AAT - Administrative Appeals Tribunal

AEMO - Australian Energy Market Operator

ASIC - Australian Securities and Investments Commission

ASIO - Australian Security Intelligence Organisation

ASIO Act - *Australian Security Intelligence Organisation Act 1979*

Criminal Code - Criminal Code Act 1995

FATA - *Foreign Acquisitions and Takeovers Act 1975*

FIRB - Foreign Investment Review Board

MTOFSA - *Maritime Transport and Offshore Facilities Security Act 2003*

MW - megawatts

NEM - National Energy Market

NSI Act - *National Security Information (Criminal and Civil Proceedings) Act 2004*

Privacy Act - *Privacy Act 1988*

Regulatory Powers Act - *Regulatory Powers (Standard Provisions) Act 2014*

SCADA - Supervisory Control and Data Acquisition

TSSR - Telecommunications sector security reforms contained in the *Telecommunications and Other Legislation Amendment Act 2017*

SECURITY OF CRITICAL INFRASTRUCTURE BILL 2017

GENERAL OUTLINE

1. The Security of Critical Infrastructure 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.

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 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 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 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 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 five 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.
- **Gas:** Gas in Australia is an important energy source, an export commodity and an input for a wide range of industrial, commercial and residential uses. Gas is particularly important for gas powered electricity generators which account for approximately 20 per cent of Australia's electricity, and manufacturing which relies on gas for approximately 40 per cent of net energy requirements.
- **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 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 is implementing 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.

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-business 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.

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.

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 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.

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.

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.

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.

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 there is a risk that is prejudicial to ***security*** that cannot otherwise be mitigated.

[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.

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 an exposure draft Bill.

26. In October 2017, an exposure draft of this Bill was released for five weeks of public consultation. Throughout that period, the Centre, on behalf of the Australian Government, consulted extensively with owners and ***operators***, industry, including law firms and investment advisers, and state and territory governments. The feedback provided through the consultation process has informed the final Bill.

27. The Bill will regulate approximately 140 assets in the highest-risk sectors of ports, electricity, gas 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 FATA.

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 limited ***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. It has been assessed that the ***Register*** will impose a minimal compliance burden on industry (see full regulatory impact statement contained at the end of this explanatory memorandum). The ***Register*** reporting requirements ensure the Government can build a sufficiently comprehensive picture of ownership and control of high risk assets, with a minimum administrative burden to industry.

34. The Ministerial directions power will allow the Minister to issue a direction to an owner or ***operator*** of a ***critical infrastructure asset*** to mitigate risks that are prejudicial to ***security***. Part 3 details the requirements for the use of the Ministerial directions power.

35. The Ministerial directions power will only be able to be used in situations where:

- there is a risks that is prejudicial to ***security***
- 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.

36. Under the Bill, 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, and
- ensuring the direction is a proportionate response to the risk.

37. 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 Government must consider the use of existing mechanisms, including state and territory regimes, before issuing a direction. This includes direct consultation with the ***First Minister*** in the relevant state or territory.

38. These safeguards will ensure the power is used appropriately and not exercised beyond the remit of specific risks that are prejudicial to ***security*** and cannot be addressed through other means.

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

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

41. The 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***).

FINANCIAL IMPACT

42. Nil, however, the ongoing costs of resourcing and administering the scheme will be undertaken by the Centre which has been allocated ongoing funding to understand and manage ***national security*** risks from foreign involvement in Australia's critical infrastructure.

REGULATION MAPPING

43. The regulation impact statement appears at the end of this explanatory memorandum.

STATEMENT OF COMPATIBILITY WITH HUMAN RIGHTS

Prepared in accordance with Part 3 of the Human Rights (Parliamentary Scrutiny) Act 2011

Security of Critical Infrastructure Bill 2017

This Bill is compatible with the human rights and freedoms recognised or declared in the international instruments listed in section 3 of the *Human Rights (Parliamentary Scrutiny) Act 2011*.

Overview of the Bill

44. The Security of Critical Infrastructure Bill 2017 will 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.

45. 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.

46. The Bill will apply to the highest risk ***critical infrastructure assets*** in the following sectors determined to be most at risk from sabotage, coercion and espionage:

- **Electricity** – Electricity is fundamental to every facet of Australian society, underpinning our social and economic wellbeing in the digital age. Many other critical infrastructure sectors are reliant on electricity.
- **Water** – A clean and reliable supply of water is essential to all Australians, and many of our critical infrastructure sectors and businesses. A disruption to Australia's water supply or water treatment facilities could have major health consequences and impact the diverse range of businesses that rely on water — from the cooling towers used at power stations to food processing.
- **Ports** – 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.
- **Gas** – The adequate supply of gas is important as an energy source, an export commodity and an input for a wide range of industrial, commercial and residential uses. Gas is particularly important for gas powered electricity generators which accounts for 20 per cent of Australia's electricity.

47. The Bill will not apply to the telecommunications sector, which is the highest-risk critical infrastructure sector. The *Telecommunications and Other Legislation Amendment Act 2017* (the Telecommunications Sector ***Security*** Reforms (TSSR)), which received Royal Assent on 18 September 2017, was designed to mitigate risks in this sector.

48. Part 2, Division 2 of the Bill contains the provisions creating a ***Register*** of ***Critical Infrastructure Assets*** which 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. 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.

49. Part 3, Division 2 of the Bill provides the Minister with a power to direct a ***reporting 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. Recognising the potential impacts of such a direction, there are substantial safeguards built into the Bill. Importantly, the Minister will only issue a direction where:

- 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 *Australian Security Intelligence Organisation Act 1979*).

50. In considering whether to issue a direction, the Bill also requires the Minister to consider:

- any existing regulatory mechanism that could be used to address the risk
- the costs likely to be incurred by the ***entity***
- the consequences for competition, and
- the consequences for customers.

51. Finally, to ensure the direction is only issued where necessary and appropriate, the Minister is required to consult directly with the affected ***entity*** and the relevant state or territory Minister, and Premier or Chief Minister.

52. Part 4, Division 2 of the Bill empowers the ***Secretary*** to request certain information from ***reporting entities*** and ***operators*** of ***critical infrastructure assets***. The use of the information gathering powers is limited to where the information or document:

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

53. Part 6, Division 2 of the Bill outlines that a Minister can privately declare an asset to be a ***critical infrastructure asset*** for the purposes of the Act if the:

- asset is not otherwise a ***critical infrastructure asset***
- asset relates to electricity, gas, water or ports, as well as any industry prescribed by the ***rules***, and
- Minister is satisfied that the asset is critical infrastructure that affects ***national security*** and there would be a risk to ***national security*** if this were publicly known.

Human rights implications

54. This Bill engages the following rights:

- the right to privacy (Article 17 of the *International Covenant on Civil and Political Rights* (ICCPR)), and
- the right to a fair trial and fair hearing (Article 14 of the ICCPR).

Right to privacy – Article 17 of the ICCPR

55. Article 17 of the ICCPR provides that no one shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful attacks on his

or her honour or reputation, and that everyone has the right to the protection of the law against such interference or attacks.

56. Interferences with privacy may be permissible, provided that they are authorised by law and not arbitrary. In order for an interference with the right to privacy not to be arbitrary, the interference must be for a reason consistent with the provisions, aims and objectives of the ICCPR and be reasonable in the particular circumstances.[2] The United Nations Human Rights Committee (the HRC) has interpreted 'reasonableness' in this context to mean that 'any interference with privacy must be proportional to the end sought and be necessary in the circumstances of any given case'.

57. The following measures in the Bill engage the right to privacy under Article 17 of the ICCPR:

- the obligation of a ***reporting entity*** for a ***critical infrastructure asset*** to give information and notify of events for the ***Register*** of ***Critical Infrastructure Assets*** under Part 3, Division 2 of the Bill, and
- information gathering powers granted to the ***Secretary*** under Part 4, Division 2.

Obligation to give information and notify of events

58. The obligation of a ***reporting entity*** to give and notify of events to the ***Register*** is a permissible limitation of the right to privacy. The ***reporting entity*** is required to provide high-level information on who ultimately controls or influences an asset though ownership, including beneficial ownership, or through operation arrangements, such as outsourcing arrangements.

59. The information required by the ***Register*** will include limited personal information and information which is sensitive to the commercial interests of ***direct interest holders***, ***responsible entities*** and ***operators***. To that extent, the ***Register*** will result in the incidental collection of personal information and will limit the right to privacy in Article 17. However, this limitation is permissible as the collection of personal information would be lawful, would not be arbitrary and would be reasonable, necessary and proportionate to achieving a legitimate ***national security*** objective.

60. The ***Register*** is used by the Government to prioritise and inform risk assessments to identify and manage ***national security*** risks in ***critical infrastructure assets***. The ***interest and control information*** and ***operational information*** on the ***Register*** provides the Government with a more comprehensive understanding of how the asset and sector operates, and where there may be vulnerabilities. The information on the ***Register*** also influences the Government's ability to develop strategies to mitigate or reduce ***national security*** risk for assets which, if disrupted, would significantly impact the operations of large population hubs, economic interests and government operations.

61. The Government has taken sufficient steps to ensure that the limitations on the right to privacy are no more restrictive than necessary as the use and disclosure of information on the ***Register*** is restricted to purposes authorised under the Bill. All information obtained under the Act, including the information provided for the ***Register***, is ***protected information***. It is a criminal offence to use or disclose ***protected information*** other than as authorised by Part 4, Division 3 of the Bill. This Division enables disclosure for ***national security***, foreign investment in Australia, taxation policy, industry policy, defence purposes or to assist regulatory bodies with oversight of any ***relevant industry*** for the ***critical infrastructure asset***. Part 4, Division 3, Subdivision B of the Bill provides criminal penalties to deter the disclosure of ***protected information***.

62. The information on the ***Register*** may be shared with the relevant states and territories. This information may have broader policy implications for states and territories, particularly in relation to maintaining the ***security*** and resilience of ***critical infrastructure assets*** vital for their jurisdiction.

[2] *Toonen v Australia*, Communication No. 488/1992, U.N. Doc CCPR/C/50/D/488/1992 (1994) at 8.3.

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.

Secretary*'s general power to obtain information or documents*

63. The ***Secretary***'s information gathering power is a permissible limitation to the right to privacy. Subclause 37(1) empowers the ***Secretary*** to request certain information from ***reporting entities*** and ***operators*** of ***critical infrastructure assets***. The Bill allows for the ***Secretary*** to request information or documents that may be relevant to:

- the ***Secretary***'s duty and function to keep a ***Register*** under clause 19
- the Minister's power to issue a direction under subclause 32(2), and
- the ***Secretary***'s power to undertake an assessment of a ***critical infrastructure asset*** to determine if there is a ***national security*** risk under clause 57.

64. The information requested may include procurement plans, tender documentation, contracts, name and citizenship of board members and other documents specifying business operations. The notice may require personal information which will limit the right to privacy.

65. 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. Any personal information collected is incidental to the key objective of developing a more detailed understanding of possible ***national security*** risks.

66. The power has been drafted with reference to the Administrative Review Council's best practice principles for implementing and exercising information gathering powers in its 2008 report, *Coercive Information Gathering Powers of Government Agencies*.

67. In practice, Government agencies will also engage with the relevant ***entity*** prior to issuing a notice to discuss the nature of the information required and, if necessary, the terms of the notice. This ensures the ***Secretary***'s notice is a proportionate response which has regard to a range of matters including the right of privacy.

68. The information and documents provided to the ***Secretary*** are ***protected information*** and the use and disclosure is restricted in line with provisions at Part 4, Division 3 of the Bill. This Division enables disclosure for ***national security***, foreign investment in Australia, taxation policy, industry policy, defence purposes or to assist regulatory bodies with oversight of any ***relevant industry*** for the ***critical infrastructure asset***. Part 4, Division 3, Subdivision B of the Bill provides criminal penalties to deter the disclosure of ***protected information***.

69. The information on the ***Register*** may be shared with the relevant states and territories. This information may have broader policy implications for states and territories, particularly in relation to maintaining the ***security*** and resilience of ***critical infrastructure assets*** critical for their jurisdiction. 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.

70. Further, safeguards for the protection of personal informational specified in the Australian Privacy Principles (APPs) under the *Privacy Act 1988* will apply to ***interest and control information***, and ***operational information*** gathered under Part 2 and Part 4 of the Bill. This includes requirements regarding the ***security*** of personal information specified under Australian Privacy Principle 11 and requirements regarding use or disclosure under Australian Privacy Principle 6.

Right to a fair trial and fair hearing – Article 14 of the ICCPR

71. Article 14 of the ICCPR provides for the right to a fair trial and fair hearing and includes Article 14(3)(g). The right to a fair trial is protected in Article 14 of the ICCPR and is aimed at ensuring the proper administration of justice by upholding, among other things, the right to a fair hearing.[3] Article 14 also includes the right of protection against self-incrimination. The right to a fair trial and fair hearing may be subject to permissible limitations provided that the limitations are for a legitimate objective, and are reasonable, necessary and proportionate to that objective.

72. The Bill engages and supports the right to a fair trial through the legislated safeguards which apply prior to the Minister issuing a direction. This includes:

- Clause 32(3)(c), which requires the Minister to be given an ***adverse security assessment*** before issuing a direction. The ***adverse security assessment*** (as defined in clause 35 of the ASIO Act) will set out in writing ASIO's advice in respect of the exercise of the directions power by the Minister. 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.
- the availability of appropriate review mechanisms:
  - 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 AAT, and
  - the ***entity*** may seek judicial review of the Minister's decision to issue a direction on the basis that procedural fairness has not been observed as per subclause 5(1)(a) of the *Administrative Decisions (Judicial Review) Act 1977*.
- mandatory consultation with the ***entity*** that would be issued a direction (minimum 28 days), ensuring the power does not limit the principles of procedural fairness. Importantly, this requirement does not negate the requirement for earlier good faith negotiation with the ***entity*** to manage the ***security*** risk. In practice, it is likely that Government agencies will have ongoing engagement with the relevant ***entity*** prior to the Minister issuing a direction to mitigate the ***security*** risks on a collaborative basis.

73. Clause 40 requires an ***entity*** to abide with a notice under the ***Secretary***'s information gathering power 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.

74. However, subclause 40(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-compliance with the exercise of the information gathering power itself. This does not prevent the information or document being used if obtained through means unrelated to this Bill.

[3] UN Human Rights Committee, General Comment No 13 (1984).

Conclusion

75. The Bill is compatible with human rights because it will promote rights and, to the extent that the Bill may also limit rights, those limitations are reasonable, necessary and proportionate to the objective of managing ***national security*** risks from foreign involvement in ***critical infrastructure assets***.

PART 1—PRELIMINARY

Division 1—Preliminary

Clause 1 – Short title

76. This clause provides for the short title of the Bill, if enacted, to be the *Security of Critical Infrastructure Act 2017*.

Clause 2 – Commencement

77. This clause provides that the provisions in this Bill 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.

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

79. 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

80. The objects outline the purpose and intention of this Bill 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, gas, ports and water.

81. 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 disrupt critical infrastructure sectors in a way that would have serious impacts on Australia's national and economic security, both in terms of immediate costs incurred and long-term sector vulnerability.

82. The Bill has two key mechanisms to support the management of these ***national security*** risks: a ***Register*** of ***Critical Infrastructure Assets*** and a ministerial directions power.

83. 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.

84. The directions power (outlined in Part 3 of the Bill) will provide Government with the ability to manage an identified risk that is prejudicial to ***security*** 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 relationships between government and industry. This includes utilising existing regulatory mechanisms wherever possible.

However, the ministerial directions power will ensure that risks can be managed where existing mechanisms are not effective.

Clause 4 – Simplified outline of this Bill

85. While simplified outlines are included in the Bill 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.

86. 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 that is prejudicial to ***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 Bill is ***protected information*** and can only be disclosed in certain circumstances and for particular purposes (Part 4, Division 3).
- Enforcement measures under this Bill 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 a ***critical infrastructure asset*** 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 Bill (Part 7, Division 4).

87. 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.

88. The ministerial directions power will ensure that in cases where no other mechanisms are available, the Government has the ability to require actions to be taken to manage risks that are prejudicial to ***security***.

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

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

Division 2—Definitions

Clause 5 – Definitions

91. ***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.

92. ***Acquisition of property*** has the same meaning as section 51(xxxi) of the Australian Constitution. This definition relates specifically to clause 35 of the Bill, which provides a limitation to use of the Minister's directions power under clause 32. Clause 35 provides that the Minister's directions power at clause 32 cannot be used in a way that would result in the ***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***.

93. ***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.

94. 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 clause 32(2). This is to ensure that the Minister's directions power is reserved for instances where there is a ***security*** risk that warrants ASIO furnishing an ***adverse security assessment***.

95. Under subclause 32(5)(a), the Minister must give the greatest weight to the ***adverse security assessment*** when considering whether to issue a direction under clause 32. This is to ensure that mitigating the ***security*** risk is given precedence over other considerations such as costs of complying with the direction or consequences to competition in the ***relevant industry***.

96. ***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 subclause 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 subclause (b)(ii) of the definition of foreign company in the *Corporations Act 2001*), is required to report ***interest and control information*** (defined in clause 6) in accordance with Part 2, Division 3.

97. 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 Bill sets out the information to be provided, the ***approved form*** will be the practical tool by which to provide this information. An example of the ***approved forms*** can be found at the end of Part 2 of this document.

98. ***Civil penalty provision*** has the same meaning as subclause 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.

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

- clause 23 – Initial obligation to give ***interest and control information*** and/or ***operational information*** and notify of events
- clause 24 – Ongoing obligations to give ***interest and control information*** and/or ***operational information***
- clause 34 – Requirement to comply with a direction (under clause 32), and
- clause 37 – ***Secretary*** may obtain information or documents from ***entities***.

100. 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.

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

102. Given this Bill 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 Bill 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 Bill.

103. ***Critical electricity asset*** is defined under clause 10, which states that networks, systems or interconnectors used for transmission or distribution of electricity that ultimately service at least 100,000 customers, or electricity generation stations that are critical to ensuring the security (security in this context to have its ordinary meaning – see ***security*** definition) and reliability of an electricity network in a state or territory, as prescribed by the rules, are ***critical electricity assets*** for the purposes of this Bill. This definition forms part of the definition of ***critical infrastructure asset*** in clause 9, which itself outlines the assets to which this Bill applies.

104. ***Critical gas asset*** is defined at clause 12, which states that ***critical gas assets*** are those processing and storage facilities, distribution network or systems and transmission pipelines that are critical for ensuring the security (security in this context to have its ordinary meaning – see ***security*** definition) and availability of gas to the Eastern, Western and Northern markets, and to meet Australia export demands. This definition forms part of the definition of ***critical infrastructure asset*** in clause 9, which itself outlines the assets to which this Bill applies.

105. ***Critical infrastructure asset*** is defined at clause 9 of the Bill and states that a ***critical infrastructure asset*** is a ***critical electricity asset*** (clause 10), a ***critical port*** (clause 11), a ***critical water asset*** (in clause 5), a ***critical gas asset*** (clause 12), an asset declared under clause 51 to be a ***critical infrastructure asset***, or an asset prescribed by the ***rules*** for the purposes of this subclause.

106. 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.

107. This definition is fundamental to the operation of the Bill as it outlines the assets that fall within the scope of the Bill 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.

108. ***Critical port*** is defined at clause 11, and means specific Australian ports that have been gazetted as ***security regulated ports*** under clause 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 clause 9, which itself outlines the assets to which this Bill applies.

109. ***Critical water asset*** is defined at clause 5 and captures those water or sewerage systems or networks 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.

110. This definition forms part of the definition of ***critical infrastructure asset***, which itself outlines the assets to which this Bill applies.

111. ***Direct interest holder*** in relation to an asset is defined in clause 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 clause 5, has the obligation to report ***interest and control information*** (defined in clause 6) in accordance with Part 2, Division 3.

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

113. ***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 Bill operates to compel these various structures to adhere to obligations under the Bill, 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 Bill, including obligations to provide ***interest and control information*** and ***operational information*** to the ***Register*** in accordance with Part 2, Division 3.

114. ***First Minister*** means the Premier of a State, or the Chief Minister of the Australian Capital Territory or the Northern Territory. The Bill reinforces the Government's intention to strengthen and formalise a collaborative approach to managing ***national security*** risks by, when required, consulting ***First Ministers*** and considering formal state views in the administration of the Bill. ***First Ministers*** will be consulted to ensure any formal state views are considered prior to the Minister issuing a direction under clause 32(2). This ensures that the Minister has consideration for formal state views on the proposed risk, how it could or should be addressed, including through a possible direction, and the impacts of such a direction. ***First Ministers*** are also consulted when the Minister prescribes an asset as a ***critical infrastructure asset*** under clause 9(1)(f). This ensures that state or territory governments are aware of the ***critical infrastructure assets*** in their jurisdiction to which the legislation applies and are able to work collaboratively with the Government to manage any risks that may arise, including through leveraging existing state or territory regulatory mechanisms.

115. ***Grace period*** means the six-month period from whenever an asset becomes a ***critical infrastructure asset*** for the purposes of the legislation. Subclauses (a) and (b) ensure that whether a ***critical infrastructure asset*** is identified as such at the commencement of the Bill, 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***.

116. ***Interest and control information*** is defined in clause 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 Bill which is to better understand who owns and controls our highest-risk critical infrastructure.

117. ***International relations*** has the same meaning as section 10 of the NSI Act and means political, military and economic relations with foreign governments and international organisations. The term is defined in the Bill as it forms part of the definition of ***national security***.

118. The definition of ***national security*** is partially drawn from section 8 of the NSI Act where national security means Australia's defence, ***security***, ***international relations*** or law enforcement interests. For the purposes of this Bill, 'law enforcement interests' are not included.

119. A ***notifiable event*** is defined in clause 26 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 subclauses 23(3) or 24(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 24, 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***.

120. ***Operational information*** is defined in clause 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***.

121. 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.

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

123. ***Operators*** are defined under this Bill 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 clause 23 and clause 24, they will be subject to the information gathering and directions power under Part 4, Division 2. ***Operators*** include any ***entity*** or person that has operational control of the entire or part of a ***critical infrastructure asset*** for a period of time, or the ability to influence control of the asset or part thereof. For example, ***entities*** that run the SCADA and/or operational technology systems that control or manage the operation of the asset are considered to be ***operators*** for the purpose of this legislation. ***Entities*** that provide other services that are not clearly linked to operational activities are not ***operators*** for the purposes of this legislation. For example, ***entities*** such as cleaners, maintenance companies and retail ***operators*** do not fall within the definition of ***operators*** for the purpose of this Bill, as they are not operating the asset itself, or a part of the asset.

124. ***Port facility*** takes its meaning from clause 10 of the MTOFSA. ***Port facility*** is defined to determine whether an ***operator***, defined in clause 5, is a ***port facility operator*** (within the meaning of the MTOFSA) for a ***critical port***.

125. ***Protected information*** is defined to capture any information obtained under this Bill. 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 Bill. Importantly, this definition is used to ensure that information obtained by the Government under the Bill is afforded the appropriate protections, given the likely sensitive nature of the information. For example, the type of information that is obtained under the Bill 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. The protections under ***this Act*** afforded to ***protected information*** only extend to people who have received the information as a result of the Act. They do not otherwise limit the use or sharing of that information. For example, it does not limit a ***reporting entity*** using or disclosing contractual information relating to an ***operator*** arrangement.

126. Importantly, a direction issued by the Minister is not ***protected information***. An ***entity*** issued a direction may publicly disclose the fact and the details of the direction unless separately prevented through the specifics of the direction. However, the ***entity*** must not publicly disclose a direction if it relates to an asset which has been privately declared by the Minister to be a ***critical infrastructure asset***. This is to avoid the ***entity*** from inadvertently disclosing the fact that a ***critical infrastructure asset*** has been privately declared.

127. ***Register*** means the ***Register*** of ***Critical Infrastructure Assets*** kept by the ***Secretary*** under clause 19. The ***Register*** is being established under this Bill 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***.

128. 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.

129. ***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 Bill 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 clauses 23, 24, 34 and 37).

130. ***Relevant industry*** refers to the industries covered by the Bill, namely electricity, water, ports, gas 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.

131. ***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 clause 5 as the ***entity*** ultimately responsible for the operation of the asset. A ***direct interest holder*** is defined in clause 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.

132. ***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 clause 7) in accordance with Part 2, Division 3.

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

- for a ***critical electricity or gas 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 water asset,*** the ***water utility*** that holds the licence, approval or authorisation (however described), under a law of the Commonwealth, a State or a Territory, 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 clause 57 as the ***responsible entity*** for a ***critical infrastructure asset***, or
- an ***entity*** specified by the ***rules*** in relation to an asset prescribed to be a ***critical infrastructure asset*** for the purposes of subclause 9(1)(f).

134. 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***.

135. ***Rules*** means the ***rules*** able to be made by the Minister under clause 60. Clause 60 states that the Minister may, by legislative instrument, make ***rules*** prescribing matters that are required or permitted by the Bill to be prescribed; or matters necessary or convenient to be prescribed for carrying out or giving effect to the Bill. 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.

136. ***Secretary*** means the ***Secretary*** of the Australian Government Department that administers this Bill.

137. ***Security***, other than in clauses 10 and 12, has the same meaning as in clause 4 of the ASIO Act. For clauses 10 and 12, ***security*** has its ordinary meaning. The definition of ***security*** is a central concept in the exercise of the Minister's directions power under clause 32. The Minister may only provide a written direction to a ***reporting entity*** or ***operator*** 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***.

138. The concept of ***security*** is also referenced in the Minister's rule-making power under subclause 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***.

139. ***Security regulated port*** has the same meaning as subsection 13(1) of the MTOFSA. ***Security regulated ports*** often refer to the boundary of an area of land and water. For the purposes of this Bill, the definition of a ***critical port*** asset, which refers to ***security regulated ports***, relates to the land on the port.

140. ***Superannuation fund*** takes its meaning from clause 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.

141. The Bill defines this term to clarify that a ***superannuation fund*** is captured as a ***direct interest holder*** under subclauses 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 clause 5 and would therefore have the obligation to report ***interest and control information*** (defined in clause 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 subclause 8(1).

142. Including a definition of ***superannuation fund***s 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 Bill to assist in determining control and operation of ***critical infrastructure assets***.

143. ***This Act*** includes the ***rules***, ensuring that the ***rules*** are taken to be part of the operation of the Act once it commences.

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

145. ***Water utility*** has been defined to clarify that the obligations under this Bill only apply to those entities that manage a ***critical water asset*** **and** hold a licence, approval or authorisation (however described), under a law of the Commonwealth, a State or a Territory, to provide water services.

Clause 6 – Meaning of *interest and control information*

146. Clause 19 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 clause 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.

147. Clause 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 clause 5 to mean an individual, a body corporate, body politic, a trust, a partnership, a ***superannuation fund***, or an ***unincorporated foreign company***.

148. ***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.

149. Subclause 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***.

150. Subclause 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:

- exercise voting or veto rights
- materially impact the day-to-day operations or strategic direction of the asset
- appoint persons to the body that governs 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.

151. Subclause 6(1)(g) 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 Bill, 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)(g).

152. Subclause 6(1)(h) is a key component of the Bill 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 Bill, 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.

153. Influence and control extends to the ability to:

- exercise voting or veto rights
- materially impact the day-to-day operations or strategic direction of the asset
- appoint persons to the body that governs 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.

Example

Fifty percent of the shareholdings in Company A, which 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. Company X would need to report all information covered by subclauses 6(1)(a) to (g) for itself and, in accordance with subclause 6(1)(h), report information on Mr Smith, such as Mr Smith's shareholding in Company X, and that Mr Smith resides at 1 Smith Street, in Auckland, New Zealand and is an American citizen.

154. A rule-making provision is included in subclause 6(1)(i) 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.

155. Subclause 6(2) prescribes that the information required under subclause (1) may include personal information (within the meaning of the Privacy Act).

156. Subclause 6(3) clarifies that in instances where a State Governor, Minister or Administrator of a Territory, in their professional capacity identifies as a ***direct interest holder***, these individuals are not required to provide the ***interest and control information*** under clause 6. An example of such a situation may be where a State Minister or Governor appoints the Board of a state-owned statutory corporation that is captured under the legislation. This may equate to holding an interest in the asset that puts them in a position to directly or indirectly influence or control the asset. Accordingly, such a State Minister or Governor may identify as meeting the criteria of a ***direct interest holder*** under clause 8(1)(b).

157. Subclause 6(4) further clarifies that the exemption at subclause 6(3) for State Ministers, Governors and Administrators of a Territory from providing ***interest and control information*** does not apply to a State or Territory that identifies as a ***direct interest holder*** under subclause 8(1). In fact, the Bill requires that in meeting the requirements under subclause 6(1), the State or Territory would identify any State Ministers, Governors or Administrators of a Territory that have rights or powers (such as, to appoint the Board) as part of the information that relates to exercising influence and control in relation to an asset under subclauses 6(1)(f) to 6(1)(h).

Clause 7 – Meaning of *operational information*

158. Clause 19 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***.

159. Clause 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.

160. The ***responsible entity*** is defined in clause 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 clause 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 and address of each ***operator's*** head office (or principal place of business). Company A would also need to report where each ***operator*** is incorporated, which would include stating that Operator X is incorporated in New Zealand.

161. Subclause 7(1)(d) requires the reporting of the full name and citizenship details of the chief executive officer of the ***responsible entity***. The chief executive officer (however described) has ultimate responsibility for the operations of the ***critical infrastructure asset***. In the event that the ***Secretary*** undertakes a risk assessment of the asset (see clause 57), the chief executive officer would be a primary contact for the Government during the risk assessment process. The name and citizenship details of the chief executive officer also assists in determining the level of foreign control or operation of the asset.

162. ***Operational information*** required for the ***Register*** extends to arrangements under which an ***entity***, in this case an ***operator***, operates or controls the asset or a part of the asset (subclause 7(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.

163. ***Operational information*** will also include information relating to arrangements under which data prescribed by the ***rules*** is maintained. Given the critical importance of data, and its potential attractiveness for espionage and sabotage purposes, this clause will ensure there is visibility of any outsourced arrangements relating to data. The clause requires the ***rules*** to specify the particular types of data that the clause applies to. While subject to government decisions, this is likely to include bulk data sets (including personal information), data relating to the asset load or output and data relating to the operations of the asset.

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 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.

164. Subclause 7(1)(g) provides the Minister with a rule-making power to prescribe other ***operational information*** for this definition. This subclause 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.

165. Subclause (2) prescribes that the information required under subclause (1) may include personal information (within the meaning of the Privacy Act).

Clause 8 – Meaning of *direct interest holder*

166. The ***direct interest holder***, which is a ***reporting entity*** under clause 5, has the obligation to report ***interest and control information*** (defined in clause 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.

167. This definition covers all ***entities*** that hold a direct interest greater than 10% in a ***critical infrastructure asset*** or are in a position to directly influence or control the asset. This aligns with a key objective of the Bill which is to provide Government with a more detailed understand of who owns and controls ***critical infrastructure assets***.

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

169. Influence and control extends to the ability to:

- exercise voting or veto rights
- materially impact the day-to-day operations or strategic direction of the asset

- appoint persons to the body that governs 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.

170. ***Direct interest holders*** are obligated to report ***interest and control information*** under the Bill 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 Bill, a ***direct interest holder*** is separately defined from a ***responsible entity*** (defined in clause 5) as the latter would not always have access to interest and control information.

171. Subclause 8(2) clarifies that subclause 8(1) applies where the ***entity*** is a trust, partnership, ***superannuation fund*** or an ***unincorporated foreign company***. This subclause is included to ensure that the reporting obligations apply to any ***direct interest holder*** regardless of the nature of that interest holder.

Clause 9 – Meaning of *critical infrastructure asset*

172. 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 Bill as a ***critical electricity asset*** (clause 10), a ***critical gas asset*** (clause 12), a ***critical port*** (clause 11), a ***critical water asset*** (clause 5), an asset declared under clause 51 to be a ***critical infrastructure asset***, or an asset prescribed by the ***rules*** for the purposes of this subclause.

173. 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 Bill 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.

174. This approach is based on the shared definition of 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.

175. The electricity, gas, water and ports 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.
- **Gas** – Gas in Australia is an important energy source, an export commodity and an input for a wide range of industrial, commercial and residential uses. Gas is particularly important for gas powered electricity generators, which account for approximately 20 per cent of Australia's electricity, and manufacturing which relies on gas for approximately 40 per cent of net energy requirements.
- **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 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.

176. ***National security*** purposes – Clause 51 provides the Minister with the power to privately declare an asset to be a ***critical infrastructure asset*** under the Bill, where the asset is critical for ***national security*** purposes, but where there would be a risk to ***national 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 Bill will be directly notified. It is expected that this will only apply to a limited number of ***critical infrastructure assets***.

177. Additional assets or classes of assets – subclause 9(1)(f) 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 Bill 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 Bill, under subclause 9(3) 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).

178. This two limb test ensures that the Bill 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.

179. Subclauses (4) and (5) ensure that prior to prescribing an asset as a ***critical infrastructure asset***, the Minister must:

- consult the relevant Premier or Chief Minister, and state or territory minister who has oversight of the ***relevant industry*** in the jurisdiction in which the asset is located, and
- give consideration to any formal representation made by the state or territory, who will have at least 28 days to respond.

180. This provision ensures the Minister has regard to the formal views of the state or territory in which the asset is located.

181. Subclause 9(6) recognises that subclause 9(4) does not prevent the Minister consulting persons other than those in subclause 9(4) when considering whether to declare an asset as a ***critical infrastructure asset***.

Clause 10 – Meaning of *critical electricity asset*

182. This clause defines which electricity assets are considered to be critical and therefore captured for the purposes of this legislation. Specifically, this clause provides that an asset is a ***critical electricity asset*** if it is a network, system or interconnector used for transmission or distribution of electricity that ultimately services 100,000 customers. 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.

183. 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 Bill. The four components are:

- **Generation** – generators produce electricity and ensure the system or network is stable. Only electricity generation stations that are most critical to ensuring the security and reliability of the system or network in a state or territory will be captured by the Bill. An electricity generation station includes all the generating units in the station. The ***rules*** will specify the basis for determining critical electricity generation stations captured by the Act once in force. This is likely to be based on whether the generating station:
  - is a synchronous generator which generates electricity above a particular MW threshold in the jurisdiction in which it is located. The intended thresholds are:
    - New South Wales – 1400MW
    - Victoria – 1200MW
    - Queensland – 1300MW
    - Western Australia – 600MW
    - South Australia – 600MW
    - Tasmania – 700MW
    - Northern Territory – 300MW.

    These thresholds are consistent with the MW capacities held in reserve for each jurisdiction (i.e. the system is designed to be able to withstand the loss of this level of MW capacity), and/or

- is contracted to provide a system restart service. These generation stations are able to start without an external power supply and connect and provide energy to an electricity system or network for the transmission of electricity. They provide the ability to restart generators in the electricity network and ultimately commence restoration of load.

- **Transmission** – electricity transmission transports power from generators to distributors, and to other state transmission networks via interconnectors. The Bill will capture all nine major 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 major electricity distribution systems or networks in Australia. The Bill 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 in the NEM. 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.

Clause 11– Meaning of *critical port*

184. This clause lists the ports that the Bill will apply to. Additionally, it clarifies that the Bill will apply to the land that forms any part of the specific ports. These ports have been specifically listed 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.

185. Subclause 11(u) provides that further ports are able to be captured for the purposes of the legislation by listing in a ***rule*** made under clause 60. This ensures that the legislation is flexible and is able to adapt to changing circumstances.

Clause 12 – Meaning of *critical gas asset*

186. This clause defines which gas assets are considered to be critical and therefore captured for the purposes of this Bill. Specifically, this clause provides that a processing and storage facility, and a distribution and transmission asset which is critical for ensuring the security and availability of gas to the Eastern, Western and Northern markets, and/or those that meet Australia's export demands, is a ***critical infrastructure asset*** for the purpose of this Bill

187. The Bill will capture the following four key components involved in ensuring the security and availability of gas for the domestic and export markets:

- Processing facilities with a capacity of at least 300 terajoules per day. This will capture critical processing assets involved in removing impurities from extracted gas to meet consumer requirements.
- Storage facilities with a maximum daily quantity capacity of at least 75 terajoules per day. This will capture critical facilities which store surplus gas to meet future supply shortages and preserve stability in the domestic gas market.
- Distribution networks or systems ultimately servicing 100,000 customers. This will capture assets critical for transporting gas to households, commercial buildings and small industrial sites in most of Australia's capital cities, major regional areas and towns.
- Transmission assets that are critical for transporting gas from processing plants to major demand centres for distribution networks or large gas users such as electricity generators and industrial users, and to certain facilities and hubs for export purposes. Subclause 12(2) prescribes that the ***rules*** will specify the basis for determining critical transmission assets captured by the Act once in force. This is to be based on a set terajoule capacity per day for the particular market the transmission asset services. The intended thresholds for each market are:
  - Eastern market – 200 terajoules per day
  - Northern market – 80 terajoules per day
  - Western market – 150 terajoules per day

Division 3—Constitutional provisions and application of this Act

Clause 13 – Application of this Act

188. This clause clarifies the constitutional heads of power that the Government relies on in establishing this Bill and the regulatory framework within it. This clause cites the following heads of power and their corresponding provisions within the Australian Constitution as the powers upon which this Bill relies:

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

189. This clause, 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 Bill.

Clause 14 – Extraterritoriality

190. Clause 14 confirms that the Bill 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.

191. 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.

Clause 15 – This Act binds the Crown

192. Subclause 15(1) states that the Bill binds the Crown in each of its capacities, which means that the Bill 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 Bill must apply to the Crown in all its capacities to ensure that the regulatory framework operates effectively.

193. Subclause 15(2) confirms that under this Bill, the Crown is not liable to be prosecuted for a criminal offence. The criminal offences under this Bill relate specifically to unauthorised disclosure of ***protected information*** by a person and will apply to that person in their personal capacity (clause 45). However, the Crown is liable for the civil penalties and related remedies under this Bill.

Clause 16 – Concurrent operation of State and Territory laws

194. To the extent that this Bill and any state and territory laws can operate concurrently, this Bill 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 Bill does not seek to disrupt or override the operation of such laws.

Clause 17 – State constitutional powers

195. The Government acknowledges that ownership and operation of the highest-risk ***critical infrastructure assets*** captured under this Bill resides primarily with state and territory governments. Clause 17 confirms that powers under the Bill 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 Bill highlights the Government's acknowledgement of this important principle.

PART 2—REGISTER OF CRITICAL INFRASTRUCTURE ASSETS

Introduction

196. 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.

197. 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***. Information provided to the ***Register*** will assist the ***Secretary*** to identify which ***critical infrastructure assets*** should be the subject of a proactive risk assessment in accordance with clause 57.

Division 1—Simplified outline of this Part

Clause 18 – 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 2. Clause 18 is not intended to be comprehensive and should not be relied on in place of the substantive provisions within Part 2.

199. 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 clause 26). 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.

200. 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 that is considered to be prejudicial to ***security*** (see Part 3, Division 2).

Division 2—Register of Critical Infrastructure Assets

Clause 19– Secretary must keep Register

201. 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.

202. Clause 19 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 Bill.

203. 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 clause 58.

Clause 20 – Secretary may add information to Register

204. 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 clause 7) and ***interest and control information*** (defined in clause 6) on a ***critical infrastructure asset***.

205. 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***.

Clause 21 – Secretary may correct or update information in the Register

206. This clause 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***.

Clause 22 – Register not to be made public

207. 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 Bill provides that any information provided to the ***Register*** falls within the definition of ***protected information*** in clause 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 governs the use, recording and disclosure of ***protected information***. Clause 45

provides an offence for the disclosure of ***protected information***, including a penalty of two years imprisonment or 120 penalty units, or both.

208. In addition to the protections afforded by those provisions, this clause 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 Bill.

Division 3—Obligation to give information and notify of events

Clause 23 – Initial obligation to give information

209. The purpose of this clause is to outline the reporting obligations of the ***reporting entity*** for a ***critical infrastructure asset***. The ***reporting entity***, defined in clause 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 clause 5 and has sector specific meanings:

- for a ***critical electricity asset*** or a ***critical gas 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 water asset***—the water utility that holds the licence, approval or authorisation (however described), under a law of the Commonwealth, a State or Territory, 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 clause 51 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 subclause 9(1)(e).

210. A ***direct interest holder*** is defined in clause 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.

211. Clause 23 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 clause 5 as the six month period following an asset becoming a ***critical infrastructure asset*** to which the Bill applies (or six months from commencement for those assets captured by the Bill on commencement).

212. Subclause 23(2) sets out the information that each ***reporting entity*** must provide. Subclause 22(2)(a) requires the ***responsible entity*** to provide the ***operational information*** for that asset. ***Operational information*** is defined in clause 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.

213. Subclause 23(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 clause 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 Bill, other ***entity*** is considered to be any ultimate interest holder or beneficial owner of the first ***entity***.

214. 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.

215. 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 requirements 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.

216. 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.

217. 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 Bill will be utilised, including the power to request information (clause 37) and the power to conduct a risk assessment (clause 57).

218. Subclause 23(2) also outlines that where an eligible ***entity*** fails to comply with the obligations to provide information for the ***Register***, it will attract 50 civil penalty points. This penalty is a proportionate response based on the infringement and is designed to deter non-compliance.

219. Subclause 23(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***.

Clause 24 – Ongoing obligation to give information

220. To ensure that the ***Register*** is kept up to date, clause 24 outlines the ongoing obligations of ***reporting entities*** to give information. Specifically, subclause 24(1) outlines that the clause, 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***.

221. A ***notifiable event*** is defined in clause 26 to mean any event that renders the information already provided for the ***Register*** to be incorrect or incomplete.

222. Subclause 24(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***.

223. Subclause 24(2) also outlines that where a ***reporting entity*** fails to comply with the obligations of clause 24, it will be liable to a civil penalty up to 50 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.

Subclause 24(3) and (4) and clause 26 – Meaning of notifiable event

224. Subclause 24(3) contains a table which outlines the information required to be given for each type of ***notifiable event*** covered by clause 26.

225. Under clause 26, 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.*

226. In this event, items 1 and 2 in the table in subclause 24(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 subclause 26(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.

227. 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 subclause 26(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 Bill applies.*

228. This event covers two potential scenarios. Under subclause 26(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 subclause 26(c), a ***notifiable event*** is one where a ***reporting entity*** becomes an ***entity*** to which the Bill applies. This would include circumstances where an ***entity*** that does not fall within the definition of ***entity*** in clause 5 changes its structure, for example, by becoming an incorporated body.

229. Items 3 and 4 in the table in subclause 24(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*** for the asset 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 subclause 26(b), Company A would need to report its ***operational information*** to the ***Register***.

230. 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 subclause 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 Bill. As such, in accordance with subclause 26(b), it would need to report its ***interest and control information*** to the ***Register***.

231. Subclause 24(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.

Clause 25 – Information that is not able to be obtained

232. Clause 25 provides protections for a ***reporting entity*** that is unable to fulfil their obligations under clauses 23 and 24 after using best endeavours. Subclauses 25(a) and (b) could apply in two scenarios:

- where a ***reporting entity*** is unable to obtain and therefore provide the information required by the ***Register*** even after taking all reasonable steps. For example the ***reporting entity*** is not able to obtain and provide to the ***Register*** an ***operator'***s head office address after taking all reasonable steps to ascertain the ***operator***'s head office.
- where a ***reporting entity*** inadvertently provides inaccurate information on the ***Register*** even after using all reasonable steps to ensure the authenticity and accuracy of that information. For example the ***reporting entity*** provides an incorrect address for the head office of an ***operator*** on the ***Register*** based on information provided by the ***operator***.

233. In these scenarios the ***reporting entity*** will not attract the relevant civil penalty points under subclauses 23(2) and 24(2) as circumstances beyond the control of the ***reporting entity*** has prevented them meeting their obligations under clauses 23 and 24. The ***reporting entity*** bears the onus of proof for this provision to apply.

Clause 27 – Rules may exempt from requirement to give notice or information

234. The purpose of this clause is to enable classes of ***entities*** or specified ***entities*** to be exempted from giving notice or information. Clause 27 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 clause 24. In these circumstances, they will still be ***critical infrastructure assets*** for the purposes of the Bill (and therefore still subject to a direction issued under clause 32), 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

Clause 28 – Requirement for executors and administrators to give notice or information for individuals who die

235. The purpose of this clause is to ensure that the ***Register's*** information is kept up to date in the event that an individual who is a ***reporting entity***, dies. This clause provides that if an individual, who is required by clause 23 or 24 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 clause. This ensures the accuracy of the information on the ***Register*** in circumstances where an individual is unable to fulfil their obligations.

Clause 29 – Requirement for corporate liquidators to give notice or information

236. The purpose of this clause is to ensure that the ***Register*** is kept up to date in the event of a corporate liquidation. This clause provides that if a corporation required by clause 23 or 24 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,

237. The voluntary administrator, liquidator or receiver of the corporation must give the notice or information in accordance with that clause. 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.

Clause 30 – Agents may give notice or information

238. The purpose of this clause is to allow an agent to give notice or report information on an ***entity***'s behalf. This clause provides that where an ***entity*** is required by clauses 23 or 24 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 clause, 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.

Example of Approved forms

239. A ***water utility*** known as Critical Water Corporation meets the criteria of a critical infrastructure water asset as it operates under a licence issued by the New South Wales Government. Critical Water Corporation is 50.5% owned by the New South Wales Government and 49.5% owned by the private company Wet World Corporation, which is beneficially held by World of Water, a Cayman Islands incorporated ***entity***. Under the Bill, Critical Water Corporation is the ***responsible entity*** of the ***water utility*** asset.

240. Critical Water Corporation operates under the authority of its licence, with the following business specifics:

- it buys bulk water from ABC Water which it then treats in its two water treatment plants
- one water treatment plant is owned and operated by Critical Water Corporation
- one water treatment plant is owned, operated and transferred under a 30 year contract with a foreign owned company 'The Desalinators', and
- the bulk water it uses is under contract from ABC Water, which itself is separately the ***responsible entity*** of a critical bulk water supplier asset.

241. Critical Water Corporation has outsourced some components of its business:

- **Outsourced IT service provider -** 'IT Service Megacorp' is located onsite at Critical Water Corporation's head office under a five year contract to supply IT support and IT data management, including data storage services both offshore and onshore.
- **Cleaning/maintenance contracts**
  - A two year contract with 'Cleaners R us' for cleaning Critical Water Corporation's head office.
  - A five year contract with 'Keep Gardens Pretty' for maintenance of the grounds of head office.
- **Security services provider –** A three year contract with 'Service Enterprises', as the sole service provider of security measures at head office, including management of access control, control rooms, building management systems and CCTV, staff screening, and guard/patrolling services.

242. In this instance, the following would be required to be registered:

- A ***responsible entity*** registration by Critical Water Corporation for the ***water utility*** known as Critical Water
- A ***direct interest holder*** registration by the New South Wales Government for the critical ***water utility*** known as Critical Water Corporation
- A ***direct interest holder*** registration by Wet World Corporation for the critical ***water utility*** known as Critical Water, and
- Critical Water Corporation is not responsible for reporting ABC Water, which would separately complete its own ***responsible entity*** and ***direct interest holder*** registrations for the critical bulk water supplier asset.

Australian Government

Critical Infrastructure Centre

EXAMPLE OF APPROVED FORM

REGISTRATION FORM FOR RESPONSIBLE ENTITIES

INSTRUCTIONS FOR COMPLETING THIS FORM

To complete this form you will be required to provide the following information:

- ✓ The Critical Infrastructure Asset's name, location, industry sector and a description of the area it services.
- ✓ Your name and contact details
- ✓ Details of the responsible entity of the Asset:
  - Name of the entity, address, business number (however described) and incorporation details, address, and type of entity,
  - Information relating to the chief executive officer, including their full legal name and citizenship details
- ✓ Details of any Operators of the Asset, or part of the Asset:
  - Legal name, business address, business number (however described) and incorporation details
  - Information about the arrangements under which this entity operates the asset, or part of the asset

Remember, you must submit all information in one session; you will be unable to save the form for completion at a later time.

DATA COLLECTION NOTICE

All information obtained under the *Security of Critical Infrastructure Act* is provided for the *Register of Critical Infrastructure Assets* and is protected information. Part 4, Division 3 of the Act outlines how the protected information you provide may be shared or disclosed.

PRIVACY COLLECTION NOTICE

The Australian Government is collecting the information on this form in order to process your reporting obligations under Part 2 of the *Security of Critical Infrastructure Act*.

Our Privacy Policy outlines our personal information handling practices, including details on how you can seek to access or correct the personal information that we hold about you.

☑ I have read and accepted the Department's Privacy Policy.

1

Registration form for a Responsible Entity

SECTION 1 CRITICAL INFRASTRUCTURE ASSET DETAILS

What type of critical infrastructure asset are you registering?

◉ Critical water asset — Water utility

Provide the name of the Asset: Critical Water Corporation

Location of the Asset: 23 – 109 Oceanview Drive
Kingston NSW 2071

Legal description of location, if available: Lot 1299 DP 123456
Lot 12 DP 992357
Crown allot 9 Section 2 Douglasbanks

Describe the area that the Asset services. This information may be outlined in a licencing document or described in terms of the geographic locations in which services are provided. Documents can be attached to clarify or give further detail.

Critical Water covers the east of New South Wales, the Australian Capital Territory as well as the nearby satellite NSW areas of Queanbeyan, Jerrabomberra and Captains Flat to the east, Royalla to the south, and the district of Hall to the west.

Reason for registration today: ○ Existing holding - now captured within reporting threshold

2

SECTION 2 PERSONAL DETAILS

2.1 MY DETAILS

Legal name	Mr Johnathon Wigglesmith
In what capacity are you submitting this registration?	○ Agent or representative of the Responsible Entity
Employer's name:	GJ Goldsmith Law Firm
Employer's address:	23 Main Street Appleton NSW 2999 Australia
My job title / position:	Administration manager
Email address:	JonW@gjgold.com.au
Primary telephone number:	61 2 9876 5432
Alternative telephone:	61 2 401 234 567
Preferred contact method:	○ Primary telephone number

2.2 DETAILS OF SECONDARY CONTACT

Legal name	Ms Judy Johnsonsmith
Employer's name:	GJ Goldsmith Law Firm
Employer's address:	23 Tulla Road Essendon VIC 3999 Australia
My job title / position:	Victorian Branch Manager
Email address:	Judyjohns@gjgold.com.au
Primary telephone number:	61 3 3456 7890
Alternative telephone:	61 3 409 876 543
Preferred contact method:	○ Email

SECTION 3 RESPONSIBLE ENTITY

3.1 DETAILS OF THE RESPONSIBLE ENTITY

Legal name of responsible entity:	Critical Water Corporation
Type of entity:	Body politic
Country of incorporation or creation:	Australia
Business registration number (or however described):	ABN1234567890123
Address of head office or principal place of business:	628 Moorepark Avenue Douglasbanks NSW 2021

Original commencement date as responsible entity of this Asset: 23 / 02 / 1956

3.2 OPERATIONAL INFORMATION

3.2.2 Chief Executive Officer

Legal name: Mr Nathan Jonesparkway

Citizenship: Australia

☑ Dual citizen United Kingdom

Are there any other entities that are defined as operators of any parts of this critical asset?

Under the Security of Critical Infrastructure Act an operator is an entity that is authorised (however described) to operate the asset or part of the asset.

○ No - proceed to Section 5 Additional information and Declaration

◉ Yes - proceed to Section 4 Asset Operators

SECTION 4 ASSET OPERATORS

Operator 1

4.1 Operator details

Legal name of entity:	The Desalinators
Type of entity:	Partnership
Country of incorporation or creation:	New Zealand
Business registration number (or however described):	NZI123456999
Address of head office or principal place of business:	2378 Australia Way Banksia Rose Auckland New Zealand
Original date this operator commenced operating the asset:	15 / 05 / 2016

4.2 Operator arrangements

Provide details of the arrangements (such as outsourcing or offshoring) under which this entity operates the Asset or part of the Asset.

The Desalinators operates Water Sewage Treatment Plant number 2, under a 30 year contract with Critical Water Corporation. Bulk water is treated in this plant under contract with Critical Water Corp, see attached contract.

Attachment 1	**Contract with The Desalinators**

Operator 2

4.1 Operator details

Legal name of entity:	IT Service Megacorp
Type of entity:	Body corporate
Country of incorporation or creation:	Australia
Business registration number (or however described):	ABN3210987654321
Address of head office or principal place of business:	26 Moore Street Belconnen ACT 2609
Original date this operator commenced operating the asset:	02 / 03 / 2017

4.2 Operator arrangements

Provide details of the arrangements (such as outsourcing or offshoring) under which this entity operates the Asset or part of the Asset.

IT Service Megacorp is located onsite at Critical Water Corporation's head office under a 5 year contract. It supplies IT support and IT data management. All of Critical Water Corporation's data is stored by IT Service Megacorp, in 2 facilities. Customer data is stored in its main data centre located in Parramatta. All other data is stored in an offshore facility located in Mumbai, India.

Attachment 2	**Contract with IT Service Megacorp**

Operator 3

4.1 Operator details

Legal name of entity:	Service Enterprises
Type of entity:	Body corporate
Country of incorporation or creation:	Singapore
Business registration number (or however described):	998766SGR5523
Address of head office or principal place of business:	Citizen Building 1 Orchard Road Singapore
Original date this operator commenced operating the asset:	07/ 08 / 2012

4.2 Operator arrangements

Provide details of the arrangements (such as outsourcing or offshoring) under which this entity operates the Asset or part of the Asset.

Service Enterprises is the sole service provider of all security at the head office of Critical Water Corporation. This company provides the following security services:

- Management of access controls
- Control room management
- Building management systems and CCTV
- Staff screening, and
- Guard reception and patrol services, 24/7.

Attachment 3	**Security contract**

SECTION 5 ADDITIONAL INFORMATION AND DECLARATION

Provide any further information that you believe is relevant and may assist the Centre

Nil.

Is this Responsible Entity also the Direct Interest Holder for this Asset?

- (•) No
- ( ) Yes - you will be required to complete the registration form for a direct interest holder
  - [ ] Complete the Direct Interest Holder registration form now?

DECLARATION

Declaration by responsible entity, their agent or representative:

I declare that the information supplied by me is true, complete and correct to the best of my knowledge and beliefs, and are made in good faith.

I am aware that any false or misleading information supplied by me may result in a civil penalty that is enforceable under Part 4 of the *Regulatory Powers Act*.

Name: Mr Johnathon Wigglesmith 16 / 10 / 2017

List of attached documents:

Attachment 1	**Contract with The Desalinators**
Attachment 2	**Contract with IT Service Megacorp**
Attachment 3	**Security contract**

Australian Government

Critical Infrastructure Centre

EXAMPLE OF APPROVED FORM

REGISTRATION FORM FOR DIRECT INTEREST HOLDERS

INSTRUCTIONS FOR COMPLETING THIS FORM

To complete this form you will be required to provide the following information:

- ✓ Critical Infrastructure Asset name and industry sector
- ✓ Your name and contact details
- ✓ Direct interest holder – first entity:
  - Name, business number, address, type of interest (legal, equitable, lease or licence interest), percentage of interest held,
  - Description of any influence or control this entity is in a position to directly or indirectly exercise in relation to the asset, including:
    - information about the control the first entity has over decisions relating to the running of the asset (such as voting and veto rights and ability to appoint board members)
    - information relating to any person the first entity has appointed to the body that governs the asset, including:
      - full names and citizenship details of board members, and
      - direct access by these individuals to networks or systems that are necessary for the operation or control of the asset
- ✓ Direct interest holder – other entities which have the ability to exercise any influence or control over the first entity:
  - Legal name, business number (however described) and residential/business address
  - Description of the control or influence it has over the first entity

If the direct interest holder/first entity is also the responsible entity for this Asset you can also record the operational information at the same time

Remember, you must submit all information in one session, you will be unable to save the form for completion at a later time.

DATA COLLECTION NOTICE

All information obtained under the *Security of Critical Infrastructure Act* is provided for the *Register of Critical Infrastructure Assets* and is protected information. Part 4, Division 3 of the Act outlines how the protected information you provide may be shared or disclosed.

PRIVACY COLLECTION NOTICE

The Australian Government is collecting the information on this form in order to process your reporting obligations under Part 2 of the *Security of Critical Infrastructure Act*.

Our Privacy Policy outlines our personal information handling practices, including details on how you can seek to access or correct the personal information that we hold about you.

☑ I have read and accepted the Department's Privacy Policy.

SECTION 1 CRITICAL INFRASTRUCTURE ASSET DETAILS

What type of critical infrastructure asset are you registering?

(•) Critical water asset — Water utility

Provide the name of the Asset: Critical Water

Reason for registration today: ( ) Existing holding - now captured within reporting threshold

SECTION 2 PERSONAL DETAILS

Provide details of the person completing this form.

2.1 MY DETAILS

Legal name	Ms Juliette Zu
In what capacity are you submitting this registration?	(•) Agent or representative of direct interest holder
Employer's name:	The Financial Asset Management Company
Employer's address:	12 Livingston Street, Sydney NSW 2001
My job title / position:	Chief Financial Officer
Email address:	cfo@financialasset.com.au
Primary telephone number:	+61 2 9677 1234
Alternative telephone:	+61 2 0499 654 987
Preferred contact method:	( ) Primary telephone number

2.2 DETAILS OF SECONDARY CONTACT

Legal name	Mr Douglas Ray
Employer's name:	The Financial Asset Management Company
Employer's address:	12 Livingston Street, Sydney NSW 2001
Job title / position:	HR Manager
Email address:	hr@financialasset.com.au
Primary telephone number:	+61 2 9677 2000
Alternative telephone:	+61 2 0409 999 111
Preferred contact method:	( ) Primary telephone number

SECTION 3 FIRST ENTITY – DIRECT INTEREST HOLDER OF THE CRITICAL INFRASTRUCTURE ASSET

An entity is a direct interest holder in relation to an asset if the entity:

(a) holds a legal or equitable interest of at least 10% in the asset (including if the interest is held jointly with one or more other entities); or

(b) holds 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.

An entity can be an individual, a trust, body corporate, body politic, partnership, superannuation fund or unincorporated foreign company.

3.1 DETAILS OF FIRST ENTITY

Legal name of first entity:	New South Wales State Government
Type of entity:	Body politic
Type of interest in Asset:	Legal interest
Interest in asset	50.5%
Country of incorporation or creation:	Australia
Business registration number (or however described):	9977881122334
Address of head office or principal place of business:	12C/9 Double Street Parramatta NSW 2007 Australia
Original date of acquisition of the critical infrastructure asset:	23 / 07 / 1956

3.2 INFLUENCE AND CONTROL OVER THE ASSET

3.2.1 First Entity - Influence and control

Provide information about the influence and control this entity is in a position to directly or indirectly exercise in relation to the Asset.

The New South Wales Government delegates the strategic oversight of Critical Water Corporation to its board. The State, through the responsible Minister, appoints the Chairman of the Board, as well as other Board Members.

The New South Wales Government retains decision making on the sale of whole or part of the asset.

3.2.2 Structure of the Board or Governing Body

Provide information relating to any persons this entity has appointed to the body that governs the asset.

BOARD CHAIRMAN

Legal name	Commodore Wuxzjilzk ☑ Tick if you legally have a single word name
Citizenship	Australia

BOARD MEMBER

Legal name	Hon John Dibbles
Citizenship	Australia

BOARD MEMBER

Legal name	Hon Ny Uhuru
Citizenship	Australia

3.2.3 Board's influence and control over the Asset

Provide information about the ability of any person reported in 3.2.2 to directly or indirectly access networks or systems that are necessary for the operation or control of the asset.

The Board cannot access any of the assets operational or control systems.

The Board of Critical Water can direct certain aspects of the Asset's operations including:

- the construction, operation and maintenance of any associated infrastructure necessary for the operation of Critical Water;
- the approval of funding of any single capital cost for construction, operation and maintenance of any associated infrastructure necessary for the operation of Critical Water that exceed $10,000,000 in one fiscal year.

SECTION 4 OTHER ENTITY WITH INFLUENCE OR CONTROL OVER THE FIRST ENTITY

Is there an entity which has direct or indirect control or influence over this direct interest holder?

☑ No - proceed to Section 5 Additional information and Declaration

OTHER ENTITY 1

4.1 Details of other entities that can influence or control the first entity reported in Section 3

Not applicable.

SECTION 5 ADDITIONAL INFORMATION AND DECLARATION

Provide any further information that you believe is relevant and may assist the Centre:

Nil

Is the first entity named in Section 3 also the Responsible Entity for this Asset?

◉ No

DECLARATION

Declaration by direct interest holder, their agent or representative:

I declare that the information supplied by me is true, complete and correct to the best of my knowledge and beliefs, and are made in good faith.

I am aware that any false or misleading information supplied by me may result in a civil penalty that is enforceable under Part 4 of the *Regulatory Powers Act*.

Name: Juliette Zu 14 / 11 / 2017

List of attached documents:

NIL

Australian Government

Critical Infrastructure Centre

EXAMPLE OF APPROVED FORM

REGISTRATION FORM FOR DIRECT INTEREST HOLDERS

INSTRUCTIONS FOR COMPLETING THIS FORM

To complete this form you will be required to provide the following information:

- ✓ Critical Infrastructure Asset name and industry sector
- ✓ Your name and contact details
- ✓ Direct interest holder – first entity:
  - Name, business number, address, type of interest (legal, equitable, lease or licence interest), percentage of interest held,
  - Description of any influence or control this entity is in a position to directly or indirectly exercise in relation to the asset, including:
    - information about the control the first entity has over decisions relating to the running of the asset (such as voting and veto rights and ability to appoint board members)
    - information relating to any person the first entity has appointed to the body that governs the asset, including:
      - full names and citizenship details of board members, and
      - direct access by these individuals to networks or systems that are necessary for the operation or control of the asset
- ✓ Direct interest holder – other entities which have the ability to exercise any influence or control over the first entity:
  - Legal name, business number (however described) and residential/business address
  - Description of the control or influence it has over the first entity

If the direct interest holder/first entity is also the responsible entity for this Asset you can also record the operational information at the same time

Remember, you must submit all information in one session, you will be unable to save the form for completion at a later time.

DATA COLLECTION NOTICE

All information obtained under the *Security of Critical Infrastructure Act* is provided for the *Register of Critical Infrastructure Assets* and is protected information. Part 4, Division 3 of the Act outlines how the protected information you provide may be shared or disclosed.

PRIVACY COLLECTION NOTICE

The Australian Government is collecting the information on this form in order to process your reporting obligations under Part 2 of the *Security of Critical Infrastructure Act*.

Our Privacy Policy outlines our personal information handling practices, including details on how you can seek to access or correct the personal information that we hold about you.

☑ I have read and accepted the Department's Privacy Policy.

1

SECTION 1 CRITICAL INFRASTRUCTURE ASSET DETAILS

What type of critical infrastructure asset are you registering?

(•) Critical water asset — Water utility

Provide the name of the Asset: Critical Water

Reason for registration today: ( ) Existing holding - now captured within reporting threshold

SECTION 2 PERSONAL DETAILS

Details of the person completing this form.

2.1 MY DETAILS

Legal name: Mr Anthony John Doubleday Snr

In what capacity are you submitting this registration? (•) Agent or representative of direct interest holder

Employer's name:	XYZ Property Lawyers
Employer's address:	278 Pitt Street, Sydney NSW 2000
My job title / position:	Senior partner
Email address:	tonydd@xyzpropertylaw.com.au
Primary telephone number:	+61 2 9899 1234
Alternative telephone:	+61 2 0400 123 456
Preferred contact method:	( ) Primary telephone number

2.2 DETAILS OF SECONDARY CONTACT

Legal name: Ms Julie Amway

Employer's name:	XYZ Property Lawyers
Employer's address:	278 Pitt Street, Sydney NSW 2000
Job title / position:	Finance manager
Email address:	julieam@xyzpropertylaw.com.au
Primary telephone number:	+61 2 9899 2000
Alternative telephone:	+61 2 0400 654 321
Preferred contact method:	( ) Email

SECTION 3 FIRST ENTITY – DIRECT INTEREST HOLDER OF THE CRITICAL INFRASTRUCTURE ASSET

An entity is a direct interest holder in relation to an asset if the entity:

(a) holds a legal or equitable interest of at least 10% in the asset (including if the interest is held jointly with one or more other entities); or

(b) holds 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.

An entity can be an individual, a trust, body corporate, body politic, partnership, superannuation fund or unincorporated foreign company.

3.1 DETAILS OF FIRST ENTITY

Legal name of first entity:	Wet World Corporation
Type of entity:	Body corporation
Type of interest in Asset:	Legal interest
Interest in asset	49.5%
Country of incorporation or creation:	Australia
Business registration number (or however described):	123456789123456789
Address of head office or principal place of business:	234 Government Way Newcity NSA 9007 Australia
Original date of acquisition of the critical infrastructure asset:	23 / 07 / 1991

3.2 INFLUENCE AND CONTROL OVER THE ASSET

3.2.1 First Entity - Influence and control

Provide information about the influence and control this entity is in a position to directly or indirectly exercise in relation to the Asset.

Wet World Corporation has the power to appoint one Board member to the water utility known as Critical Water. The majority Direct Interest Holder, the New State of Australia, through the responsible Minister, appoints the Chairman of the Board, as well as two other Board Members.

Wet World Corporation cannot influence the asset in any other way, except by way of its one Board Member.

3.2.2 Structure of the Board or Governing Body

Provide information relating to any persons this entity has appointed to the body that governs the asset.

BOARD MEMBER

Legal name	Dr Leo Nimoy
Citizenship	Australia

BOARD MEMBER

Legal name	Mr Robert Jackson
Citizenship	New Zealand

3.2.3 Board's influence and control over the Asset

Provide information about the ability of any person reported in 3.2.2 to directly or indirectly access networks or systems
that are necessary for the operation or control of the asset.

Dr Nimoy and Mr Jackson cannot access any of the assets operational or control systems.

The Board of Critical Water can direct certain aspects of the Asset's operations including:

- the construction, operation and maintenance of any associated infrastructure necessary for the operation of Critical Water;
- the approval of funding of any single capital cost for construction, operation and maintenance of any associated infrastructure necessary for the operation of Critical Water that exceed $10,000,000 in one fiscal year.

Is there an entity which has direct or indirect control or influence over this direct interest holder?

- ○ No - proceed to Section 5 Additional information and Declaration
- ◉ Yes - proceed to Section 4 Other entity with influence and control

SECTION 4 OTHER ENTITY WITH INFLUENCE OR CONTROL OVER THE FIRST ENTITY

OTHER ENTITY 1

4.1 Details of other entities that can influence or control the first entity reported in Section 3

Legal name of entity:	The World of Water
Type of entity:	Body corporate
Type of interest in Asset:	Beneficial interest
Interest in first entity:	100%
Country of incorporation or creation:	Cayman Islands
Business registration number (however described):	2233445569
Address of head office or principal place of business:	Banksia Building 23698 Ocean Boulevard Cayman Islands

Provide a general description of the type of interest or relationship with the first entity recorded in Section 3:

The World of Water has 100% ownership of Wet World Corporation, which has a 49.5% ownership share in the water utility asset known as Critical Water.

4.2 Influence and control

Provide information about the influence and control this entity is in a position to directly or indirectly exercise in relation to the asset:

The World of Water has:

- veto rights on all financial decisions over Wet World Corp, including contractual arrangements and major expenditures over a $10,000,000 threshold, and
- has voting rights for all Board appointments to Wet World Corporation.

OTHER ENTITY 2

Is there another entity which has direct or indirect control or influence over the direct interest holder named in Section 3?

☑ No - proceed to Section 5 Additional information and Declaration

SECTION 5 ADDITIONAL INFORMATION AND DECLARATION

Provide any further information that you believe is relevant and may assist the Centre:

Nil

Is the first entity named in Section 3 also the Responsible Entity for this Asset?

(•) No

DECLARATION

Declaration by direct interest holder, their agent or representative:

I declare that the information supplied by me is true, complete and correct to the best of my knowledge and beliefs, and are made in good faith.

I am aware that any false or misleading information supplied by me may result in a civil penalty that is enforceable under Part 4 of the *Regulatory Powers Act*.

Name: Anthony John Doubleday Snr 14 / 11 / 2017

List of attached documents:

DOCUMENT 1	WET WATER CORPORATION CONSTITUTIONAL AGREEMENT

PART 3—DIRECTIONS BY THE MINISTER

243. 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.

244. 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 risk.

245. 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 risks that are prejudicial to ***security***.

Division 1—Simplified outline of this Part

Clause 31 – Simplified outline of this Part

246. The simplified outline is to assist readers to understand the substantive provisions, by providing an overview of the provisions within Part 3. Clause 31 is not intended to be comprehensive and should not be relied on in place of the substantive provisions within Part 3.

247. 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 risk that is prejudicial to ***security***. 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.

248. Noting that this Bill 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 ***security*** risks. However, if ***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.

249. 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 regulators governing what business costs may be passed on to consumers.

Division 2—Directions by the Minister

Clause 32 – Direction if risk prejudicial to security

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

251. Subclause 32(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

252. 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 connected to a ***critical infrastructure asset*** that falls within the definition at clause 9.

253. 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.

254. 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.

255. '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 or 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***.

256. The intention of the Bill is to manage risks posed by malicious insiders, including foreign state actors, where, through a 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

257. 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.

258. 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

259. 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***.

260. ***Security*** is given the same meaning as in 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, politically motivated violence, promotion of communal violence, attacks on Australia's defence system, or acts of foreign interference, as well as the protection of Australia's border integrity. The term 'prejudicial to ***security***' is to be given its ordinary meaning, but interpreted in a manner that is consistent with the term 'activities prejudicial to ***security***' contained in the ASIO Act. As a matter of guidance only, activities prejudicial to ***security*** may cover activities relevant to '***security***', as defined under the ASIO Act, that could 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.

261. 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***. 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 risk which is prejudicial to ***security*** exists.

262. 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

263. Subclause 32(2) provides the specific power for the Minister to issue a written direction requiring a ***reporting entity*** (defined in clause 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.

264. 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.

265. Given the range of ***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. However, to balance the breadth of the power, there are significant safeguards built into the use of the power at subsections subclause 32(3), 32(4) and 33. These safeguards ensure that any direction issued is only after significant consultation, consideration and is proportionate to the risk being managed.

266. In addition to the factors upon which the Minister must be satisfied (subclause 32(1)), subclause 32(3) specifies further conditions that must be considered before the Minister can issue a direction. First, under subclause 32(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 subclause 32(1). This is a proportionality test, and ensures the direction is limited to what is reasonably necessary to eliminate or reduce the 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.

267. Subclause 32(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 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.

268. 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.

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

270. Subclause 32(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.

271. 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.

272. Further to the meaning of an ***adverse security assessment*** in 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.

273. 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.

274. Subclause 32(3)(d) provides that the Minister must be satisfied that consideration has been given 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 must 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.

275. This provision reinforces the Government's intention to continue to engage collaboratively with owners and ***operators*** of ***critical infrastructure assets*** 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.

276. While subclause 32(3) sets out the matters that the Minister must be satisfied of before issuing a direction, subclause 32(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.

277. Subclause 32(4)(a) provides that the Minister must have regard to the ***adverse security assessment*** provided under subclause 32(3)(c). While recognising the importance of the other factors in subclause 32(4), paragraph 32(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.

278. Subclauses 32(4)(b) to (d) 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 subclauses 32(4)(b) to (d) 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.

279. Subclause 32(4)(e) provides that the Minister must have regard to representations made by the ***entity*** or a consulted Minister under clause 33. This ensures that prior to issuing a direction, as part of procedural fairness, the Minister gives due regard to the representations made by the relevant ***entity*** and the relevant Minister of a state or territory before issuing a direction. The inclusion of state Ministers in this provision ensures that the Commonwealth Minister allows the relevant state to provide written representations that must be taken into account in considering the use of the directions power at subclause 32(2).

280. Subclause 32(5)(b) clarifies that the matters listed in subclause 32(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, subclause 32(5)(a) still requires the greatest weight to be given to the ***adverse security assessment***.

Clause 33 – Consultation before giving direction

281. 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 that is limited to instances where a risk that is prejudicial to ***security*** can be identified.

282. Subclause 33(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 Bill strengthens and formalises a collaborative approach to managing ***national security*** risks, subclauses 33(1)(a)(i) and (ii) provide that the Minister consult with the relevant state or territory minister, and Premier or Chief Minister before issuing a direction. This provision ensures the relevant state or territory minister, and Premier or Chief Minister have been directly consulted and have provided 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.

283. Subclause 33(1)(b) imposes mandatory consultation with the relevant ***entity*** to assist in mitigating the identified ***security*** risk. Under subclause 33(1)(b), 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 as set out in subclause 32(3)(b). This notice also needs to be provided to the relevant state ministers.

284. Subclause 33(2)(a) outlines the minimum 28-day timeframe in which the Minister can require the relevant ***entity*** and Ministers to provide written representations. The provision does not prevent the Minister from providing the relevant ***entity*** and Ministers longer than 28 days in which to make representations. However, subclause 33(2)(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 risks in a timely manner.

285. While this provision provides the ***entity*** and Ministers 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*** and Ministers 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*** and Ministers could also make representations on other mechanisms that could be used to mitigate the risk. Given the Commonwealth 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.

286. Subclause 33(3) clarifies that clause 33 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 with responsibility for Foreign Affairs and Trade where there are international sensitivities, the Prime Minister and the minister responsible for the ***relevant industry***.

Clause 34 – Requirement to comply with direction

287. An ***entity*** is required to comply with a direction issued to them by the Minister under this Bill. 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 subclause 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 Bill.

288. 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 ***security*** risks that would be left unmitigated if a direction was not complied with.

Clause 35 – Exception—acquisition of property

289. Clause 35 provides that any direction issued by the Minister under subclause 32(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.

PART 4—GATHERING AND USING INFORMATION

290. 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 Bill provides the ***Secretary*** with an information-gathering power which compels the provision of information or documents.

291. 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.

292. 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

Clause 36 – Simplified outline of this Part

293. The simplified outline is to assist readers to understand the substantive provisions, by providing an overview of the provisions within Part 4. Clause 36 is not intended to be comprehensive and should not be relied on in place of the substantive provisions.

294. 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 Bill.

295. 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.

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

297. To ensure an ***entity*** complies with a notice issued by the ***Secretary***, the Bill 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

Clause 37 & 40 – Secretary may obtain information or documents from entities, and self-incrimination

298. Subclause 37(1) empowers the ***Secretary*** to request certain information from ***reporting entities*** (***direct interest holders***, ***responsible entities***) and ***operators*** of ***critical infrastructure assets***. The clause limits the use of the information gathering powers to the following, in line with the purpose and objects of the Bill:

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

299. Subclause 37(1)(a) refers to information or documents that may be relevant to:

- the ***Secretary***'s duty and function to keep a ***Register*** under clause 19
- the Minister's power to issue a direction under subclause 32(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 clause 57.

300. Under clause 19, the ***Secretary*** is required to keep a ***Register*** of ***Critical Infrastructure Assets*** containing certain information. Further, Part 2 of this Bill requires ***reporting entities*** to provide ***interest and control information*** and ***operational information*** to assist the Government to understand and assess ***national security*** risks.

301. 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.

302. Additionally, in line with the objects of the Bill and clause 57 (undertaking an assessment of a ***critical infrastructure asset***), the information gathering power in this subclause 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***.

303. Similarly, subclause 37(1)(b) would apply if the ***Secretary*** required further information relevant to determining whether to exercise a power under this Bill. For example, this power could be used to obtain further information about the way an ***operator*** of a ***critical infrastructure asset*** 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 clause 57 to conduct a ***national security*** risk assessment of a ***critical infrastructure asset***.

304. 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 Bill, as well as the functions, duties, powers and purposes prescribed in the Bill.

305. In circumstances where the clause applies (as set out in subclause 37(1)), subclause 37(2) provides that the ***Secretary*** may require, by notice in writing, the ***entity*** to provide information or a document that meets the requirements in subclause 37(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).

306. Recognising the potential impost on business of complying with such a notice, subclause 37(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.

307. Subclause 37(4) provides that an ***entity*** issued with a notice under subclause (2) to produce information or documents must comply with that notice. Subclause 37(4) is a ***civil penalty provision*** that is enforceable under Part 4 (civil penalty provisions); Part 6 (enforceable undertakings); and Part 7 (injunctions) of the ***Regulatory Powers Act***. Non-compliance with the Minister's notice will attract a pecuniary penalty of 150 civil penalty units for each day of non-compliance as prescribed in subsection 93(2) of the ***Regulatory Powers Act***.

308. 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 Bill represent the highest-risk water, electricity, gas and ports assets.

309. Furthermore, under clause 40, 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.

310. However, subclause 40(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-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 Bill.

311. Subclause 37(5) sets out the requirements for a notice issued by the ***Secretary*** under subclause 37(2). Subclause 37(2) and 37(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, subclause 37(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 clause 37, including the criminal consequences for providing misleading or false information.

312. Given the potential sensitivity of information required to be provided to the ***Secretary*** under clause 37, the Bill sets out provisions for how and when information obtained under the Bill can be used, retained and further disclosed to other persons (see Part 4, Division 3).

313. Subclause 37(6) provides that if an ***entity*** provides copies of documents in compliance with a requirement under subclause 37(2)(c), the ***entity*** is entitled to be paid reasonable compensation by the Government.

Clause 38 – Copies of documents

314. Clause 38 recognises that the documents or information that may be sought might also be required by the business. As such, this clause provides flexibility as to how the ***Secretary*** may consider documents that have been requested. Subclause 38(1) enables the ***Secretary*** to inspect a document produced under clause 37 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.

315. Subclause 38(2) also enables the ***Secretary*** to retain any copies of documents that are produced under subclause 37(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.

Clause 39 – Retention of documents

316. Under clause 39, the ***Secretary*** may retain possession of documents obtained under clause 37 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.

317. In circumstances where an original document is retained, subclause 39(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 subclause 39(4), until such time as the certified copy is produced, the ***Secretary*** must provide reasonable access to inspect and make copies of the document.

318. Finally, subclause 39(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

319. Division 3 sets out how ***protected information*** obtained under this Bill may be shared and disclosed. All information obtained under the Bill, such as information provided for the ***Register*** or obtained through the ***Secretary***'s power under clause 37, 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

Clause 41 – Authorised use and disclosure—performing functions, etc

320. Clause 41 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 Bill. 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 Bill. Some examples include:

- Information obtained under the ***Secretary***'s information gathering power 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 Ministerial 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 with them on the possible issuing of a Ministerial direction.

- Information provided to a state or territory Minister may be required to be shared with other state or territory ministers in order to develop appropriate risk mitigations.
- Information provided to a state or territory Minister may be shared with other state or territory Ministers in order to develop a whole of jurisdiction position (for example, through Cabinet processes) on a proposed Ministerial direction.

Clause 42 – Authorised use and disclosure—other person's functions, etc

321. While the information obtained under this Bill 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***. Clause 42 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.

322. Subclauses 42(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 investment in Australia by providing relevant information such as sources of domestic and 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.

323. Subclause 42(1) combined with subclause 42(2)(b), (c) and (d) allows the sharing of information obtained under this Bill with states and territories. This is in keeping with the Bill's objective to promote a collaborative and cooperative approach to managing ***national security*** risks.

324. The Bill 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.

325. The information obtained under the Bill 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.

326. 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.

Clause 43 – Authorised disclosure relating to law enforcement

327. Clause 43 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.

328. 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 Investments 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 Bill to manage ***national security*** risks relating to critical infrastructure.

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

Clause 44 – Secondary use and disclosure of protected information

330. Persons who have been provided information under clause 42 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. Information provided to a state or territory minister may also be required to be shared with other state or territory ministers for developing a whole of jurisdiction position (for example, through Cabinet processes).

Subdivision B—Offence for unauthorised use or disclosure

Clause 45 – Offence for unauthorised use or disclosure of protected information

331. This clause 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.

332. 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.

333. Subclause 45(2) notes that clause 15.1 of the Criminal Code will apply to an offence against subclause 45(1). Clause 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 subclause 45(1).

Clause 46 – Exceptions to offence for unauthorised use or disclosure

334. Clause 46 provides a range of appropriate defences to an offence of unauthorised disclosure of ***protected information***. These defences are where the disclosure is:

- required or authorised by or under a Commonwealth law, other than Subdivision A or subclause 51(3) or 52(4), or a law of a State or Territory prescribed by the ***rules***
  - The purpose of subclause 46(2) is to ensure that notification of sensitive national security assets declared under clauses 51(3) and 52(4) is not further disclosed under reporting obligations contained in the *Corporations Act 2011* or a law of the Commonwealth prescribed by the ***rules***
- disclosed in good faith in attempting to comply with provisions relating to authorised disclosure under Subdivision A or subclauses 51(3) and 51(4), or
- to a person to whom the ***protected information*** relates, or with their express or implied consent.

335. 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.

336. 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.

Clause 47 – No requirement to provide information

337. Clause 47 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 Bill. This provision protects the sensitivity of the information from being revealed in court proceedings that are not in relation to the operations of this Bill.

PART 5—ENFORCEMENT

338. This Part outlines the enforcement measures available to the Government if the ***civil penalty provisions*** within this Bill are contravened.

339. 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 Bill. 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 Bill.

Division 1—Simplified outline of this Part

Clause 48 – Simplified outline of this Part

340. The simplified outline is to assist readers to understand the substantive provisions, by providing an overview of the provisions in Part 5. Clause 48 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 Bill, 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

Clause 49 – Civil penalties, enforceable undertakings and injunctions

341. 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 Bill. Under subclause 49(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.

342. 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 Bill. For example, the Minister is likely to issue a performance injunction if an ***entity*** is unwilling to abide by a direction from the Minister to do or not do a thing under subclause 32(2) of the Bill to ensure that the risk identified as prejudicial to ***security*** is mitigated. 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***.

343. 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 Bill:

- subclause 23(2) – which requires the ***reporting entity*** to initially register ***interest and control information*** and/or ***operational information*** through the ***approved form***.
- subclause 24(2) – which requires the ***reporting entity*** to update ***interest and control information*** and ***operational information*** through the ***civil penalty provision*** if the information initially provided to the ***Secretary*** is out of date or incorrect because of a ***notifiable event***.

344. 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 Bill:

- subclause 32(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.
- subclause 37(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.

345. Subclause 49(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 Bill 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 Bill 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 Bill.

346. Subclause 58(1) provides that the ***Secretary*** may, by written instrument, delegate his or her powers, functions or duties under this Bill 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 Bill.

347. Subclause 49(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 Bill.

348. 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 Bill to a particular court.

349. Noting that some court proceedings that may be initiated under this Bill 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.

350. Subclause 49(5) provides that under this Bill, the operation of Parts 4, 6 and 7 of the ***Regulatory Powers Act***, extend outside Australia. Given the operation of this Bill triggers the ***Regulatory Powers Act***, it is important to ensure consistency of jurisdiction across all the provisions under this Bill. This Bill has extended application outside Australia, as provided at clause 13, therefore the effect of 49(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

351. This Bill applies to ***critical infrastructure assets*** captured by the definition in clause 9. Subclause 9(1)(d) explicitly provides that an asset can be privately declared under clause 51 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

Clause 50 – Simplified outline of this Part

352. The simplified outline is to assist readers to understand the substantive provisions by providing an overview of the provisions within Part 6. Clause 50 is not intended to be comprehensive and should not be relied on in place of the substantive provisions within Part 6.

353. The main feature of Part 6 is the power for the Minister to privately declare a particular asset to be a ***critical infrastructure asset*** for the purposes of this Bill. Importantly, if an asset is declared, it then falls within the operation of the Bill. 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

Clause 51 – Declaration of assets by the Minister

354. Subclause 51(1) outlines the basis upon which the Minister can privately declare an asset to be a ***critical infrastructure asset*** for the purposes of the Bill.

355. 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 clause 9, being a ***critical electricity asset***, as defined in clause 10; a ***critical gas asset*** in clause 12; a ***critical port*** as defined in clause 11; a ***critical water asset*** as defined in clause 5; or an asset prescribed by the ***rules***.

356. The second limb is that the asset relates to a ***relevant industry***. ***Relevant industry*** is defined in clause 5 as electricity, water, gas 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 Bill 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.

357. 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***.

358. 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 risks to ***national security*** if it were publicly known that the ***critical infrastructure asset*** affects ***national security***.

359. 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 Bill 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 clause will ensure there is not public visibility of the link between the ***critical infrastructure asset*** and ***national security***.

360. Subclause 51(2) requires the declaration to specify the ***entity*** that is the ***responsible entity*** for the asset. A ***responsible entity*** is defined in clause 5 and refers to the ***entity*** with ultimate operational responsibility for the asset.

361. Subclause 51(3)(a) requires the Minister to notify each ***reporting entity*** for the asset of the declaration in writing within 30 days of making the declaration, while subclause 51(4) requires the notice to specify the obligations of the ***reporting entity***. This Bill imposes obligations on ***reporting entities*** in relation to an asset to provide a range of information. These subclauses will ensure that ***reporting entities*** in relation to a declared asset are aware of their obligations. ***Direct interest holders*** (defined in clause 8) for the declared asset will be required to report their ***interest and control information*** (as defined in clause 6) and the ***responsible entity*** (as specified in the declaration as a result of subclause 51(2)) will be required to report ***operational information*** (defined in clause 7) for the asset.

362. 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***.

363. The notification to ***reporting entities*** under subclause 51(3)(a) may also outline other obligations to which the ***reporting entities*** may be subject to under the Bill, such as an information gathering request (clause 37) or a direction issued under clause 32.

364. The Minister's declaration of an asset is also ***protected information*** as per subclause (b) of that definition in clause 5. As such, the unauthorised disclosure of the fact that an asset is declared, or any information obtained under this Bill 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 Bill is afforded the appropriate protections, given the sensitivities of the information and the criticality of the asset for ***national security***.

365. Subclause 51(3)(b) requires the Minister to notify the Premier or Chief Minister of the jurisdiction in which the declared ***critical infrastructure asset*** is located following the declaration. This ensures that state or territory governments are aware of the ***critical infrastructure assets*** in their jurisdiction to which the legislation applies and are able to work collaboratively with the Government to manage any risks that may arise, including through leveraging existing state or territory regulatory mechanisms.

366. Subclause 51(4) ensures that when notifying a ***reporting entity*** of the declaration, the Minister must also specify the obligations that the ***reporting entity*** is now subject to under the Bill. This will assist the ***reporting entity*** to understand their requirements under the Bill, and may reiterate that a declared asset under clause 51 is ***protected information*** under the Bill.

367. Subclause 51(5) provides that a declaration under subclause (1) is not a legislative instrument. The declaration under subclause 51(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 Bill. Rather, it determines particular cases and circumstances in which the law will apply. The inclusion of subclause 49(4) is to assist readers and avoid doubt in this respect.

Clause 52 – Notification of change to reporting entities for asset

368. Clause 52 requires the ***Secretary*** of the department to be notified within 30 days of a change in a ***reporting entity*** for an asset privately declared by the Minister to be a ***critical infrastructure asset***.

369. Subclause 52(1) outlines that the clause will apply when an existing ***reporting entity*** either ceases to be a ***reporting entity*** or becomes aware of another ***reporting entity*** for the asset. If either of these events exist, subclause 52(2) provides that the ***reporting entity*** must notify the ***Secretary*** of that fact. The notification must provide the details of the new ***reporting entity***, to the extent that is known by the current ***reporting entity*** The required details are:

- the name of the ***entity***, and
- the address of the ***entity***'s head office or principle place of business.

Example 1

Company W is the 100% ***direct interest holder*** in a gas storage asset that has been privately declared under clause 51. *Company A* sells 50% of its interest to *Company Y*. Under subclause 52(1), *Company W* is required to provide notification to the ***Secretary*** of this fact.

Example 2

Company M is the ***responsible entity*** for a gas storage asset that has been privately declared under section 51. *Company M's* contract ends and *Company P* becomes the ***responsible entity***. Under subclause 52(1), *Company M* is required to provide notification that *Company P* is now a ***reporting entity***.

370. Subclause 52(2) provides that this information must be provided to the ***Secretary*** within 30 days. A civil penalty of 150 penalty units applies if the notification is not provided within the timeframe or does not contain the required information,

371. Subclause 52(3) notes that the first entity must use best endeavours to obtain the information required by subclause 52(2)(b). This ensures they are not liable to a penalty if they took all reasonable steps to obtain the information.

372. This provision is required as the Minister's declaration of an asset is private and ***protected information*** under subclause (b) of that definition in clause 5. Without this provision, Government may not have visibility of any changes to the ***reporting entities*** as the provisions relating to ***protected information*** would prevent the first ***reporting entity*** communicating the declaration and obligations to any subsequent ***reporting entities***.

373. Subclause 52(4) requires the ***Secretary*** to notify the other entity of their obligation as a ***reporting entity*** of an asset which has been declared by the Minister to be a ***critical infrastructure asset***. The other entity must be notified by the ***Secretary*** in writing within 30 days of he or she receiving notification of a change in ***reporting entities***. This ensures they are aware of their obligations as a ***reporting entity*** under the legislation.

374. Subclause 52(5) ensures that when notifying a ***reporting entity***, the ***Secretary*** must also specify the obligations that the ***reporting entity*** becomes subject to under the Bill. This will assist the ***reporting entity*** to understand their requirements under the Bill, and may reiterate that a declared asset under clause 51 is ***protected information*** under the Bill.

PART 7—MISCELLANEOUS

Division 1—Simplified outline of this Part

Clause 53 – Simplified outline of this Part

375. The simplified outline is to assist readers to understand the substantive provisions, by providing an overview of the provisions within Part 7. Clause 53 is not intended to be comprehensive and should not be relied on in place of the substantive provisions within Part 7.

376. Part 7 details the reporting requirements on the operation of this Bill. 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 Bill, including the delegation of powers and ***rules***.

Division 2—Treatment of certain entities

Clause 54 – Treatment of partnerships

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

378. Subclause 54(1) provides that the Bill applies to a partnership as if it were an ***entity***, but with the changes set out in this clause. Under subclause 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.

379. Subclause 54(2) provides that an obligation that would otherwise be imposed on the partnership by this Bill is imposed on each partner instead, but may be discharged by any of the partners. This Clause provides clarity as to how a partnership is to meet its obligations under this Bill (the obligations may be discharged by any of the partners).

380. Subclause 54(3) provides that an offence against this Bill 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).

381. 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.

382. Subclause 54(4) extends the application of the clause 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 clause 30), the ***civil penalty provision*** is incurred by all other partners of the partnership.

383. Subclause 54(5) outlines that for the purposes of this Bill, a change in the composition of a partnership does not affect the continuity of the partnership. This clause ensures that where a new partner is admitted, or partner retires or dies, the Bill considers that the partnership continues unaffected.

Clause 55 – Treatment of trusts and superannuation funds that are trusts

384. This clause sets out how the Bill applies to trusts and ***superannuation funds***, including apportioning legal liability for offences and ***civil penalty provisions*** against this Bill. Subclause 55(1) provides that the Bill 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 clause. Under subclause 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 subclause 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 clause 5 as having the same meaning given by section 10 of the *Superannuation Industry (Supervision) Act 1993*.

385. Subclause 55(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 Bill is imposed on each trustee instead, but may be discharged by any of the trustees, and
- an offence against this Bill 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).

386. Subclauses 55(2) and (3) ensure that the provisions of this Bill 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 Bill and also who is subject to an offence or penalty provision if the Bill is contravened in any way.

387. Subclause 55(4) extends the application of the clause 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***.

Clause 56 – Treatment of unincorporated foreign companies

388. The purpose of this clause is to set out how the Bill applies to ***unincorporated foreign companies***, including apportioning legal liability for offences and civil penalties against this Bill. Subclause 56(1) provides that the Bill applies to an ***unincorporated foreign company*** as if it were an ***entity***, but with the changes set out in this clause.

389. Under subclause 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 clause 5 as a body covered by subclause (b) of the definition of foreign company in section 9 of the *Corporations Act 2001*. An ***appointed officer*** is also defined in clause 5 to include the Secretary of the company, or an officer of the company appointed to hold property on behalf of the company.

390. Subclause 56(2) provides that an obligation that would otherwise be imposed on the ***unincorporated foreign company*** by this Bill 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 clause ensures that the provisions of this Bill are placed on the ***appointed officer*** as a legal person, as ***unincorporated foreign companies*** themselves do not have a separate legal identity.

391. Subclause 56(3) provides that an offence against this Bill 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***).

392. 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 Bill, and also who is subject to an offence or penalty provision if the Bill is contravened in any way.

393. Clause 56(4) extends the application of the provision to the contravention of a ***civil penalty provision*** in a corresponding way to the way in which it applies to an offence. This means that joint liability is imposed 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

Clause 57 – Additional power of the Secretary

394. Clause 3 outlines the object of this Bill, which is to provide a framework for managing ***national security*** risks relating to critical infrastructure. In line with this overarching objective, clause 57 provides the ***Secretary*** with the power to undertake an assessment of a ***critical infrastructure asset*** to determine if there is a ***national security*** risk.

395. This power is in addition to, and does not limit, any of the other powers or functions under this Bill. In particular, this clause complements the other provisions in the Bill 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).

396. Importantly, while not explicit in the provision, in line with the objects in clause 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.

Clause 58 – Assets ceasing to be critical infrastructure assets

397. This clause requires the ***Secretary*** to provide written notice to a ***reporting entity*** of an asset if the ***Secretary*** becomes aware that the asset has ceased to be a ***critical infrastructure asset***. An example of when this situation may arise would be when a specified ***critical infrastructure asset*** is declared to not be a ***critical infrastructure asset*** under the rule making power at clause 9(2).

Clause 59 – Delegation of Secretary's powers

398. Subclause 59(1) allows the ***Secretary*** to delegate his or her powers, functions or duties under this Bill to a Senior Executive Service (SES) employee, or an acting SES employee, in the department. The expressions 'SES employee' and 'acting SES employee' are defined in section 2B of the *Acts Interpretation Act 1901*. The ***Secretary***'s powers, functions and duties under this Bill 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 Bill.

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

400. Subclause 59(2) outlines that any employee performing functions under a delegation is compelled to only act as authorised by that delegation. This ensures the powers or functions authorised by SES employee cannot go beyond the scope of the Bill.

Division 4—Periodic reports and rules

Clause 60 – Periodic report

401. Part 7, Division 4 details the ***Secretary***'s reporting obligation to the Minister on the operation of this Bill. The periodic reporting will ensure the Government reports to Parliament (and therefore publicly) on the operation of this Bill, including details of how many times the powers in the Bill have been used in the financial year.

402. Subclause 60(1) requires the ***Secretary*** to report to the Minister each financial year on the operation of the Bill. Subclause 60(1) requires this report to be presented to Parliament.

403. Subclause 60(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 subclause 32(2)
- the use of the ***Secretary***'s information gathering power at clause 37
- any enforcement action taken relating to failures to comply with obligations under the Bill, and
- the number of assets declared as ***critical infrastructure assets*** under clause 51.

404. This annual overview on the operation of the Bill provides accountability and transparency of the Bill's application to ***critical infrastructure assets***, including how often the powers are used.

405. Despite subclause 60(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.

406. Subclause 60(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.

Clause 61 – Rules

407. Clause 61 provides the general rule-making power in the Bill. Providing for a general instrument-making power under a Bill is a long-standing practice. This is to allow certain matters, as prescribed under the Bill, to be provided for in subordinate legislation where appropriate.

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

409. 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 clause 61(2) and include creating an offence, imposing a tax, and directly amending the text of the Bill.

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

- details about what is meant by ***interest and control information*** (subclause 6(1)(i))
- details about what is meant by ***operational information*** (subclause 7(1)(g))
- prescribing assets, or not prescribing assets, for the purposes of the definition of ***critical infrastructure asset*** (subclauses 9(1)(f) and 9(2)), and
- the requirements for an electricity generation station to be critical (subclause 10(2))
- prescribing a port to be a ***critical port*** (subclause 11(u))
- prescribing specified gas transmission pipelines or requirements for a gas transmission pipeline (subclause 12(2)), and
- prescribing sections of the *Corporations Act* or another law of the Commonwealth to apply to an asset declared under clause 51 to be a ***critical infrastructure asset*** (subclause 46(2).

411. These matters (and others in the Bill) 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 should not be required to be dealt with through amendments to the Bill.

REGULATION IMPACT STATEMENT

Background

1. In January 2017, the Australian Government (the Government) established the whole-of-government Critical Infrastructure Centre (the Centre) within the Attorney-General's Department. The Centre was established 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.

2. 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 the following high-risk sectors:

- **Telecommunications:** Australian telecommunications systems and networks are part of our national critical infrastructure and form the backbone for many other critical infrastructure sectors and services. On 18 September 2017, the Parliament passed comprehensive Telecommunications Sector Security Reforms legislation to manage these risks. The Centre will implement these reforms and will operate separately to this Bill.
- **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 needs 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.
- **Gas:** Gas in Australia is an important energy source, an export commodity and an input for a wide range of industrial, commercial and residential uses. Gas is particularly important for gas powered electricity generators which account for approximately 20 per cent of Australia's electricity, and manufacturing which relies on gas for approximately 40 per cent of net energy requirements.
- **Ports:** Australia relies heavily on its commercial ports to trade goods with the world, with one third of GDP facilitated through seaborne trade. Ports support Australia's prosperity, our supply of liquid fuels, the supply chains for other critical infrastructure and are critical for Defence purposes. Disruption to our most ***critical ports*** could have wide-reaching impacts on the economy.

3. 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:

- **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, a telecommunications ***operator*** or contractor could monitor customers' voice or 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 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, or control of, critical infrastructure to apply coercive power against state, territory or Australian Governments to influence decision-making or policy. For example control of an essential critical infrastructure service could impose spurious limitations on the operation of the service to coerce government decision making.

4. In February 2017, the Australian Government commenced consultations with states, territories and industry on the operation of the Centre and two regulatory measures to assist in managing risks to ***national security***:

- a ***Register*** of ***critical infrastructure assets*** in high risk sectors; and
- a 'last resort' power for the Minister to issue a direction where there is a significant risk to ***national security*** that cannot otherwise be mitigated.

5. In October 2017, the Centre conducted nationwide consultations on exposure draft legislation. The purpose of the consultations was to:

- ensure stakeholders understood the need for the legislation and its proposed scope and application, and
- work with stakeholders to ensure the legislation imposed the minimum regulatory impact required to manage the ***national security*** risks.

The Problem

6. 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.

7. 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, nor 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.

8. 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

9. 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. 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.

10. 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

11. 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 where there may be vulnerabilities in an asset or sector. To determine what vulnerabilities may exist, it is essential to have a detailed understanding of who owns, controls or has access to a particular asset.

12. 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 Foreign Investment Review Board (FIRB).

13. In the absence of existing mechanisms to obtain this information, government agencies have difficulty in identifying and understanding legal and more specifically 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.

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

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

15. Once the Centre has assessed the risks from foreign involvement in an asset, it looks to work collaboratively with the asset owner and ***operators*** 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 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 mitigations when necessary to address risks to ***national security***.

16. 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 to manage risk. However, existing state-based mitigations 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 any identified risk of espionage, sabotage or coercion.

Further measures are needed to protect Australia's critical assets

17. Existing gaps in the Government's understanding of the ownership and control of critical infrastructure, and the lack of a mechanism at the Commonwealth level to intervene where a significant risk to ***national security*** has been identified, limit our 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. For example, the September 2016 black out in South Australia, which only lasted several days, was assessed to cost businesses $367 million.

18. The more extreme examples of risks to ***national security*** are unlikely to occur outside a significant shift in regional or global strategic relationships or imminent armed conflict. However, there are nevertheless 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 over time.

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

Case for Government action

20. 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.

21. The lack of transparency in legal and beneficial ownership makes it difficult for security agencies and the Centre to:

- identify who has ultimate control over Australia's critical infrastructure
- understand risks associated with changes of ownership and control, and
- develop suitable mitigations to address ***national security*** risks wherever they arise.

22. Further, while the Centre will work collaboratively with critical infrastructure owners and ***operators*** to mitigate ***national security*** concerns (and owners and ***operators*** have shown that they would work with the Centre to address risks to ***national security***), there are circumstances where there is nothing the Government can do if an owner/***operator*** does not implement the Centre's suggested ***national security*** mitigations.

23. The outcomes sought to address these two problems are:

1. A mechanism that sources information on ownership and control of critical infrastructure, comprising:

- legal and beneficial ownership and operation information
- description of the ***critical infrastructure asset***

- board structure and ownership rights information, and
- operational management information.

2. A mechanism that enables the Government to take steps to address ***national security*** risks where all other options have been exhausted.

24. The main constraint is ensuring that the chosen option is proportional to the identified risks and does not act as a disincentive for foreign investment and involvement in our ***critical infrastructure assets***.

Policy options

25. The Government has considered a number of options to achieve the stated outcomes above:

Outcome 1: Sourcing ownership and control information of critical infrastructure

Option 1: Maintain status quo

26. Under this option, the Government would continue to rely solely on cooperation with owners and ***operators*** to voluntarily provide information on ownership, which may not extend to beneficial ownership. The states and territories already collect information from owners and ***operators***, however this information varies from jurisdiction to jurisdiction and does not provide sufficiently detailed information about ownership and control that would be useful to the Centre in prioritising and conducting risk assessments.

27. While this option does not create any additional regulatory burden on owners and ***operators***, it means that the Government will continue to rely on limited and fragmented information sources as it aims to build a complete picture of the ***national security*** risks to critical infrastructure.

Option 2: Leverage or aggregate information from existing sources and/or registers to create a Commonwealth register for critical infrastructure

28. This option would draw on existing registers and collate their information to create a register administered by the Centre. This option would require extensive consultation with state and territory governments to establish information flows to the Centre from their existing registers. Utilising already established registers would not add extra regulatory burden to owners and ***operators***. However, the scope of information currently collected generally, or as part of a register administered by the Australian Government or states and territories, varies from one jurisdiction to another:

- Several jurisdictions administer their own critical assets registers for various purposes. However, these registers do not collect information on shareholders or beneficial ownership, identify the aggregate ownership by particular countries, include names of senior management/directors, or outsourcing arrangements.
- Reg 9.1.02 of the *Corporations Regulations 2001* identifies the information recorded on the Australian Securities and Investments Commission's (ASIC) registry. It does not identify beneficial ownership, classify data by industry sectors, or identify the aggregate ownership by particular countries. ASX listings have similar limitations and are limited to companies listed on the ASX.
- While the AEMO keeps records of legal owners, asset names and locations (and only for the electricity and gas sectors), it does not keep information that identifies beneficial ownership, aggregate ownership by particular countries, or the names of senior management/directors and registered office address.

29. Cumulatively, these existing registers do not provide sufficient information on ownership and control to address the issues identified by the Centre.

30. Additionally, this option would require extensive negotiation with the states and territories, owners, and ***operators*** to agree on a process to share information. This would likely also require legislative amendments across jurisdictions to allow information to be shared and used for purposes other than those for which it was originally collected.

Option 3: Implement a new Commonwealth critical infrastructure asset register

31. A legislated ***Register*** of ***critical infrastructure assets*** would capture and track information about who owns and operates Australia's most critical assets in the highest-risk sectors of water, ports, electricity and gas. The need to provide information for the ***Register*** would apply to all high risk asset owners, both domestic and foreign, in high-risk sectors. The Centre would engage with asset owners in the highest-risk sectors to assist them to understand and meet their requirements.

32. The Government has considered two options for the ***Register*** that balance competing considerations of potential regulatory burden and the amount/depth of information that should be reported:

Option 3(a): Broad information reporting requirements for the register:

- legal and beneficial ownership information, including name, address of companies or persons and ***ABN*** (if applicable), and country of incorporation/domicile
- detailed ***operational information***, including reporting operating contracts with third parties and supplying documentation
- detailed description of owned/operated critical assets and their footprints—maps and information on key dependencies etc.
- information on board members (full name and citizenship details) and senior management structure, including providing company constitutions that detail voting rights, board appointments and removals, organisational chart and names of directors, senior management (CEO, CIO, COO, Chief Security Officer), and
- reporting detailed information on all outsourcing and offshoring contractual arrangements, including full names and citizenship details of the ***operator's*** board members and senior management.

Option 3(b): Narrow information reporting requirements for the register:

- legal and beneficial ownership information, including name, address of companies or persons and ***ABN*** (if applicable), and country of incorporation/domicile
- basic information on entities who operate the critical asset (or parts thereof) on behalf of the owner, including a description of area(s) of operations
- short description of the ***critical infrastructure asset***
- information on board members (full name and citizenship details) and short description of board structure and ownership rights, and
- basic ***operational information*** (including outsourcing and offshoring arrangements).

33. The information collected on the ***Register*** would inform the work of the Centre, particularly informing which assets require further and more detailed ***national security*** risk assessments. The Centre would work with all levels of government, regulators, and owners and ***operators*** as appropriate during the risk assessment process to identify and manage risks.

Outcome 2: A mechanism enabling Government to address *national security* risks where all other regulatory options have been exhausted

Option 1: Maintain status quo

34. Under this option, the Government would continue to rely on cooperation with states, territories and industry to manage risks. This option would continue the current reliance on existing powers in Commonwealth, state and territory legislation. Noting that only some jurisdictions have legislative regimes to manage critical infrastructure, and the regulation of the high-risk sectors varies, there would continue to be gaps in the Government's ability to compel a critical infrastructure owner or ***operator*** to mitigate an identified ***national security*** risk. These limitations exist at both state and federal levels. For example, the powers available to the Office of Transport Security in managing ***security*** risks to ports and airports are directly related to preventing acts of terrorism and do not extend to broader ***national security*** concerns such as foreign interference.

Option 2: Work with states and territories to strengthen existing regulatory mechanisms

35. This option recognises that states and territories are primarily responsible for the management of the high risk sectors, particularly water, gas and electricity. Through this option, the Centre would actively work with the states and territories to strengthen their existing legislative/regulatory regimes. The Government would work closely with each jurisdiction to identify any gaps in existing state regimes, and ensure they have the necessary powers to mitigate identified ***national security*** risks. In some states, this may require fairly significant revisions to existing laws.

36. This option would likely involve significant time and resources working with each state and territory (similar to negotiating with the states and territories to adjust their existing registers). It may also be difficult to get consensus with each state and territory, resulting in different mechanisms across jurisdictions. If this occurs, and for example, powers in one state or territory are more comprehensive than another, it may leave some assets more vulnerable to exploitation by foreign intelligence services.

37. In the event existing state and territory regimes were strengthened, the Government would still rely on state cooperation to implement risk mitigations through these regimes. There may be occasions where a state or territory has a vested financial interest in the privatisation of a particular ***critical infrastructure asset*** and may be reluctant to fully accept Commonwealth advice on an identified risk. Alternatively, they may agree with the risk identified, but disagree with the mitigations recommended to manage the risk.

Option 3: Implement a Ministerial directions power

38. Under this option, the Minister would have the power to issue a direction to the legal owner or an ***operator*** of an asset to mitigate significant ***national security*** risks.

39. A Ministerial direction would only be able to be issued in instances where certain ***national security*** risks cannot be appropriately mitigated through the:

- best efforts of the Centre to work with the asset owner or ***operator***, or
- application of existing regulatory frameworks, such as licensing schemes that already require critical infrastructure owners to comply with a range of operating conditions.

40. The Government has considered four options for the Ministerial directions power, which vary in accordance with the scope of directions available and the level of safeguards. These options are outlined in the below matrix:

		Scope of Directions	
		Narrow	**Broad**
Safeguards	**High**	Option 3(a): The Minister **must:** - observe all safeguards; and - issue directions limited to certain matters (not including terminating contracts etc)	Option 3(b): The Minister **must:** - observe all safeguards; and - issue directions on a broad range of matters (including terminating contracts etc)
	Low	Option 3(c): The Minister **may:** - have regard to safeguards; and - issue directions limited to certain matters (not including terminating contracts etc)	Option 3(d): The Minister **may:** - have regard to safeguards; and - issue directions on a broad range of matters (including terminating contracts etc)

Description of safeguards and scope of directions

41. The following table outlines the safeguards that must be observed before a direction is issued and the scope of directions available:

Safeguards		**Scope of Directions**	
Low level	• Mandatory consideration of an ASIO Adverse Security Assessment • Good faith negotiations with the asset owner • Consult with the relevant state/territory First Minister; • Consider existing Commonwealth, state and territory regulatory mechanisms • Written notice	Narrow	• Require onshoring of data into a certified cloud services provider • Directions to provide sensitive information
High level	The above safeguards AND: • Direction must be proportionate to the identified risk	Broad	The above scope AND, for example, directions that: • Limit offshore access to

• Consideration of:
  o Costs of complying with the direction
  o Consequences to industry competition
  o Consequences to services or customers
		industrial control systems
		• Prevent outsourcing core network operations to certain providers (terminating contracts)
		• Prevent sourcing core operational systems technology from certain providers

Option 3(a) – a Ministerial directions power that is limited to certain matters and a high-level of safeguards are in place

42. Under this option, while the full range of safeguards would be observed by the Minister, the Minister's powers would be limited to directing an owner or ***operator*** of an asset to provide sensitive information on certain matters or require actions to manage data security such as onshoring data into a certified cloud services provider. It would not allow the Minister to direct the owner/***operator*** to take, or refrain from taking, steps to mitigate the risk and would therefore be a limited tool for Government.

Option 3(b) – a Ministerial directions power where a broad range of directions are available and a high-level of safeguards are in place

43. This option provides the Minister with a directions power that can address a broad range of ***national security*** risks—including directions that compel owners/***operators*** to perform certain risk mitigation actions. This directions power is coupled with strong safeguards that ensure the direction is proportionate to the identified risk for which costs and consequences to industry and their customers are considered.

Option 3(c) – a Ministerial directions power that is limited to certain matters and a low-level of safeguards are in place

44. Under this option, the Minister's powers would be limited to directing an owner or ***operator*** of an asset to provide information on certain matters or require actions to manage data security such as onshoring data into a certified cloud services provider. It would not allow the Minister to direct the owner/***operator*** to take any steps to mitigate the risk and would therefore be a limited tool for Government. Low-level safeguards would accompany this directions power, which means there would be no consideration of the costs and consequences for the owner/***operator*** or the flow-on effect to customers. Because of this, low-level safeguards are unlikely to be supported by owners and ***operators***.

Option 3(d) – a Ministerial directions power where a broad range of directions are available and a low-level of safeguards are in place

45. This option provides the Minister with a directions power that can address a broad range of ***national security*** risks to critical assets. However, industry is likely to consider this directions power to be overbearing when coupled with low-level safeguards. Under this option, the Minister would not be required to ensure that the direction is proportionate to the risk, or consider the cost or consequences to industry and their customers. Given the potential uses of a broad Ministerial directions power, there is a far greater need for stringent safeguards.

Cost and benefits of each option

Outcome 1: Sourcing ownership and control information of critical infrastructure

Option 1: Maintain status quo

Benefits:

46. The benefit of this option is that it would not result in additional administrative or compliance costs for industry. Under current circumstances, costs would continue to be incurred by industry in reporting information as part of existing regulatory requirements, such as reporting changes to the ASIC registry.

Costs:

47. The Australian Government, states and territories would incur ongoing indirect costs of not having clear visibility of legal and beneficial ownership and control of ***critical infrastructure assets*** and may result in circumstances where the Government is not able to clearly identify and address ***national security*** risks. This would have particular impacts on the ability of the Government to effectively manage ***national security*** issues.

Option 2: Leverage or aggregate information from existing information and/or registers to create a Commonwealth register for critical infrastructure

Benefits:

48. This option would not involve any costs for business. The benefit of this option is that it utilises existing data sets to identify ownership and control of ***critical infrastructure assets***, although the scope and application of this information is limited. This option would not impose any additional regulatory burden on business as all information is currently collected.

Costs:

49. This option would involve significant allocation of resources in the Australian Government and state governments. Utilising existing information sources/registers would be resource intensive as it would require significant consultation with each state and territory (with no guarantee that the consultations will be successful). It may also require the Government to provide funding to the states and territories to implement updates to their information sources/registers to enable the information to be fed to the Government. There would also be significant time costs for jurisdictions if legislative updates were required to provide information to the Government for these purposes. The resulting register would still fall short of providing information on beneficial ownership of ***critical infrastructure assets*** which is an important indicator of influence and control over an asset.

50. Integration of the Centre's ***Register*** with other registers, such as ASIC would reduce the reporting burden to some extent. However, The Treasury and the Department of Industry, Innovation and Science are undertaking work to modernise business registers administered by the ASIC and the Australian Taxation Office. While it would be highly beneficial to integrate the critical assets ***Register*** contained in this Bill with this work, it appears that the register modernisation work will not be ready to incorporate other registers until 2020 at the earliest.

Option 3(a): Implement a new Commonwealth critical infrastructure assets register (broad information reporting requirements)

Benefits:

51. The benefit of this option is that it provides a single comprehensive resource of information on legal and beneficial ownership and control of ***critical infrastructure assets***. Information from the ***Register*** would also be able to be shared with states and territories in prescribed circumstances to assist in their understanding of ***critical infrastructure assets*** in their jurisdiction.

Costs:

52. Public sector: The estimated cost of building an IT solution for the ***Register*** has not yet been determined. However, funding already provided to the Attorney-General's Department over the forward estimates will be used to support the development of an IT solution.

53. Investment: A ***Register*** with broad information requirements may act as a disincentive for foreign entities to invest into Australia if they perceive that the regulatory requirements are cumbersome, intrusive or beyond the scope of usual business requirements.

54. Regulatory: The regulatory cost for captured ***critical infrastructure asset*** owners and ***operators*** can be broken down into a once-off reporting requirement and an ongoing obligation to update the owner/***operators' Register*** entry in response to changes of circumstances.

55. Total annual once-off reporting costs of the required information for captured assets in the water, ports, gas processing, storage, transmission and distribution, and electricity generation, transmission and distribution sectors is $108,780, or $711 per captured critical asset owner/***operator***. This is averaged out over a 10 year period.

56. The annual costs of ongoing reporting of changes in ownership and control information for the captured assets in the four sectors is $36,607 or $239 per captured critical asset owner/***operator***.

Average annual regulatory costs (from business as usual)		
Change in costs	Business	Total change in cost
Electricity generation	$40,393	$40,393
Electricity transmission/distribution	$19,091	$19,091
Gas processing/storage	$17,780	$17,780
Gas transmission/distribution	$32,049	$32,049
Ports	$14,952	$14,952
Water	$21,122	$21,122
Total	$145,387	$145,387

57. Cost assumptions: The regulatory burden of the ***Register***'s reporting obligations varies 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 outlined above 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)).
- Gas transmission and distribution assets each have two ***direct interest holders*** (a majority & minority holder) in addition to its ***responsible entity*** and three ***operators***. Each ***direct interest holder*** has one 'other ***entity***'.
- Gas processing and storage assets each have two ***direct interest holders*** (a majority & minority holder) in addition to its ***responsible entity*** and three ***operators***. Each ***direct interest holder*** has one 'other ***entity***'.
- 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 17.5 hours providing the initial ***interest and control information*** and then four 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 40.2 hours spent providing the initial ***operational information*** and then 11.45 hours updating ***operational information*** when required.
  - On average, an electricity, gas, water and 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 executive 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 executive officer is assumed to happen 1.4 times.
  - ***Operational information*** includes detailed information on asset ***operators*** and a description of the regulated/licenced area of the asset; providing information on company constitutions and organisational charts, and name, citizenship details and access rights of the Board members, Chief Operating Officer, Chief Information Officer and Chief Security Officer; detailed information on

outsourcing and offshoring contracts, and the names of ***operators'*** board members and senior management (including citizenship details).

- 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.

Option 3(b): Implement a new Commonwealth critical infrastructure assets register (narrow information reporting requirements)

Benefits:

58. The benefit of this option is that it minimises the reporting burden on critical infrastructure owners, given it only requires narrow information. It will also be a single targeted resource of legal and beneficial ownership and control of ***critical infrastructure assets***. Information from the ***Register*** would be available to the states and territories in prescribed circumstances to assist in the understanding of ***critical infrastructure assets*** in their jurisdiction.

59. A ***Register*** with narrow information requirements is less likely to reduce foreign entities interest in investing in Australia. Providing limited information, which is readily available in the normal course of business operations, is more likely to be consistent with a company's investment objectives to make a positive contribution to the country and to comply with Australian laws.

Costs:

60. Public sector: The estimated cost of building an IT solution for a ***Register*** with narrow information reporting requirements will be similar to Option 3(a).

61. Regulatory: Total annual once-off reporting costs of the required information for captured assets in the water, ports, gas processing, storage, transmission and distribution, and electricity generation, transmission and distribution sectors is $73,265 or $478.85 per captured critical asset owner/***operator***. This is averaged out over a 10 year period.

62. The annual costs of ongoing reporting of changes in ownership and control information for the captured assets in the four sectors is $13,524, or $88.39 per captured critical asset owner/***operator***.

Average annual regulatory costs (from business as usual)		
Change in costs	Business	Total change in cost
Electricity generation	$24,887	$24,887
Electricity transmission/distribution	$11,939	$11,939
Gas processing/storage	$10,442	$10,442
Gas transmission/distribution	$18,514	$18,514
Ports	$9,103	$9,103

Average annual regulatory costs (from business as usual)		
Water	$11,924	$11,924
Total	$86,789	$86,789

63. Cost assumptions: The regulatory burden of the ***Register***'s reporting obligations varies 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 outlined above 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)).
- Gas transmission and distribution assets each have two ***direct interest holders*** (a majority & minority holder) in addition to its ***responsible entity*** and three ***operators***. Each ***direct interest holder*** has one 'other ***entity***'.
- Gas processing and storage assets each have two ***direct interest holders*** (a majority & minority holder) in addition to its ***responsible entity*** and three ***operators***. Each ***direct interest holder*** has one 'other ***entity***'.
- 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 16 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 16 hours spent providing the initial ***operational information*** and then 1.25 hours to updating ***operational information*** when required.
  - On average, an electricity, gas, 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 executive 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 executive 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 executive 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.

Outcome 2: A mechanism enabling Government to address *national security* risks where all other regulatory options have been exhausted

Option 1: Maintain status quo

Benefits:

64. The benefit of this option is that there would be no administrative or compliance cost on industry. Under current arrangements, industry would continue to incur costs of complying with existing regulatory regimes.

Costs:

65. The cost would be the Australian Government, state and territories' inability to mitigate against identified ***national security*** risks if they do not fall within the remit of an existing regulatory regime.

Option 2: Work with states/territories to strengthen existing regulatory mechanisms

Benefits:

66. The benefit of this option is that it could simplify the regulatory compliance obligations for industry, who are already familiar with the existing state and territory regulatory bodies and mechanisms. Working individually with the states/territories, however, may lead to measures that are inconsistent between jurisdictions. This would impose an added burden on industry to ensure they are meeting obligations that differ between states and territories.

Costs:

67. This option may involve additional costs for business, depending on the extent that state and territory governments agree to implement additional regulatory mechanisms to address risks to ***national security***. Because of the wide variability in the possible expansion of state/territory regulatory mechanisms, it cannot be determined what would be the associated costs for business. An estimate would place costs to industry in a similar range to the costs outlined for Option 3.

68. Further costs associated with this option would be the resources required for both the Australian Government and state and territory governments to negotiate the requirements of additional regulatory mechanisms in each jurisdiction to address potential risks to ***national security***. Similar to Outcome 1, Option 2, negotiation may take between one and two years to complete and may not be entirely successful. There will also be potential costs for the Government if negotiations resulted in inconsistent state and territory regulatory mechanisms that impede its ability to mitigate ***national security*** risks in particular jurisdictions.

Option 3: Implement a Ministerial direction power

Benefits:

69. Introducing a Ministerial directions power will ensure the Government has the necessary powers to address ***national security*** risks to critical infrastructure where these cannot be managed through other mechanisms.

70. Without this power, the Government would only be able to request assistance from critical infrastructure owners to mitigate risks, and rely on mutual interest to ensure the risk is addressed. The benefit of the directions power will be in instances where assistance is not provided and risks are not mitigated. Subject to the safeguards in issuing a direction, this power will allow the Government to ensure the ***national security*** risks are addressed.

Costs:

71. The regulatory costs of imposing a Ministerial direction would vary widely depending on the scope of the direction and the individual circumstances of the ***entity*** subject to the direction.

72. The Minister's use of the directions power may change foreign investors' perceptions of sovereign risk in Australia if it is considered that the directions power is being abused. This would have a significant impact on the Australian economy which is highly dependent on foreign capital which is needed to grow the economy, increase productivity and living standards, and to create jobs.

73. To assist in providing indicative costs, four different scenarios have been modelled. Each of the costs provided below have been developed using the following assumptions:

- 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 18 ***entity*** types (small, medium large by electricity (generation, transmission/distribution), gas (processing, storage, 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***.

74. The total annual expected regulatory burden, averaged out over each scenario, sector and ***entity*** size based on the assumptions above, including using a Ministerial direction once every three years) is $8.12 million.

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

75. The annual compliance burden for captured asset owners and ***operators*** in the electricity, gas, water and ports sectors is $497,004.

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

- Costs of breaking contract with current data storage provider.
  - The 18 ***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. No multipliers are used, given procurement costs are unlikely to differ between ***entity*** size and industry.
- 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 is used based on the amount of data held.
- Independent compliance audit.
  - Assumed cost of approximately $60,000 with a frequency of 0.3 per year.

Average annual regulatory costs (from business as usual)			
Change in costs	Entity size	Costs to entity	Total sector change in cost
Electricity generation	Small	$1,782	$17,717
	Medium	$5,617	
	Large	$10,318	
Electricity transmission/ distribution	Small	$15,892	$149,128
	Medium	$49,739	
	Large	$83,496	
Gas processing/storage	Small	$10,662	$116,284
	Medium	$37,187	
	Large	$68,434	
Gas transmission/distribution	Small	$10,662	$116,284
	Medium	$37,187	
	Large	$68,434	
Ports	Small	$2,988	$32,737
	Medium	$10,749	

Average annual regulatory costs (from business as usual)			
	Large	$19,001	
Water	Small	$6,343	$64,855
	Medium	$21,325	
	Large	$37,187	
Total, by sector		$497,004	

One-off costs for scenario 1		
Electricity generation	Small	$64,155
	Medium	$101,098
	Large	$185,728
Electricity transmission/ distribution	Small	$572,126
	Medium	$895,305
	Large	$1,502,931
Gas processing/storage	Small	$383,849
	Medium	$669,373
	Large	$1,231,813
Gas transmission/distribution	Small	$383,849
	Medium	$669,373
	Large	$1,231,813
Ports	Small	$107,555
	Medium	$193,476
	Large	$342,010
Water	Small	$228,342
	Medium	$383,849
	Large	$669,373

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

77. The annual compliance burden for captured asset owners and ***operators*** in the electricity, gas, water and ports sectors is $67,488.

78. 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.
  - SCADA complexity and industry multipliers are applied.
- 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.
  - SCADA expertise and industry multipliers are applied.
- 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.

Average annual regulatory costs (from business as usual)			
Change in costs	Entity size	Costs to entity	Total sector change in cost
Electricity generation	Small	$1,559	$7,348
	Medium	$2,950	

Average annual regulatory costs (from business as usual)			
	Large	$2,839	
Electricity transmission/ distribution	Small	$3,609	$16,708
	Medium	$6,717	
	Large	$6,382	
Gas processing/storage	Small	$1,764	$8,284
	Medium	$3,327	
	Large	$3,193	
Gas transmission/distribution	Small	$2,994	$13,900
	Medium	$5,587	
	Large	$5,319	
Ports	Small	$1,969	$9,220
	Medium	$3,704	
	Large	$3,547	
Water	Small	$2,584	$12,028
	Medium	$4,833	
	Large	$4,610	
Total, by sector		$67,488	

One-off costs for scenario 2		
Electricity generation	Small	$56,119
	Medium	$53,107
	Large	$51,099
Electricity transmission/ distribution	Small	$129,933
	Medium	$120,898
	Large	$114,874
Gas processing/storage	Small	$63,500

	Medium	$59,886
	Large	$57,477
Gas transmission/distribution	Small	$107,789
	Medium	$100,560
	Large	$95,742
Ports	Small	$70,882
	Medium	$66,665
	Large	$63,854
Water	Small	$93,026
	Medium	$87,002
	Large	$82,987

Scenario 3: Direction preventing a business from outsourcing the operations of its core network to certain low-cost, low-quality providers.

79. The annual compliance burden for captured asset owners and ***operators*** in the electricity, gas, water and ports sectors is $3.79 million.

80. 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 (calculated with a 20% cost premium). 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. No multipliers are used, given that procurement costs are unlikely to differ between ***entity*** size and industry
- Costs of new SCADA system – initial setup and ongoing maintenance (software updates).
  - The cost of a new SCADA system is calculated with industry multipliers and also depends on the size of the critical asset and the sector in which it operates, ranging from $7 million for a small port and up to $75 million for a large electricity transmission/distribution network.

- Software updates and maintenance costs are calculated as the 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.

Average annual regulatory costs (from business as usual)			
Change in costs	Entity size	Costs to entity	Total sector change in cost
Electricity generation	Small	$21,848	$348,825
	Medium	$123,558	
	Large	$203,419	
Electricity transmission/ distribution	Small	$61,779	$1,027,645
	Medium	$363,141	
	Large	$602,725	
Gas processing/storage	Small	$25,841	$416,707
	Medium	$147,516	
	Large	$243,350	
Gas transmission/distribution	Small	$49,800	$823,999
	Medium	$291,266	
	Large	$482,933	
Ports	Small	$29,834	$484,589
	Medium	$171,475	
	Large	$283,280	
Water	Small	$41,814	$688,235
	Medium	$243,350	
	Large	$403,072	
Total, by sector		$3,789,999	

One-off costs for scenario 3

Electricity generation	Small	$786,541
	Medium	$2,224,041
	Large	$3,661,541
Electricity transmission/ distribution	Small	$2,224,041
	Medium	$6,536,541
	Large	$10,849,041
Gas processing/storage	Small	$930,291
	Medium	$2,655,291
	Large	$4,380,291
Gas transmission/distribution	Small	$1,792,791
	Medium	$5,242,791
	Large	$8,692,791
Ports	Small	$1,074,041
	Medium	$3,086,541
	Large	$5,099,041
Water	Small	$1,505,291
	Medium	$4,380,291
	Large	$7,255,291

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

81. The annual compliance burden for captured asset owners and ***operators*** in the electricity, gas, water and ports sectors is $3.77 million.

82. 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.
  - Infrastructure costs and industry multipliers are applied depending on industry sector.

- 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). No multipliers are used, given that procurement costs are unlikely to differ between ***entity*** size and industry.
- 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.
  - Infrastructure costs and industry multipliers are applied depending on industry sector.
- 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.
  - Infrastructure costs and industry multipliers are applied depending on industry sector.
- Costs to train staff in new intelligent devices.
  - 50 staff requiring one week of training for a large electricity (transmission/distribution) company.
  - Infrastructure costs and industry multipliers are applied depending on industry sector.
- Cost of Independent compliance audit.
  - Assumed cost of approximately $60,000 with a frequency of 0.3 per year.

Average annual regulatory costs (from business as usual)			
Change in costs	Entity size	Costs to entity	Total sector change in cost
Electricity generation	Small	$2,721	$102,245
	Medium	$21,374	
	Large	$78,149	
Electricity transmission/ distribution	Small	$190,186	$3,029,896
	Medium	$947,362	

Average annual regulatory costs (from business as usual)			
	Large	$1,892,348	
Gas processing/storage	Small	$8,866	
	Medium	$40,346	$127,249
	Large	$78,037	
Gas transmission/distribution	Small	$16,404	
	Medium	$78,037	$247,860
	Large	$153,419	
Ports	Small	$2,081	
	Medium	$6,424	$18,699
	Large	$10,193	
Water	Small	$16,404	
	Medium	$78,037	$247,860
	Large	$153,419	
Total, by sector		$3,773,808	

One-off costs for scenario 4		
Electricity generation	Small	$97,970
	Medium	$384,737
	Large	$1,406,684
Electricity transmission/ distribution	Small	$6,846,684
	Medium	$17,052,523
	Large	$34,062,255
Gas processing/storage	Small	$319,166
	Medium	$726,229
	Large	$1,404,666
Gas	Small	$590,541

transmission/distribution	Medium	$1,404,666
	Large	$2,761,541
Ports	Small	$74,929
	Medium	$115,635
	Large	$183,479
Water	Small	$590,541
	Medium	$1,404,666
	Large	$2,761,541

Summary of regulatory burden

83. The below table consolidates the regulatory burden for all of the proposed options.

Total average annual regulatory costs (from business as usual)				
Change in costs ($ million)	**Business**	**Community organisations**	**Individuals**	**Total change in costs**
Outcome 1: Sourcing ownership and control information of critical infrastructure				
Option 1: Maintain status quo	$0	$0	$0	$0
Option 2: Leverage or aggregate information from existing sources and/or Registers to create a Commonwealth Register for critical infrastructure	$0	$0	$0	$0
Option 3(a): Implement a new Commonwealth critical infrastructure asset Register with broad information reporting requirements	$145,387	$0	$0	$145,387
Option 3(b): Implement a new Commonwealth critical infrastructure asset Register with narrow information reporting requirements	$86,789	$0	$0	$86,789
*Outcome 2: A mechanism enabling Government to address **national security** risks where all other regulatory options have been exhausted*				

Total average annual regulatory costs (from business as usual)				
Change in costs ($ million)	**Business**	**Community organisations**	**Individuals**	**Total change in costs**
Option 1: Maintain status quo	$0	$0	$0	$0
Option 2: Work with states/territories to strengthen existing regulatory mechanisms	Unable to be determined[4]	$0	$0	Unable to be determined
Option 3(a): A Ministerial directions power that is limited to certain matters and a high-level of safeguards are in place	$497,004	$0	$0	$497,004
Option 3(b): A Ministerial directions power where a broad range of directions are available and a high-level of safeguards are in place	$8,128,299	$0	$0	$8,128,299
Option 3(c): A Ministerial directions power that is limited to certain matters and a low-level of safeguards are in place	$497,004	$0	$0	$497,004
Option 3(d): A Ministerial directions power where a broad range of directions are available and a low-level of safeguards are in place	$8,128,299	$0	$0	$8,128,299

84. This Regulation Impact Statement was submitted to the Office of Best Practice Regulation (OBPR) for early assessment in August 2017. OBPR assessed that the Regulation Impact Statement provided a good basis for decision making but that it could be further improved. The suggested improvements have been incorporated into this document.

Consultation

85. The options for the regulatory measures have been developed in close consultation with relevant Australian Government agencies, including the Australian Trade and Investment Commission and the departments of Agriculture and Water Resources, Communications and the Arts, Defence, the Environment and Energy, Foreign Affairs and Trade, Health, Infrastructure and Regional Development, Treasury and the Prime Minister and Cabinet.

86. In February 2017, the Government invited submissions to a discussion paper seeking views on the Centre's operations and the proposed regulatory measures. Accompanying the release, officials from the Centre travelled to each state and territory to brief government officials and

[4] While costings were not developed, the potential costs could be similar to Options 3(b) and (d).

industry representatives on the proposed regulatory measures. The Government again met with state and territory officials in May and June 2017.

87. The reforms were also discussed at a range of other fora including the Industry Consultation on National Security, Critical Infrastructure Advisory Council, and the Trade and Investment Minister's meeting.

88. At the June 2017 COAG meeting, the Australian Government, and states and territories committed to continuing to work together, and with industry, to manage the shared ***national security*** risks arising from foreign involvement in Australia's critical infrastructure.

89. On 2 August 2017, the Government again met with representatives from each jurisdiction to discuss the proposed regulatory measures. This was in addition to consultative forums with states and territories in February and June 2017.

90. In order to provide further clarity to investors, in June 2017 the Government held roundtable meetings for investment advisory companies and law firms.

91. An exposure draft of the legislation was circulated publicly on 10 October 2017 supported by a detailed explanatory document and relevant fact sheets. During the consultation process, there was direct, detailed engagement with key stakeholders in each jurisdiction, as well as industry owners and ***operators***, industry associations and law firms and investors.

92. The state and territory governments supported the need to address risks to ***national security*** concerning critical infrastructure and focused their comments on:

- constitutionality issues of the proposed measures, particularly ensuring that the proposed measures do not conflict with the States' constitutional functions (the Melbourne Corporations principle)
- clarifying how the proposed measures interact with existing regulatory mechanisms at the state/territory and Commonwealth level (including the foreign investment review process)
- the Government's approach to engagement on proactive risk assessments
- clarifying asset definitions and how the Government would add new assets to the legislation
- the consultation before an asset is declared by the Minister as a ***critical infrastructure asset***, and
- how the Government would share information provided to the assets ***Register***.

93. Officials-level submissions from the states considered that it was difficult to quantify potential costs of reporting obligations without detail on the scope and amount of information required to be reported and the associated time required to approve information that is reported to the ***Register***. Further detail on reporting requirements have been included in the Explanatory Memorandum, including various examples of information that would need to be reported in accordance with the ***approved forms***. In addition, the costs of complying with reporting obligations have been refined to better take account of the costs associated with internal approval processes required before information can be reported to the ***Register***.

94. Industry stakeholders also broadly supported the objective of the Bill, with feedback focusing on:

- clarifying reporting obligations and asset definitions

- the commercial impact of compliance with a Ministerial direction and the costs of complying with ***Register*** obligations
- ensuring the ***security*** and limited distribution of ***protected information***, and
- the need for clear guidance on the definition of ***operator***.

95. The costings in this Regulation Impact Statement have been revised in light of feedback from industry, resulting in a more accurate indication of the potential costs of complying with the ***Register***'s obligations. Feedback from industry also identified some unintended consequences from the Bill's definitions that would have further increased the regulatory burden on industry. For example, the scope of the definition of a ***critical infrastructure asset***.

Option selection/conclusion

96. The preferred approach is to pursue a new risk-based legislative framework that balances the need to manage the ***national security*** risks to critical infrastructure while supporting operational efficiencies and further investment.

Outcome 1: A mechanism to source ownership and control information of critical infrastructure

97. Of the options considered, Option 3(b), implementing a new Commonwealth ***Register*** of ***critical infrastructure assets*** with narrow information requirements, best meets the Government's need for a greater understanding of legal and beneficial ownership of critical assets, in order to build a comprehensive picture of risk.

98. Under Option 3(b), the ***Register***'s framework would strike a balance between getting the information necessary to inform risk assessments and minimising the administrative burden on industry. Specifically, the information required to be provided by ***reporting entities*** would ensure governments have greater transparency around access, control and ownership, particularly through the beneficial ownership disclosure requirements. If required, further detailed information would be sought from the ***entity*** under Part 4, Division 2 of the legislation.

99. Under Option 3(b), there will be a minor increase in the regulatory burden to industry in addition to existing administrative and compliance costs, which would vary from small to large-sized entities and across the four highest risk sectors. The regulatory burden for ***reporting entities*** across the four highest risk sectors under Option 3(b) is expected to be $86,789 per year.

100. Option 3(a) would impose a far greater administrative burden on industry at nearly double the cost of Option 3(b) ($145,387 per year). This option would also create a greater administrative impost on Government, who would be responsible for assessing the detailed information provided by industry. The Centre's preference is to collect basic information from ***reporting entities*** and triage what further targeted information should be requested (as part of more detailed risk assessments) to gain a clearer picture of ***national security*** risks.

101. Option 2 is not preferred as existing registers do not provide sufficient information on ownership and control to address the ***national security*** risks identified by the Centre. Additionally, this option would require extensive negotiation with the states and territories, owners and ***operators*** to agree on a process to share information. This option would likely also require legislative amendments across jurisdictions to allow information to be shared and used for purposes other than those for which it was collected. This option is therefore unlikely to effectively reach the desired outcome.

Outcome 2: A mechanism allowing Government to address *national security* risks where all other regulatory options have been exhausted

102. Of the options considered, Option 3(b), implementing a Ministerial directions power, is Government's preferred option. This option would enable the Minister to direct specific risk mitigation actions, where significant ***national security*** risks are present and all other risk management avenues have been exhausted. Option 3(b) would include stringent safeguards, ensuring that risk mitigations are proportionate to the identified risk, consultations occur with the relevant State/Territory ***First Minister***, good faith negotiations have occurred with the relevant ***entity***, and consideration is given to the cost and consequences of the mitigation on the owner/***operator*** and their customers or services, and on competition in the sector.

103. These safeguards were developed following consultation with the states and territories who sought specific safeguards to guard against the Commonwealth exercising powers in circumstances where existing state and territory frameworks were able to be used. Consultation also highlighted the importance of continued collaboration with states, territories and industry.

104. As part of considering whether to issue a direction, the Minister must consider the costs of complying with the direction and the impact on consumers and competition (for the ***entity*** itself and the sector as a whole). This would include considering who would bear the costs of the direction and whether those costs could be (in part or in full) passed on to consumers in accordance with the regulatory pricing regime of the asset in question.

105. The other sub-options under Option 3 do not strike the appropriate balance between ensuring that the Minister has the ability to direct appropriately targeted risk mitigations, and stringent safeguards to govern the application of the directions power.

106. Option 2, working with states/territories to strengthen existing regulatory mechanisms, would likely involve significant time and resources in working with each state and territory (similar to negotiating with the states and territories to adjust their existing registers) to get consensus. Under this option, the Commonwealth would also still rely on states' cooperation to implement risk mitigations. This option is therefore unlikely to effectively reach the desired outcome.

107. There will be an increase in regulatory burden to an asset owner or ***operator*** in complying with a Ministerial direction. In the absence of a Ministerial direction, there will be no additional burden on industry from this option. The costs incurred if a direction was issued would vary from small to large-sized entities and in the scope of the direction imposed. The annual regulatory burden to industry under Option 3(b) is expected to be $8.12 million per year (assuming the directions power is used once every three years).

Implementation and evaluation

108. Should Parliament pass this Bill, the Government would work closely with industry and state and territory governments to ensure that they are aware of and understand their obligations during the six-month ***grace period***. The legislation would be supported by administrative guidelines (issued and updated whenever required), and timely and specific advice from security agencies on identified areas of risk and steps required to mitigate those risks.

109. Recognising the potential burden these measures may place on industry, and the risk-based approach being taken, the Centre will continually review the risk environment to ensure the measures are targeted only at the highest risk assets. In the event the risk environment changes, Government will adjust the high-risk assets that the measures applies to and/or the reporting requirements of the ***Register***. As part of this process, the Centre will collaborate with relevant Commonwealth agencies, industry stakeholders and states and territories. The Centre will review the provided information, and the use of any directions, to ensure they have been targeted appropriately and are no more onerous than what was required to manage the risks.

110. The Centre is developing a website and associated ICT systems which will provide an online function for ***reporting entities*** to register their information. The online forms will be built in line with the Australian Government's Digital Service Standard, and meet the requirements of Web Content Accessibility Guidelines (WCAG) 2.0 web standard. This will be ready in time for the commencement of the legislation.