QUESTION TAKEN ON NOTICE

Parliamentary Inquiry : 09 February 2018

HOME AFFAIRS PORTFOLIO

(*SOCI/001*) – PJCIS - Security of Critical Infrastructure - 1. The Committee sought advice on what other legal or regulatory mechanisms could be used to mitigate risks, prior to the Ministerial Directions Power being used -

Asked:

The Committee sought advice on what other legal or regulatory mechanisms could be used to mitigate risks, prior to the Ministerial Directions Power being used.

Answer:
The Critical Infrastructure Centre was established to better understand and manage the complex and evolving national security risks from foreign involvement in Australia's critical infrastructure. A key mechanism the Centre uses to do this is conducting national security risk assessments.

Depending on the outcome of a risk assessment, the Centre may recommend controls to mitigate risks to an asset. Such mitigations will be developed and implemented through consultation and cooperation, or by leveraging existing regulatory mechanisms wherever possible.

The Centre will also utilise non-regulatory mechanisms to mitigate risks, where possible. These will include providing best practice guidance to industry, through factsheets and sector-wide advice. This guidance will help asset owners and operators make their own national security risk decisions.

The regulatory environment for the identified sectors is multi-layered and varies across each jurisdiction. As part of the consultation process that will occur prior to a direction being issued, the Centre will work closely with the asset operator and both Commonwealth and state or territory regulators to gain a detailed understanding of:

1. the existing regulatory environment in which the asset operates, and
2. whether the mitigations could be implemented by leveraging existing regulatory mechanisms.

QUESTION TAKEN ON NOTICE

Parliamentary Inquiry : 09 February 2018

HOME AFFAIRS PORTFOLIO

(*SOCI/002*) – PJCIS - Security of Critical Infrastructure - 2: The Committee sought information on the timeline and endpoint for ensuring whole-of-government coordination on the information required of industry, so as to minimise duplication. -

Asked:

The Committee sought information on the timeline and endpoint for ensuring whole-of-government coordination on the information required of industry, so as to minimise duplication.

Answer:
A key role of the Critical Infrastructure Centre is to ensure that Government takes a coordinated approach to managing the national security risks from foreign involvement in our critical infrastructure. This is the very reason for the establishment of the Centre in January 2017.

To give effect to this, the multi-agency, multi-disciplinary Centre hosts staff from a range of Commonwealth agencies including ASIO, Treasury, Defence, Department of Foreign Affairs and Trade, Department of the Environment and Energy, and Austrade. The Centre also has a seconded staff member from the Independent Pricing and Regulatory Tribunal (IPART), the NSW regulator, and is working with industry to identify other regulator and industry secondments.

The Centre also engages directly with the existing Trusted Information Sharing Network for Critical Infrastructure Resilience (TISN), and Australian Cyber Security Centre (ACSC) to provide advice, gain industry input, and ensure alignment of its work with the broader Strategy for Critical Infrastructure Resilience.

The transition of the Centre into the newly formed Department of Home Affairs provides further opportunities to minimise duplication for industry in engaging with Government. Home Affairs brings the Department of Immigration and Border Protection together with security, law enforcement and national security policy, critical infrastructure and emergency management from the Attorney-General's Department, counter-terrorism and cyber security policy from the Department of the Prime Minister and Cabinet, multicultural affairs from the Department of Social Services and the Office of Transport Security from the Department of Infrastructure and Regional Development.

The Home Affairs portfolio provides central coordinated strategy and policy leadership for national security, including critical infrastructure resilience. It also

provides an opportunity to develop a critical infrastructure centre of expertise and remove duplicate areas for engagement for industry. In a world of changing and evolving threats the new Department enhances our nation's ability to respond to foreign interference and cyber intrusions and streamline government's engagement with industry on a range of national security related matters.

QUESTION TAKEN ON NOTICE

Parliamentary Inquiry : 09 February 2018

HOME AFFAIRS PORTFOLIO

(*SOCI/003*) – PJCIS - Security of Critical Infrastructure - 3: The Committee sought the Centre's response to legislative issues raised in submissions to the Inquiry. -

Asked:

The Committee sought the Centre's response to legislative issues raised in submissions to the Inquiry.

Answer:
Issues related to 'direct interest holder'

Issues were raised with the term 'direct interest holder' and its interaction with other provisions in the legislation.

To address these concerns, the department will seek to clarify that a 'direct interest holder' under section 8 is limited to the immediate shareholder or interest holder and does not extend to any intermediate or ultimate holding entities. Information relating to these intermediate or ultimate holding entities is still a key component of the register, but is required to be reported by the 'direct interest holder' as a result of paragraph 6(1)(h) of the definition of 'interest and control information'. This paragraph requires information to be provided in relation to any other entity that is in a position to influence or control the direct interest holder.

To provide further clarity on the interaction between the term 'direct interest holder' and other entities in a position to exercise influence and control, the department will look to introduce a definition of 'influence and control' drawing on the guidance already included in the explanatory memorandum (paragraph 150). In addition to the guidance in the explanatory memorandum, to provide even greater certainty, the department would look to include a specific percentage of 10% that would amount to the ability to influence and control. This would be combined with a tracing power designed to ensure that the direct interest holder reports relevant interests up an ownership chain, and not just their own immediate interest holder. The department would also make the necessary adjustments to the explanatory memorandum to align with these amendments.

The department will also clarify that a 'direct interest holder' includes, but is not exclusive to, those entities listed in subclause 8(2).

Moneylending agreements

The Law Council of Australia raised concerns that the current definition of interest and control may capture certain money-lending agreements in which financiers have a certain level of influence or control over the asset.

It is not the intention of the legislation to capture money lenders where their interest in the asset is through a financing arrangement with the true 'direct interest holder' and as a result are not in a position to exercise any influence or control. To address these circumstances, we will look to provide a carve-out modelled on regulation 27 of the Foreign Acquisitions and Takeovers Regulation 2015. However, the form of the carve-out may vary from that in the *Foreign Acquisitions and Takeovers Act 1975*, given the different purposes of the two Acts.

The Bill should be consistent with the Australian Privacy Principles.

The provisions in the Bill have been developed to be consistent with the Australian Privacy Principles (APPs). The department will consider amendments to the explanatory memorandum to clarify that the Centre in administering the legislation will comply with all relevant Australian Privacy Principles.

Retrospective use of the Ministerial Power

The Law Council of Australia expressed concerns that a ministerial direction may impact on existing arrangements with the Commonwealth, states or territories on how the asset is operated and regulated. As part of considering any mitigations during the collaborative risk assessment process, the department would work closely with, and consult all relevant agencies to ensure that mitigations or a specific direction do not conflict with existing arrangements. This would include existing state or territory licensing arrangements or any conditions imposed as a result of foreign investment approval.

The term 'prejudicial to security' should be defined in the legislation itself

As outlined by the Attorney-General's Department in its supplementary submission to the Committee in its consideration of the Telecommunications and Other Legislation Amendment Bill 2016, it would not be appropriate to introduce a definition of the phrase 'prejudicial to security'. The Department of Home Affairs continues to support that view in the context of the Security of Critical Infrastructure Bill 2017. Defining the phrase 'prejudicial to security' may result in the phrase being given inconsistent meanings between different national security legislative frameworks, thereby causing unintended operational consequences.

'Security' is already defined in the legislation as having the same meaning as in the ASIO Act. What is 'prejudicial to security' will be interpreted using the ordinary rules of statutory interpretation. That is, the words 'prejudicial to' as used in the Bill will have their 'ordinary meaning' (as described in a dictionary). The words are not intended to have a special or restricted meaning (and thus do not require a definition).

Use of the directions power should

The Centre notes the concerns put forward by Law Council of Australia regarding the use of the directions power.

We consider that the provision as drafted, including the requirement for an ASIO adverse security assessment already ensures that the Minister's directions power is properly limited to circumstances where there is a sufficient level of risk.

Notwithstanding, the department is open to considering ideas for further clarifying the intended limited scope of the directions power including the concept of 'substantial risk'.

However, including a temporal element to the test may unnecessarily limit the use of the power given the Bill is designed to enable action to be taken to prevent pre-positioning for acts of sabotage.
In these circumstances, it may not be possible to satisfy an 'imminence' test. Additionally, the requirement of 'unauthorised' access or interference may be difficult to satisfy in circumstances where the risk arises through legitimate involvement in the critical infrastructure asset, for example, through direct ownership or legitimate business activities.

Consequential amendments to the ASIO Act – based on advice in the Inspector-General of Intelligence and Security's (IGIS) submission

The Centre has discussed the issue raised by the IGIS directly with her office. It was always the intention that an unclassified statement of the grounds for the adverse security assessment, which is included in the assessment, be provided to the affected critical asset owner or operator to assist them in understanding the security concern and need for a Ministerial direction. With the Bill as currently drafted, it would be open for the Attorney-General to withhold the notice on national security grounds. This was never the Department's intent.

To address the concern, the Department will look to amend the Security of Critical Infrastructure (Consequential and Transitional Provisions) Bill 2017 to ensure that the directions power under subsection 32(2) of the Security of Critical Infrastructure Bill 2017 is included in section 38A, rather than section 38, of the *Australian Security Intelligence Organisation Act 1979*.