Australian Government
Attorney-General's Department

March 2017

Telecommunications and Other Legislation Amendment Bill 2016

Attorney-General's Department's response to Questions on Notice

This document responds to written questions received from the Parliamentary Joint Committee on Intelligence and Security Secretariat on 22 February 2017.

General

1. **How is the Department planning to work with industry during the 12 month implementation period? i.e. Through what mechanism is this consultation with industry likely to occur?**

ANSWER:

The newly established multi-agency Critical Infrastructure Centre, housed in the Attorney-General's Department (Department), will work with industry on implementation of the reforms. The Centre was established in response to the complex and evolving national security risks to critical infrastructure, and recognises that appropriate risk mitigation strategies are best developed in partnership with businesses. The Centre brings together expertise and capability from across the Australian Government, including the Australian Security Intelligence Organisation (ASIO) and the Department of Communications and the Arts, into a single location to enable more active engagement with industry to better manage the national security risks to Australia's critical infrastructure.

The Centre will work with industry during the 12 month implementation period to ensure guidance material, including the Administrative Guidelines, provides industry with the information it needs to implement the reforms. The Centre intends to use existing fora, such as the Communications Sector Group of the Trusted Information Sharing Network for Critical Infrastructure Resilience and other fora, to reach out to industry for this purpose. This group engagement will take place in parallel with bilateral engagement with carriers and carriage service providers (C/CSPs), which will continue throughout the implementation period.

Regulatory framework and performance

2. **Industry suggests the Bill should include information about the Attorney-General Department's role as regulator and, specifically, whether Government's Regulator Performance Framework will apply to the framework. A key concern of industry appears to be the transparency and accountability of regulatory arrangements (Optus: p6, para 4.1, 4.2):**
    - **Would Government's Regulator Performance Framework apply to the reforms?**
    - **If not, how will the Department ensure the regulatory arrangements are transparent and accountable?**

ANSWER:

The issue of whether the Government's Regulator Performance Framework applies is complex given the national security considerations. The Department is seeking advice on the application of the Framework but is committed to transparent reporting to the extent possible under these circumstances.

Section 315J of the Bill requires the Secretary of the Department to report on the operation of the reforms and for the Attorney-General to table that report in Parliament. While the Bill does not

specify what the report must contain, the report could include information such as the number of notifications received, the Communications Access Co-ordinator's average response timeframes and the number of occasions on which the information-gathering power has been exercised.

The Department notes the other measures in the Bill which ensure decisions of Government to implement the reforms are transparent and accountable. These include:

- prior to directing a C/CSP to do or not do a specified thing, the Attorney-General must:
  - give the C/CSP a written note setting out the proposed direction and given the C/CSP at least 28 days to respond (unless urgent circumstances apply)
  - be satisfied that the C/CSP and government have negotiated in good faith to achieve an outcome to eliminate or reduce the identified risk, and
  - have regard to matters including the costs likely to be incurred by the C/CSP, the consequences on competition and customers
- the Attorney-General must consult with the Minister for Communications (and the Prime Minister if the direction is to cease a service) prior to directing a C/CSP and give the Australian Communications and Media Authority (ACMA) a copy of any direction
- the Attorney-General's directions powers to do or not do a specified thing can only be used after an adverse security assessment in respect of the C/CSP has been given to him or her by ASIO. Assessments are subject to merits review and information sharing requirements (see ss38A(2) and 54(1) of the *Australian Security Intelligence Organisation Act 197*9 (ASIO Act)),
- section 38A of the ASIO Act requires that the relevant carrier, carriage service provider or carriage service intermediary be given written notice of the assessment, and a copy of that assessment including an unclassified statement of grounds. Providers will be able to seek merits review of an adverse security assessment in the Administrative Appeals Tribunal, and
- C/CSPs that are subject to a direction from the Attorney-General can seek review under the *Administrative Decisions (Judicial Review) Act 1977* (ADJR Act).

3. Industry suggests that, if the statutory timeframe requirements for the Communications Access Co-ordinator responding to notifications and security capability plans are not met, then the notification or security capability plan should be deemed as 'agreed', unless a formal notice is provided by the Communications Access Co-ordinator of an extended assessment period (Optus: p7, para 4.3, 4.4):

- **What is your view on this proposal?**
- **Would you be opposed to the Bill or Explanatory Memorandum specifying what would happen in circumstances where the Communications Access Co-ordinator does not respond within the specified time period?**

ANSWER:

A provision that deemed notifications or security capability plans to be 'agreed' where the Communications Access Co-ordinator does not meet prescribed timeframes would not be appropriate or effective within the framework established by the Bill. The Communications Access Co-ordinator does not have any role in agreeing to (or rejecting) notifications or security capability

plans. The purpose of the notifications and security capability plans and the role of the Communications Access Co-ordinator is to enable early engagement and advice on changes that create a risk of unauthorised interference with, or unauthorised access to, telecommunications networks or facilities and to enable appropriate risk mitigation strategies to be implemented.

In the unlikely event the Communications Access Co-ordinator does not respond to a notification or security capability plan within the prescribed timeframe, this would be a factor the Attorney-General would need to consider before exercising the direction under s315B. The Attorney-General is required to consider if all attempts to negotiate in good faith with the C/CSP had occurred before issuing this direction.

The Department is open to amending the Explanatory Memorandum to specify that, if the Communications Access Co-ordinator does not respond within the prescribed timeframe (to the relevant notification or security capability plan), the Attorney-General must take account of this as part of his or her assessment of whether negotiations with the carrier or nominated carriage service provider (C/NCSP) had been carried out in good faith.

Protecting disclosure of personal information

4. **The Office of the Australian Information Commissioner notes that section 315H(2) restricts the disclosure of 'identifying information' to a person who is not a Commonwealth officer. They note that identifying information 'means information that identifies the C/CSP or intermediary concerned'. They suggest, as an additional protection, that this restriction on the disclosure of 'identifying information' is extended beyond commercial information to apply to 'personal information' as defined in the Privacy Act (p2, last para).**
    - **Do you have any concerns with this proposal?**

ANSWER:

Extending subsection 315H(2) to 'personal information' is unnecessary as there are already strong protections in place for the protection of personal information.

The Attorney-General's Department, the Department of Communications and the Arts and other government departments, are subject to the *Privacy Act 1988*, which sets out how personal information is handled. ASIO's handling of personal information is governed by the ASIO Act and the Attorney-General's Guidelines (made under the Act) and is also subject to the oversight of the Inspector-General of Intelligence and Security.

Section 315H of the Bill is intended to cover other information, such as commercially sensitive information, that would not necessarily be captured under existing personal information protections (e.g. company names).

Security Obligation – Scope and Application

5. **Industry is particularly concerned by the terminology of the security obligation to protect networks and facilities owned, operated and <u>used by</u> the carrier or carriage service provider from unauthorised access and interference. Industry has sought clarification about the sorts of measures that could be put in place to demonstrate compliance with this obligation (Industry Associations p13, para 3.3):**
    - **What can be done to give industry further clarity about how they can demonstrate compliance with this part of the security obligation to protect networks and facilities?**
    - **How would the best efforts test be applied in circumstances where infrastructure is 'used', but not necessarily owned or operated by a C/CSP?**

ANSWER:

The security obligation is framed in terms of the C/CSP doing 'its best' to protect networks and facilities it uses in connection with its operation of telecommunications networks or facilities or its supply of carriage services. This does not impose an absolute obligation, rather it requires C/CSPs to take all reasonable steps to prevent unauthorised access and interference. The obligation to protect networks and facilities 'used' by a C/CSP reflects the interconnected nature of telecommunications networks and services. A C/CSP using the facilities or networks of another provider to deliver its service may give that provider access to sensitive information, such as customer billing information, or core parts of that C/CSP's network, and the C/CSP's staff may have access to the networks and facilities of the other provider.

C/CSPs would be expected to be capable of demonstrating that, as far as is reasonable, they have processes and arrangements in place to manage who can access systems, networks and facilities. This could include the C/CSP maintaining reasonable supervision and oversight of any access by its employees to networks or facilities it is using, or seeking assurances from another provider whose network or facilities it is using about the security applied by that other provider. The relationship between a Mobile Virtual Network Operator (MVNO) and a carrier, where the MVNO's 'uses' the carrier's networks and facilities, serves as a useful example. In this example, the security obligation requires the MVNO to protect its own store of customer information from unauthorised access and interference, in addition to ensuring the carrier is similarly protecting its customers' information and telephony services. This can be achieved through commercial contracts. The Department understands the actions that need to be taken by C/CSPs to comply with their security obligations will differ, depending on their level of involvement in provision of different services.

The Bill already differentiates between ownership and operation of networks and facilities on the one hand, and use on the other. Subsection 313(1B) clarifies that the obligation to maintain competent supervision of, and effective control over, telecommunications networks and facilities applies to networks and facilities owned or operated by the C/CSP.

The Bill does not specify or prescribe what solutions must be used to secure networks or facilities. This approach is intended to provide flexibility to industry, acknowledging that the approach adopted by individual C/CSPs will depend upon the risk factors specific to that provider.

The department will engage with industry to assist them to identify risks and mitigation measures. This process will provide clarity for industry on specific risks as they are identified.

6. **Industry has raised a concern that, if a company has infrastructure located in a foreign country, it may be difficult for them to demonstrate that they are meeting the security obligation if a foreign intelligence service in that country is able to make access requests in accordance with the domestic laws of that country. Industry has asked whether having 'an ability to log, within Australia, any lawful access requests made to Australian systems offshore would be sufficient to fulfil their obligations set out in the Bill (Industry Associations: pages 13 and 14, para 3.4):**
    - **What is your view on the proposal that industry log any lawful access requests made to Australian systems?**
    - **Should this be a requirement set out in the Bill? If not, why not?**
    - **What else can be done to give industry further clarity about how they can demonstrate compliance with the security obligation in circumstances where all or part of their network/facilities is located off-shore?**
    - **Would the Department be comfortable for these concerns to be addressed through amendments to the Explanatory Memorandum and Administrative Guidelines to clarify whether C/CSPs would be in breach of the security obligation (section 313) if they acted in accordance with an applicable law of a foreign country?**

ANSWER:

The security obligation requires a C/CSP to do its best to protect networks and facilities from unauthorised interference or unauthorised access. The Bill does not prohibit C/CSPs from offshoring parts of their networks or facilities. However, where a C/CSP does elect to offshore part of its network or facilities, the level and nature of risks associated with that decision, and the available mitigation strategies, will depend on a range of factors, including the applicability of foreign laws.

While it may be desirable for industry to log lawful access requests made to Australian systems, depending on the laws of the relevant foreign country, imposing a statutory requirement for C/CSPs to provide Australian Government officials with details about foreign lawful telecommunications access requests may create a conflict of laws issue for the relevant industry member. Accordingly, the Bill does not require C/CSPs to retain logs of lawful access requests made to Australian systems located offshore.

Early engagement between C/CSPs and Government in situations where C/CSPs are considering offshoring parts of their networks or facilities is the appropriate mechanism for industry to obtain clarity about meeting their obligations. This will enable risks and potential mitigation strategies to be identified, including what mechanisms industry can put in place to demonstrate compliance. The Administrative Guidelines could also be updated with examples of how demonstrating appropriate supervision and control can be achieved. The Guidelines are more appropriate than the Explanatory Memorandum as they are a living document that can be updated from time to time as examples of how compliance can be demonstrated evolve.

7. **Industry suggests that the term 'facilities' needs to be clarified. Specifically, they seek to better understand the application of the Bill to cloud computing as the existing definition of the term 'facility' in the *Telecommunications Act 1997* does not currently include any reference to cloud computing (Industry Associations: p16 and 17, para 3.9):**
    - **Will cloud computing be subject to the obligations set out in the Bill?**
    - **To address this, would it be most appropriate for further guidance to be set out in the Bill, Explanatory Memorandum or administrative guidelines?**

ANSWER:

Cloud computing is a concept used to describe the ability to access information or services (stored remotely) via the internet. Cloud computing is reliant on telecommunications networks, infrastructure and facilities (terms already defined in legislation) for its operation.

C/CSPs that use or offer cloud computing services or infrastructure are required to take all reasonable steps to prevent unauthorised access and interference for the purpose of protecting the confidentiality of information stored 'in the cloud' and the availability and integrity of networks and services. The Administrative Guidelines reference the Australian Signals Directorate's Information Security Advice, Cloud Computing Security Considerations, as a helpful guide for businesses wanting to know more about how to perform risk assessments of cloud computing services, and use these services securely.

Given the dynamic natures of both the telecommunications and national security environments, the Department considers the Administrative Guidelines to be the most appropriate place to detail examples specific to cloud computing. This can be further developed, in consultation with industry, prior to commencement.

8. **Foxtel is concerned that the scope of the Bill is broad and unclear in relation to its application to infrastructure and facilities used to supply broadcasting and content services. They have suggested the Explanatory Memorandum and administrative guidelines be amended to clarify that where infrastructure and facilities are used solely or principally for the supply of broadcasting services, it is not intended to be subject to the proposed reforms (Foxtel: p4):**
    - **Do you see any problems with this suggestion?**

ANSWER:

The *Telecommunications Act 1997* exempts a broadcaster from being treated as a CSP where the sole or principal use of its carriage service is to supply (a) broadcasting services to the public, or (b) secondary carriage service by means of the main carrier signal of a broadcaster. In these circumstances, the broadcaster is not subject to the reforms set out in the Bill.

The Department understands that Foxtel owns and operates telecommunications infrastructure that supplies communication services other than broadcasting. Where a broadcaster owns, operates or uses telecommunications networks and facilities and is not exempted, the broadcaster is required to meet the security obligation set out in the Bill. This is appropriate as the aim of the reforms is to

protect telecommunications networks and facilities. The Department notes that only C/NCSPs are subject to the notification requirements.

Notification Requirement

9. **Industry has asked that the kinds of changes and circumstances in which industry must notify Government of changes to their networks should be set out in the Bill as an 'exhaustive' list. They claim the existing terminology is so broad that they will be required to notify about 'just about anything' in the course of normal network and system management (Industry Associations: p14, para 3.5):**
    - **Why is the existing list of notifiable equipment in subsection 314A(2) so broad and is there any reason it cannot be more specific?**

ANSWER:

Given the dynamic nature of both the telecommunications and national security environments, the Department considers it is not prudent to set out in legislation technical descriptions that are specific to a particular point in time. This could render the reforms set out in the legislation redundant in the near future.

The Department considers it is more appropriate to continue to detail examples in the Administrative Guidelines to support an evolving understanding of the risk environment between Government and industry. The Department has committed to developing the Guidelines further, in consultation with industry.

A number of examples of changes likely to trigger the notification requirement are currently set out in the Administrative Guidelines. However, the Department acknowledges industry members' need for more clarity on operation of the reforms, specifically regarding changes where it is envisaged they won't need to notify the Communications Access Co-ordinator.

Accordingly, the Department has provided below a list of changes it envisages industry will not be required to notify the Communications Access Co-ordinator of, either because they do not meet the notification threshold or due to them being exempted from the requirement:

- Day to day changes, such as routing changes or software updates, which do not materially change the C/NCSP's effective control or competent supervision arrangements.
- Emergency changes, such as when a C/NCSP needs to make an urgent change to maintain the availability of the network, one that cannot be delayed to allow for the notification process.
- Testing or trials for C/NCSP testing that is not connected to the Australian telecommunications network, where protections are applied to customer data.
- Specific business changes that do not impact a C/NCSP's ownership, effective control or competent supervision. This may include replacing existing equipment with equipment of the same make and same (or similar) model.

Further examples of changes that may be exempted from the notification requirement will be canvassed with industry during the implementation phase. C/CSPs wishing to discuss whether a change requires notification will also have the option of contacting the Department.

10. Industry seeks that an adverse security assessment should be a requirement for a notification (in addition to being a requirement of a direction) (Industry Associations: p15, para 3.6):

- **Is there any specific reason why the notification requirement is currently not subject to an adverse security assessment?**

ANSWER:

Requiring an adverse security assessment as a precondition for the notification requirement would significantly undermine the effectiveness of the reforms. It would require ASIO to provide an adverse security assessment on a proposed change without being notified or informed of that change in order to trigger the notification requirement. It is not possible for ASIO to provide an adverse security assessment relevant to a provider, without knowledge of that provider's networks, facilities, services and any proposed changes. The purpose of the reforms is to ensure early engagement between industry and Government to identify, and appropriately mitigate, risks to telecommunications networks and facilities.

11. Foxtel has suggested the Bill be amended to provide a legislative framework around the exemptions process, including criteria for exemptions and timeframes. Page 28 of the administrative guidelines contains the sorts of things that would be taken into account when making a decision about whether or not to provide an exemption (e.g. market share, sensitivity of the customer base etc.) (Foxtel: p3):

- **Is there a reason why there is no application process for exemptions?**
- **Is there any reason why the criterion currently set out at the top of page 28 of the administrative guidelines is not included in the Bill?**
- **Is there any reason why the ability of the Communications Access Co-ordinator to vary or revoke the exemption is not made explicit in the Bill?**
- **Within what timeframe following enactment is industry likely to be advised if they are exempt from the notification requirement?**
- **Is there any reason why these timeframes for exemptions should not made more explicit in the Bill?**

ANSWER:

The reforms set out in the Bill focus on building effective partnerships between industry and Government to identify, and appropriately mitigate, risks to telecommunications networks and facilities. They differ from other obligations set out in the *Telecommunications (Interception and Access) Act 1979* in that they are not focussed on the existence of a service-level capability. Accordingly, a framework requiring the Communications Access Co-ordinator to "approve" or "not approve" a C/NCSP's application is not appropriate.

It is envisaged that exemptions granted under the reforms will mostly focus on exempting a C/NCSP from notifying the Communications Access Co-ordinator of certain types of changes or changes

involving a particular business unit, rather than a blanket exemption applicable to that C/NCSP's entire operations. The Department has provided some examples of changes it envisages may not be subject to the notification requirement (including those subject to an exemption) in its answer to Question 9, above. Given the focus of the reforms is to ensure national security considerations are taken into account early in a C/CSP's planning phase, it makes sense to keep the communication lines between industry and Government open.

However, noting industry's concerns, the Department is open to amending the Bill to include an exemption application process.

12. Foxtel notes there is no detailed legislative framework or criteria if the Minister wishes to declare a carriage service provider a 'nominated carriage service provider' under section 197(4) of the *Telecommunications (Interception and Access) Act 1979,* which triggers the notification requirement in section 314(A). They argue this does not provide sufficient certainty regarding the future application of the proposed reforms and they suggest there should be a legislative framework or criteria to declare a carriage service provider a 'nominated carriage service provider' under the Act (Foxtel: p3, first para):

- **Do you have any comments?**

ANSWER:

The ability for the Attorney-General to nominate a CSP already exists in the *Telecommunications (Interception and Access) Act 1979*.

Nominations are made following consultation with law enforcement and intelligence agencies and based on maintaining the ability of those agencies to undertake national security operations or law enforcement investigations into serious offences. The CSP would be consulted on any proposed recommendation for nomination and the Department would consider the broader impact on the CSP (including increased regulatory burden). A CSP would not be nominated without its knowledge.

Directions Powers

13. Industry suggests that in order to ensure directions are only issued when absolutely required, the Bill should make explicit that they can only be issued when the 'risk of unauthorised access and interference is specified as substantial and imminent' (Industry Associations: p17, second last para):

- **Do you have any comments? Please make it clear if you see any risks with this proposal.**

ANSWER:

This proposal would undermine the purpose of the reforms, which is to encourage industry to engage early with Government to ensure any potential national security risks are appropriately mitigated before they become substantial and imminent. The Attorney-General would only issue a direction under s315B where he or she is satisfied there is a risk that would be 'prejudicial to security' and the direction is reasonably necessary to eliminate or reduce that risk.

The Explanatory Memorandum makes clear that the Attorney-General's power to direct a C/CSP to do or not do a thing or act is only to be used as a 'measure of last resort' where all efforts to reach

agreement cooperatively have failed. The Bill also contains a requirement for the Attorney-General to be satisfied that reasonable steps have been taken to negotiate in good faith prior to this direction being issued to a C/CSP.

In addition, the Bill addresses the risk of arbitrary exercise of this power by requiring an adverse security assessment from the ASIO and for the Attorney-General to consult with the Minister for Communications and consider a range of matters from the perspective of the telecommunications industry, prior to a direction being issued. The Attorney-General also must provide the ACMA with a copy of any direction issued to a C/CSP.

These measures ensure that impacts on the C/CSP, end user, market and economy more broadly are considered before a direction under s315B is issued.

14. Industry suggests the meaning of 'prejudicial to security' should be defined in legislation rather than the Explanatory Memorandum (the existing meaning of this term is outlined in para 178 of the Explanatory Memorandum) (Industry Associations p17, para 3 and 4):

ANSWER:

The Department does not support amending the Bill to introduce a definition of the phrase 'prejudicial to security', as doing so may result in the phrase being given inconsistent meanings between different national security legislative frameworks, thereby causing unintended operational consequences.

The Bill specifies that the term 'security' has the same meaning as in the ASIO Act. The Department considers that the phrase 'prejudicial to security' is readily understood and does not require further definition. 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 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) and this approach is currently reflected in the Attorney-General's Guidelines.

The phrase 'prejudicial to security' is not defined in other Acts that reference it. Defining the phrase in the Bill could produce inconsistency between core national security legal frameworks.

Adverse Security Assessments

15. Industry seeks increased transparency of the adverse security assessment and the criteria used by ASIO to make an assessment (Industry Associations p17, 5th para):

- **Can the criteria for the adverse security assessment be made publicly available?**

ANSWER:

There are no 'standard criteria' for the making of an adverse security assessment by ASIO. Each security assessment will be based on:

- the individual facts and circumstances of the telecommunications service, network or facilities in question; and

- the nature and degree of the assessed risk to security arising from the use of, or unauthorised interference with or access to, the service, network or facilities in light of those facts and circumstances.

It would not be appropriate to make public the criteria for an adverse security assessment in this context. More broadly, the Department would not support making public detailed information about how ASIO assesses risks to security. Making such information public may enable foreign intelligence services, and others seeking to harm Australia's security, to plan and carry out their activities in a manner designed to go undetected by ASIO.

However, when ASIO does provide an adverse security assessment to the Attorney-General (in connection with ss 315A or 315B of the Bill) section 38A of the ASIO Act requires that the relevant carrier, carriage service provider or carriage service intermediary be given written notice of the assessment, and a copy of that assessment including an unclassified statement of grounds. Providers will be able to seek merits review of an adverse security assessment in the Administrative Appeals Tribunal. In this way, the making of the adverse security assessment and the grounds for that assessment are transparent and ASIO is accountable for them.

Retrofitting of existing systems

16. Industry has raised concerns (Industry Associations: p18, para 3.10; and Macquarie Telecom: 3rd page) about the possible retrofitting of existing systems to meet the security obligation. Industry suggests the Bill makes explicit the intention to:

(1) not require retrofits except in rare and extremely serious circumstances, and

(2) for a sunset clause to be included on the ability to issue a direction for network retrofit:

- **What is your view on these proposals?**
- **Do you see any risks in what is being proposed?**

ANSWER:

C/CSPs are not expected to retrofit existing systems on commencement of this security obligation. However, there may be very rare cases where a significant security vulnerability is found in an existing system that could facilitate acts of espionage, sabotage and foreign interference. In such cases, government agencies will work with the C/CSP to develop cost effective solutions to better manage risks posed by the identified vulnerability.

If a risk was identified for an existing system (as opposed to a risk associated with a proposed change), this would be taken into account in any direction making process, particularly with regard to the requirement that agencies and industry negotiate in good faith. The Attorney-General would only issue a direction to do or not do a specified act or thing as a measure of last resort where all efforts to reach agreement cooperatively have failed. This power also requires the Attorney-General to take into account a range of matters, including costs likely to be incurred by the C/CSP.

Data Retained in Australia

17. Macquarie Telecom raises concerns around about offshoring certain data and considers it important that Australia retains sovereignty over certain types of information (3rd page):

- **Do you consider that certain kinds of data should be retained on-shore?**

ANSWER:

The Bill does not specify where or how data must be stored. Instead, it supports a risk-based approach to managing national security concerns to the telecommunications sector, while also retaining flexibility in decision making for industry. This approach has been chosen to support industry's need to be innovative and competitive in the global telecommunications market.

C/CSPs would be expected to pay particular attention to identifying and addressing risks posed by higher risk service delivery models (such as offshoring). C/CSPs would be expected to be able to demonstrate, for example, that they have processes and arrangements in place to manage who can access systems and networks and facilities. If any risks were identified government would work with industry to mitigate those risks, including where consultations were ineffective, the use of the directions making power.

International approaches

18. Industry has raised a number of concerns regarding the approach outlined in the Bill when compared to international approaches (Industry Association: p7, para 2.2):

- **How would you respond to industry's claims that the telecommunications security framework adopted by New Zealand caused some companies to relocate their business operations off-shore to countries where the legislative requirements were less onerous?**
- **Do you consider the Bill to be as onerous as the New Zealand legislation?**

ANSWER:

The department considers the Bill has been developed to best fit the construction of the Australian telecommunications market. The Bill strikes an appropriate balance between allowing C/CSPs to make decisions in their own interest while recognising that government is best placed to identify and assess national security risks and provide guidance to industry on effective protections and mitigation strategies. Impacts on competition, consumers and costs both to industry and government were taken into account during development of the Bill.

Avoidance of any unintended consequences on Australia's ability to remain competitive and relevant in the global telecommunications market was a key driver behind government's decision to engage in extensive consultation on the reforms with industry, prior to the Bill's introduction.

The department is unable to comment on the drivers behind a business's decision on where it might be located. However, the Department notes that the New Zealand legislation requires network operators to submit annual plans to the New Zealand Government, in addition to their notification obligations. The reforms set out in the Bill provide flexibility for C/NCSPs to decide whether individual notifications or an annual security capability plan better suits their business model.