Australian Government
Department of Home Affairs

# Parliamentary Inquiry into Security of Critical Infrastructure Bill 2017

Parliamentary Joint Committee on Intelligence and Security

# Table of Contents

# Introduction

1. The Department of Home Affairs (Home Affairs) welcomes the opportunity to make a submission to the Parliamentary Joint Committee on Intelligence and Security's Inquiry into the Security of Critical Infrastructure Bill 2017 (the Bill).
2. The Bill is designed to strengthen the Government's capacity to manage the national security risks of espionage, sabotage and coercion arising from foreign involvement in Australia's critical infrastructure.
3. Critical infrastructure underpins the functioning of Australia's society and economy and is integral to the prosperity of the nation. 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.
4. The Australian Government (the Government) welcomes foreign involvement in the economy and in Australia's infrastructure. 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. To ensure Australia remains competitive in attracting foreign investment it is important we maintain our reputation and credibility as an open and welcoming place to invest.
5. While recognising its many benefits, foreign involvement can greatly increase a malicious actor's ability to access and control Australia's critical infrastructure, in a way that is difficult to detect or attribute. Access and control can enable targeted activity which could disrupt the continuity of services to citizens, and result in extreme consequences for other dependent infrastructure or defence assets.
6. Recognising this, on 23 January 2017, the Government launched the Critical Infrastructure Centre (the Centre). The Centre was established to develop a deeper understanding of the national security risks across our highest-risk critical infrastructure sectors, and to develop and implement mitigation strategies. The Centre works collaboratively with industry and states and territories to ensure national security risks are being managed in a way that does not inhibit the ability of business to operate in a global economy.
7. The Bill supports the Centre's analysis, and ensures Government has the means to intervene when specific risks are identified, which cannot be managed through collaboration with operators or other existing regulatory mechanisms. More information about the Critical Infrastructure Centre is at Attachment A.

# Home Affairs and Critical Infrastructure

8. On 18 July 2017, the Prime Minister announced significant reforms to Australia's national security and intelligence arrangements, including Home Affairs and a Home Affairs Portfolio. These reforms were needed to preserve the operational focus and strengths of frontline agencies engaged in the fight against terrorism, organised crime and other domestic threats.
9. On 20 December 2017, the Home Affairs Portfolio, including Home Affairs, was formally established. Home Affairs is a central policy agency, providing coordinated strategy and policy leadership for Australia's national and transport security, federal law enforcement, criminal justice, cyber security, border, immigration, multicultural affairs, emergency management and trade-related functions.

10. Home Affairs includes the entirety of the former Department of Immigration and Border Protection. It also includes national security, emergency management and criminal justice functions from the Attorney-General's Department; the Office of Transport Security from the Department of Infrastructure and Regional Development; multicultural affairs from the Department of Social Services; and the counter-terrorism coordination and cyber security policy functions from the Department of the Prime Minister and Cabinet (PM&C).
11. The Centre, and responsibility for critical infrastructure security policy, now sits within Home Affairs.

# Why the need for regulation?

12. Most critical infrastructure in Australia is either privately owned and operated, or run on a commercial basis by government. The responsibility for ensuring the continuity of operations and the provision of essential services to the Australian economy and community is shared between owners and operators of critical infrastructure, state and territory governments and the Australian Government.
13. Owners and operators understand and manage many of the risks to the continuity of their operations as a core part of their businesses. However, the national security risks to critical infrastructure are complex and have evolved over recent years. Critical infrastructure assets are subject to rapid technological change with increased cyber connectivity, and they are increasingly reliant on global supply chains and the outsourcing and offshoring of key enabling services. These arrangements can greatly increase the opportunity for malicious foreign actors to undertake espionage, sabotage or coercion. For example:
    a. foreign intelligence services could target critical infrastructure assets for data that is not publicly available
    b. 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, and
    c. in extreme cases, a foreign actor could use access to critical infrastructure to apply coercive power against the Australian Government to influence decision-making or policy.

    While the more extreme examples of risk are unlikely, it is important to ensure the measures put in place now are flexible enough to respond to changes in the national security environment.
14. The Government’s ability to understand, manage and respond to national security risks is currently limited by existing gaps in the Government’s understanding of the ownership and control of critical infrastructure. It is also hampered by the lack of a mechanism at the federal level to intervene where a significant risk to national security has been identified.
15. The Bill provides a risk-based regulatory framework to manage national security risks from foreign involvement in Australia’s critical infrastructure. This risk-based approach focuses on Australia’s electricity, gas, water and ports sectors, where threats and vulnerabilities are high, and existing regulatory mechanisms may be insufficient or impractical to assess and manage specific risks.

# Key elements of the Bill

16. To allow the Government to better understand and manage national security risks in the highest risk critical infrastructure sectors, the Bill introduces three key measures:
    a. a Register of critical infrastructure assets
    b. an information gathering power, and

c. a ministerial directions power.

17. The Bill will regulate approximately 140 assets in the highest-risk sectors of electricity, gas, water and ports. 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.
18. The Register's obligations on reporting entities are intended to capture targeted information on critical infrastructure asset owners and operators, including ultimate beneficial ownership of critical infrastructure assets.
19. The information gathering power allows the Secretary of Home Affairs to request further information to complete a Register entry, conduct a risk assessment, or to inform whether a ministerial direction is required.
20. The Bill contains important safeguards for exercising the ministerial directions power. These safeguards will ensure that 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.
21. 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 for specific purposes (set out in Part 4, Division 3—Use and disclosure of protected information). The only criminal offence in the Bill relates to unauthorised disclosure of protected information obtained under this Bill.

## Why the electricity, gas, water and ports sectors?

22. The highest-risk sectors were determined by considering which critical infrastructure sectors were most at risk from sabotage, coercion and espionage by foreign actors, and where existing regulatory regimes may not support federal government direction.
23. Criticality within these sectors has been assessed from a national perspective. However, in some cases, that has included consideration of jurisdictional impact, where those impacts are significant (such as electricity generation). The Centre first considered which assets in each of the highest-risk sectors, if destroyed, degraded or rendered unavailable for an extended period would have a significant impact on large population hubs, the national economy, government operations and/or defence. The Centre also considered the availability of redundancies and existing mitigations as part of this analysis. Based on these criteria, the Critical Infrastructure Program for Modelling and Analysis (CIPMA) within the Centre provided analytical reports on the critical assets in each of the sectors, which are the foundations of the thresholds for each of the sectors in the Bill.
24. **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 protected.
25. **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. Manufacturing relies on gas for approximately 40 per cent of net energy requirements.
26. 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.

27. 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, supply chains for other critical infrastructure, and Defence purposes. Disruption to our most critical ports could have wide-reaching economic impacts.

28. The Bill will not apply to the telecommunications sector, which presents the highest level of risks of espionage, sabotage and coercion from foreign involvement. 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 manage risks in this sector.

29. While other critical infrastructure sectors, including banking and finance, health and aviation are at risk from espionage, sabotage and coercion, the level of existing regulation in place lowers their risk profile. The Centre will continue to work with these sectors through existing mechanisms including the Trusted Information Sharing Network (TISN) to improve their understanding of the threats of espionage, sabotage and coercion and to develop mitigation strategies.

## Register of Critical Infrastructure Assets

30. The Bill establishes a register of critical infrastructure assets, which will enhance the capability of the Government to understand who owns, controls, and has access to Australia's critical infrastructure. This Register will support more proactive management of the risks faced by assets in our highest-risk sectors.

31. The Bill will impose reporting requirements on two sets of entities: direct interest holders and responsible entities. Direct interest holders of a critical infrastructure asset will be required to provide interest and control information in respect of the asset. Some stakeholders have recently indicated that our definition of direct interest holder may not capture some entities that we intended it to (for example, entities whose subsidiaries hold an interest in the critical infrastructure asset). Home Affairs is working with the Office of Parliamentary Counsel to correct this through re-drafting to ensure that the policy intent to capture such ownership is clarified. Home Affairs appreciates the collaboration and feedback we continue to receive from stakeholders.

32. 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 information on operator and outsourcing arrangements. This information is essential to informing a deeper understanding of who has access to, control of, or the ability to influence, the critical infrastructure on which we all rely.

33. 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 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. Given the sensitivity of the information required to be provided and stored in aggregate, the Register will be held on a classified network. This will ensure that all information provided for the Register, including commercially sensitive information, is kept secure.

34. The reporting requirements have been designed to impose a minimal compliance burden on industry. Modelling prepared for the Centre concludes that the total once-off regulatory burden per captured critical asset owner/operator is $478.85, and then $88.39 per year for reporting changes in ownership and control information.

## Ministerial Directions Power

35. Part 3 of the Bill will enable the Minister to issue a direction to an owner or operator of a critical infrastructure asset to mitigate national security risks which cannot be managed through cooperation or existing regulatory mechanisms. It is modelled on a similar power in the TSSR. The ministerial directions power could be used to direct asset owners and operators to undertake, or refrain from, certain actions. Importantly, this power is limited to instances where:

    a. there is a risk identified which is prejudicial to security

    b. through collaboration, the owner or operator does not or cannot implement mitigations to address the risk, and

    c. there are no existing regulatory frameworks that can be used to enforce mitigations.

    In this way, it operates as a necessary safeguard to address national security risks where they cannot otherwise be managed.

36. The Bill includes a range of important safeguards for the ministerial directions power. Before a direction is able to be issued, the Minister will be required to be satisfied of certain matters, to consult with stakeholders, and to give consideration to a number of factors, including:

    a. giving primary consideration to a mandatory ASIO adverse security assessment

    b. being satisfied that the Government has negotiated in `good faith'

    c. consulting directly with, and considering any representations made by, the relevant First Minister and state or territory Minister and the entity to which the direction applies

    d. considering the costs to the entity and consequences to services in implementing the mitigation, and

    e. ensuring the direction is a proportionate response to the risk.

    The ministerial directions power is also subject to judicial review while the ASIO adverse security assessment will be subject to merits review.

37. While it is difficult to accurately cost the regulatory burden of the ministerial directions power, given it would depend on the direction given, we have been able to provide some guidance based on modelling of four different scenarios in each of the highest-risk sectors. The total annual estimated regulatory burden where a direction is issued once every three years is $8.12 million.

## Information gathering power

38. The information gathering power is designed to support the Centre's work in assessing and managing national security risks to Australia's critical infrastructure, but within the remit of the Bill's framework. The information gathering power is limited in the sense that the Secretary can use the power to obtain information in the following circumstances:

    a. to ensure that the Register information is correct and up to date

    b. to inform risk assessments, and

    c. to determine whether a ministerial direction should be made to mitigate a national security risk.

39. Information received in response to an information gathering notice will be protected information under the Act and can only be disclosed to certain persons and/or for restricted purposes (see Part 4, Division 3).

## Declaration of assets by the Minister

40. The Minister is vested with the power to privately declare a particular asset to be a critical infrastructure asset for the purposes of this Bill under section 51. The Minister's declaration power is necessary to ensure that the legislation can apply to those assets that do not meet the required thresholds to be captured under the Bill, but are critical for national security purposes and where there would be significant national security implications if that was known publicly. The Government will, however, inform the relevant First Minister of the state or territory in which the asset is located, that the asset has been declared to be a critical infrastructure asset for the purposes of the Bill.

# Interaction with other legislation

41. This Bill has been developed taking Australia's international trade law obligations into account. The Bill will apply to both Australian and foreign investors – the measures are not investor or country-specific and focus on national security risks related to critical infrastructure.
42. This Bill does not change Australia's foreign investment framework under the *Foreign Acquisitions and Takeovers Act 1975*.
43. As noted above, TSSR, which received Royal Assent on 18 September 2017, was designed to manage risks in the telecommunications sector. The extreme level of risk in this sector has required additional measures, not captured in the Bill. These include obligations on carriers and carriage service providers to do their best to protect networks and facilities from unauthorised access and interference, and notify the Government of proposed system and network changes. The Centre is implementing TSSR and working 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.
44. The National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017 complements the work of the Centre and the Bill, by strengthening existing espionage offences and introducing comprehensive new sabotage offences, which will enable the Government to prosecute malicious actors, including those that use critical infrastructure to engage in espionage and sabotage activities.

# Consultation

45. Recognising the significance of the reforms, the Government consulted widely over the course of 2017 to ensure the proposed measures were appropriately designed and targeted. The Government released an initial discussion paper following the establishment of the Centre in February. In March and June 2017, the Centre conducted separate rounds of consultations with officials from state and territory governments and industry to seek views on the proposed regulatory measures.
46. Consultations were undertaken with state and territory governments in the lead up to the 9 June COAG meeting, where the Commonwealth, 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.
47. 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 Government, consulted extensively with owners and operators, industry, law firms and investment advisers, and state and territory governments.

48. The Bill reflects the feedback received during these consultations. This includes refining key definitions, strengthening consultation requirements, and applying the legislation to specific critical assets in the gas sector. The desire from some stakeholders to include the gas sector was raised during consultations and its addition, including the proposed thresholds, was advised to stakeholders in November 2017.
49. Gas plays the most versatile role in the energy network, and the security and reliability of the electricity sector is reliant on gas supply. Gas, in particular, is relied upon to correct unstable networks and respond to periods of high demand. The application of this legislation to the gas sector will enable the Government to continue to work closely with industry, states and territories to ensure the ongoing security of our gas systems and networks.
50. The Centre acknowledges that the gas sector has had less time than other sectors to comment on the development of the Bill. Home Affairs considers the reference of the Bill to the Committee as a further opportunity for stakeholders to engage on this particular issue (as well as others), and welcomes ongoing engagement on the Bill.

# Implementation

51. Home Affairs through the Centre will be responsible for implementing the Bill once passed, along with TSSR. The Centre will continue to work collaboratively with states, territories and industry to undertake risk assessments on critical assets, and, where appropriate and with further consultation, consider and develop any mitigations that need to be put in place to address the risk.

# Conclusion

52. This Bill aligns with the Government's clear intention to continue to cooperate and collaborate with all levels of government, regulators, owners and operators of critical infrastructure. It strikes an appropriate regulatory balance by acknowledging the shared responsibility for managing national security risks, while empowering the Government to intervene to mitigate a risk where existing regimes cannot be used.
53. While maintaining competitiveness in a rapidly changing global market is essential, with this Bill, the Government is taking the steps necessary to strengthen the security and resilience of Australia's critical infrastructure.

# Attachment A

## Critical Infrastructure Centre

Australia's Critical Infrastructure Resilience 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 influence their operating environments to the extent required to ensure the continuity of essential services.

While Australian intelligence agencies have a well-developed understanding of the security threats and vulnerabilities, the expertise of industry and state and territory governments who own, operate and regulate our critical infrastructure, is essential to better understand existing risk management controls, and to develop mitigation strategies which leverage existing regimes where possible.

That is why the Australian Government established the Critical Infrastructure Centre (the Centre) to manage the complex and evolving national security risks from foreign involvement in Australia's critical infrastructure. The Centre, located in Home Affairs, brings together expertise and capability from across the Australian Government.

The Centre focuses on the potential for malicious actors to gain access and control to Australia's critical infrastructure, through ownership, offshoring, outsourcing and supply chain arrangements. The Centre collaborates with owners and operators and state and territory regulators to identify risks and develop and implement asset-specific mitigation strategies and sector-wide best practice guidelines.

Reflecting telecommunications' status as the highest risk sector, the Centre administers the Telecommunications and Other Legislation Amendment Act 2017, which will place new security obligations on carriers and carriage service providers.

The Centre complements and supports initiatives under Australia's Cyber Security Strategy, which aims to boost partnerships with critical infrastructure owners and operators, raise awareness and understanding of cyber security issues and promote strong cyber defences of Australia's networks and systems.

Through CERT Australia, the Government is also working closely with industry to mitigate cyber risks, including through the establishment of the Joint Cyber Security Centres (JCSC).

The Trusted Information Sharing Network (TISN) for critical infrastructure resilience is located within the Centre and is a key mechanism for engaging with industry. For many years, the Government has worked in partnership with industry through the TISN, to build critical infrastructure resilience in the face of all hazards (for example, natural disasters, cyber security, terrorism and negligence).

The Government will continue to engage with industry through the TISN, to share information and resilience building initiatives, including communicating any messages from the Centre.