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 • Consideration of: o Costs of complying with the direction o Consequences to industry competition o Consequences to services or customers	Broad	The above scope AND, for example, directions that: • Limit offshore access to 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
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	
	Medium	$5,617	$17,717
	Large	$10,318	
Electricity transmission/ distribution	Small	$15,892	
	Medium	$49,739	$149,128
	Large	$83,496	
Gas processing/storage	Small	$10,662	
	Medium	$37,187	$116,284
	Large	$68,434	
Gas transmission/distribution	Small	$10,662	
	Medium	$37,187	$116,284
	Large	$68,434	
Ports	Small	$2,988	
	Medium	$10,749	$32,737
	Large	$19,001	
Water	Small	$6,343	
	Medium	$21,325	$64,855
	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	
	Medium	$2,950	$7,348
	Large	$2,839	
Electricity transmission/ distribution	Small	$3,609	
	Medium	$6,717	$16,708
	Large	$6,382	
Gas processing/storage	Small	$1,764	
	Medium	$3,327	$8,284
	Large	$3,193	
Gas transmission/distribution	Small	$2,994	
	Medium	$5,587	$13,900
	Large	$5,319	
Ports	Small	$1,969	
	Medium	$3,704	$9,220
	Large	$3,547	
Water	Small	$2,584	
	Medium	$4,833	$12,028
	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	
	Medium	$123,558	$348,825
	Large	$203,419	
Electricity transmission/ distribution	Small	$61,779	
	Medium	$363,141	$1,027,645
	Large	$602,725	
Gas processing/storage	Small	$25,841	
	Medium	$147,516	$416,707
	Large	$243,350	
Gas transmission/distribution	Small	$49,800	
	Medium	$291,266	$823,999
	Large	$482,933	
Ports	Small	$29,834	
	Medium	$171,475	$484,589
	Large	$283,280	
Water	Small	$41,814	
	Medium	$243,350	$688,235
	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	
	Medium	$21,374	$102,245
	Large	$78,149	
Electricity transmission/ distribution	Small	$190,186	
	Medium	$947,362	$3,029,896
	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 transmission/distribution	Small	$590,541
	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*				
Option 1: Maintain status quo	$0	$0	$0	$0
Option 2: Work with states/territories to strengthen existing regulatory mechanisms	Unable to be determined[1]	$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	$497,004	$0	$0	$497,004

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

Total average annual regulatory costs (from business as usual)				
Change in costs ($ million)	**Business**	**Community organisations**	**Individuals**	**Total change in costs**
certain matters and a low-level of safeguards are in place				
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 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.