Australian Government
Attorney-General's Department

February 2017

Submission to the Parliamentary Joint Committee on Intelligence and Security

Telecommunications and Other Legislation Amendment Bill 2016

Table of Contents

Introduction

1. The reforms in the Telecommunications and Other Legislation Amendment Bill 2016 (the Bill) provide a balanced framework that enhances collaboration between industry and government to better manage national security risks to Australia's telecommunications networks and facilities. The reforms implement the recommendations of two separate reports of the Parliamentary Joint Committee on Intelligence and Security (PJCIS).[1]

2. Australia's national security, economic prosperity and social wellbeing are reliant on telecommunications networks and infrastructure. Underpinning our use of internet and telephony services is our telecommunications infrastructure, which carries and stores significant amounts of government, business and individuals' information and communications. Much of the information held on and carried over telecommunication networks and facilities can be sensitive. This includes not only the content of communications but also customer billing and management systems and lawful interception systems which, if unlawfully accessed, can reveal the location of persons or sensitive law enforcement operations.

3. Australian telecommunications networks form the backbone for the delivery and control of many other critical infrastructure sectors such as health, finance, transport, water and power. The government is addressing the protection of our critical infrastructure in a number of ways, including through the establishment of the Critical Infrastructure Centre (the Centre) in January 2017. The Centre will support the reforms proposed in the Bill, and in recognition of the shared responsibility for protecting our most critical assets, will work collaboratively with critical infrastructure owners and operators to identify and manage national security risks.

4. The information contained within the network and the connection to other critical infrastructure sectors make telecommunications networks and facilities a key target for espionage, sabotage and foreign interference activity. Advances in technology and communications have increased vulnerabilities, including the ability to disrupt, destroy or alter telecommunications networks and associated critical infrastructure, as well as the information held on these networks. Risks to the availability, confidentiality and integrity of our national telecommunications infrastructure can come from hardware vulnerabilities, misconfiguration, hacking and trusted insiders.

5. The threat of cyber intrusions into critical telecommunications networks is increasing.[2] Foreign states, as well as malicious individuals or groups, are able to use computer networks to view or siphon sensitive,

---

[1] Recommendation 19, *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation*, May 2013 and Recommendation 36, *Advisory Report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014*, February 2015.

[2] Between July 2015 and June 2016, the Computer Emergency Response Team Australia (CERT) responded to 14,804 cyber security incidents affecting Australian businesses, 418 of which involved systems of national interest and critical infrastructure. 11.7% of those were communications businesses [Australian Cyber Security Centre 2016 Threat Report, page 14, 15].

private, or classified information for the purpose of political, diplomatic or commercial advantage. Individual records or files stored or transmitted on telecommunications networks may not be classified or particularly sensitive in and of themselves but, in aggregate, they can give foreign states and other malicious actors a range of intelligence insights not otherwise readily available.

6. The government has introduced a number of measures which enhance Australia's cyber security. The reforms in the Bill are consistent with and complement the actions in the Cyber Security Strategy launched in 2016 which is designed to enable innovation, growth and prosperity for all Australians through strong cyber security. The strategy recognises the importance of private and public sector collaboration and information-sharing to combat cyber security threats. The government's commitment to this objective is demonstrated in a number of ways, including through the expansion of the national Computer Emergency Response Team (CERT) Australia and creation of Joint Cyber Security Centres to facilitate the timely sharing of cyber security information between business and government.

7. In recent years, the national security environment for critical infrastructure, including the telecommunications sector, has changed significantly. The number of suppliers in the market has dramatically increased and business models have evolved and now commonly rely on outsourcing and offshoring. A key source of vulnerability for unauthorised access and interference is in the supply of equipment, services and support arrangements. Australian telecommunications networks rely on global suppliers of equipment and managed services, which are often located in, and operate from, other countries. This can create challenges in implementing controls to mitigate personnel, physical and information and communications technology (ICT) security risks thereby making this infrastructure more vulnerable to unauthorised access and interference.

8. The current framework for addressing national security risks to Australia's telecommunications networks and facilities relies on voluntary cooperation and the goodwill of carriers/carriage service providers (C/CSPs). Where security risks are identified and agreement cannot be achieved, the only existing legislative avenue for government is the power to cease a service under section 581(3) of the *Telecommunications Act 1997* (Telecommunications Act). Ceasing a service under this provision is a tool of last resort, given the detrimental effect ceasing a service would have on both a C/CSP and on the community. The power has never been used. The reforms proposed by the Bill would ensure that national security risks can be more appropriately mitigated through other, more proportionate, measures.

9. The absence of a comprehensive and proportionate security framework means security agencies do not presently have adequate levers (except in the most extreme circumstances) to engage with companies who choose not to engage on a voluntary basis with government. The existing approach also limits security agencies' visibility of potential national security vulnerabilities to telecommunications networks and facilities, something C/CSPs may not be aware of when they are constructing, changing or developing their networks and facilities. A clear understanding of national security risks, for both government and industry, is essential to identifying telecommunications network vulnerabilities and managing them effectively.

10. The reforms set out in the Bill provide a risk-based and proportionate framework for managing national security risks to Australia's telecommunications infrastructure and facilities. The Bill will amend the Telecommunications Act and related legislation to:

    - make clear that C/CSPs are required to protect their networks and facilities from national security risks of unauthorised access and interference

    - establish a notification requirement for carriers and nominated CSPs (NCSPs)[3] to provide government with information to assist in the assessment of national security risks to telecommunications infrastructure, and

    - introduce escalating engagement and enforcement mechanisms to encourage compliance and proportionately manage national security risks to the telecommunications sector.

    The enforcement mechanisms would be used as a last resort and be supported by independent review mechanisms.

11. The Bill will formalise and strengthen industry and government relationships, ensuring greater consistency, transparency and accountability for managing national security risks across the telecommunications sector. The strengthened framework will encourage engagement between industry and government during the planning and design stage of investment and procurement decisions. Early engagement to address national security risks will minimise delay and costs and allow industry and government to achieve national security outcomes on a cooperative basis.

Why a regulatory approach?

12. In developing the Bill, the Attorney-General's Department (the department) considered a number of different approaches, including ones employed by other countries, and determined that a regulatory framework was the most appropriate option.

13. In particular, the department considered the net benefits of the following alternative options, detailed in the Regulation Impact Statement (RIS):

    (1) maintaining the status quo
    (2) developing an industry code, and
    (3) investment plans.

[3] 'Nominated Carriage Service Provider' means a carriage service provider declared to be a nominated carriage service provider by the Attorney-General under section 197 of the *Telecommunications (Interception and Access) Act 1979*.

International approaches

14. Similar to Australia, other countries are taking steps to manage security risks associated with telecommunications infrastructure and supply chains.
15. Internationally, there is an increasing trend for government to take action to secure networks and enhance information sharing between government and industry. These approaches differ but include:

    - broad security obligations to protect the security and resilience of networks (sometimes coupled with a requirement for independent verification that systems meet requirements)
    - notification regimes
    - data breach notification regimes
    - information gathering powers
    - powers of direction
    - enforcement mechanisms, and
    - restricting certain suppliers from the market, or limiting certain suppliers to providing limited services (outside of core or sensitive parts of networks).

16. The United States, United Kingdom, Canada, New Zealand and the European Parliament have enacted legislative frameworks to address cyber security in the telecommunications sector and encourage information sharing. Like Australia, these countries recognise that managing national security risks to telecommunications infrastructure is a joint responsibility between government and industry that requires collaboration.

17. New Zealand's framework requires providers to notify its government of proposed changes to equipment or services in addition to an annual reporting requirement. The United Kingdom and India impose a legislative obligation on service providers to secure their own networks. India also requires operators to audit their networks once a year. Under the Canadian approach, providers are encouraged to follow voluntary best practice guidelines on how to protect their networks.

18. International voluntary compliance frameworks, such as those outlined in the joint submission of the Australian Industry Group, Australian Information Industry Association, Australian Mobile Telecommunications Association and Communications Alliance, are often cyber security focused and outline voluntary procedures for sharing cyber threat information. As outlined in the introduction, Australia has voluntary information sharing forums in place which focus on cyber security generally. The proposed framework extends beyond general cyber security to enable the protection of Australia's critical infrastructure from specific national security risks. Formalising the existing and emerging relationships with the telecommunications industry will enable government to identify where security risks are and enable engagement at the earliest possible time.

Approach proposed by the Bill

19. The department determined that a regulatory framework would most effectively address the primary policy objective of providing an effective and efficient mechanism for managing national security risks. Impacts on competition, consumers and costs both to industry and government were taken into account.[4] The Bill strikes an appropriate balance between allowing C/CSPs to make decisions in their own interest while recognising that the government is best placed to identify and assess national security risks and provide guidance to industry on effective protections and mitigation strategies.[5] The department agrees with the submissions of the Australian Industry Association and Optus in that effective communication between government and industry will be critical to the success of these reforms. The government will work closely with industry, including through the Critical Infrastructure Centre and Communications Access Coordinator in the Attorney-General's Department, to support C/CSPs to identify and manage national security risks.

20. A risk-based approach, rather than a prescriptive approach, was adopted to recognise the variances within the telecommunications sector, in particular that the way a C/CSP designs its network and services can significantly change the assessed level of risk posed by a proposed change. The notification requirement allows an assessment to take into account the individual characteristics of a C/CSPs networks and services and the dynamic nature of both the threat environment and telecommunications sector. This approach was chosen for its flexibility, allowing individual assessments to be made based on risks relevant to the individual C/CSP.

21. This approach recognises that not all data, parts of networks or business operating models necessarily give rise to national security concerns. The proposed legislative obligation to protect networks and facilities will elevate the prioritisation of national security considerations by industry Boards of Executives and increase the visibility of procurement processes by security agencies (through the notification requirement). This will allow for a better informed and targeted approach to managing security risks at all levels of the telecommunications sector. The risk-based approach also limits the regulatory impact on industry as those aspects of telecommunications networks that do not necessarily give rise to national security concerns are not affected by the requirements.

22. The Bill proposes a balanced and risk-based approach to take into account the needs of the Australian telecommunications sector to remain competitive and innovative in the market, having regard to minimising regulatory impacts. The framework outlined in the Bill draws on international experience, rather than being identical to any of the approaches in place in other countries.

[4] Regulation Impact Statement, page 42.
[5] Regulatory Impact Statement, page 50.

Reforms costs

23. The reforms outlined in the Bill will put in place minimal regulatory requirements, with the total estimated cost to industry to comply being $220,000 per annum.[6] The estimated regulatory burden has been offset through the removal of the retail price controls in the telecommunications sector through amendments to the *Telecommunications (Consumer Protection and Service Standards) Act 1999*.[7]

24. The total estimated cost to government in administering and enforcing the scheme would be $1.6 million:

- Security agencies costs of $1.1 million – for engaging and monitoring compliance with the framework, including engagement with C/CSPs, developing security threat assessments and advice to C/CSPs on risk and risk mitigation strategies, and collaborating with the Attorney-General's Department (as regulator) on enforcement action and compliance with enforcement action.

- Attorney-General's Department costs of $500,000 – in establishing and maintaining regulatory functions, including implementing processes to engage and obtain information from lower risk C/CSPs, supporting security agency engagement processes, and advising C/CSPs of obligations and requirements.[8]

Key elements of the Bill

Obligation to protect telecommunications networks and facilities

Amendment to the Telecommunications Act:

- ***New subsection 313(1A) and (2A):*** *Requires C/CSPs to do their best to protect telecommunications networks and facilities owned, operated or used by the C/CSP from unauthorised interference or unauthorised access, including maintaining competent supervision and effective control over their networks and facilities.*

25. The Bill requires all C/CSPs to do their best to protect networks and facilities they own, operate or use from unauthorised interference and access for the purpose of security (within the meaning of the *Australian Security and Intelligence Organisation Act 1979* (ASIO Act)).[9] This is consistent with the existing obligations in section 313 of the Telecommunications Act and avoids imposing an absolute obligation. Compliance with this requirement requires C/CSPs to take all *reasonable steps* to prevent unauthorised access and interference for the purpose of protecting the confidentiality of information

[6] Telecommunications Sector Security Reforms – Regulatory Impact Statement, 6 July 2015: http://ris.dpmc.gov.au/2015/07/06/telecommunications-sector-security-reforms/.
[7] This decision was made in consultation with OBPR and is reflected in the RIS (pages 38 and 53). The instrument can be accessed here - https://www.legislation.gov.au/Details/F2015L00330.
[8] *Ibid*.
[9] Security includes the protection from espionage, sabotage and acts of foreign interference.

and the availability and integrity of networks. In this way, the provision acknowledges that it may not be possible to prevent all unauthorised access and interference.

26. In order to comply with the legislative obligation, C/CSPs would be expected to be able to demonstrate they have implemented effective security measures to identify and manage risks of unauthorised access and interference to networks and facilities owned, operated or used by the C/CSP.

27. The Bill does *not* specify or prescribe what solutions a C/CSP must use to secure networks or facilities. This approach is intended to provide flexibility to industry, acknowledging that the approach adopted by individual C/CSPs will be highly dependent upon the risk factors specific to each provider.

28. Compliance with the security obligation includes a requirement that the C/CSP demonstrate competent supervision of, and effective control over, networks and facilities owned or operated by the C/CSP.

29. Competent supervision - refers to the ability of a C/CSP to maintain proficient oversight of its networks, data and facilities. Competent supervision could include arrangements to maintain:

    - visibility of network and facility operations
    - visibility of data flow and locations
    - awareness of parties with access to network infrastructure, and
    - the ability to detect security breaches and compromises.

30. Effective control - refers to a C/CSPs ability to maintain direct authority to ensure that its network and facilities, infrastructure and information stored or transmitted, is protected from unauthorised interference and access. This would include authority over all parties with access to network infrastructure and, as noted above, the ability to control who has access to networks and facilities, and information held by the C/CSP. Effective control might include the ability to:

    - direct actions to ensure the integrity of network operations and the security of information carried on them
    - terminate contracts where there has been a security breach or data breach reasonably attributable to the contracted services or equipment
    - direct contractors to carry out mitigation or remedial actions
    - oblige contractors to monitor and report breaches to the C/CSP, and
    - re-establish the integrity of data or systems where unauthorised interference or access has occurred (for example to confirm accuracy of information or data holdings).

31. One way of demonstrating a C/CSP has effective control, may be through third party assurance (i.e implementing controls which can be tested and providing evidence that primary information security requirements have been satisfied (or are able to be satisfied)).

Notification obligations

Amendments to the Telecommunications Act:

- ***New section 314A:*** *Requires Carriers and Nominated Carrier Service Providers (C/NCSPs) to notify the Communications Access Co-ordinator (CAC) of a change that is proposed to telecommunications services or systems that is likely to have a material adverse effect on the ability of the C/NCSP to comply with its security obligation (under subsections 313(1A) and (2A) of the Telecommunications Act).*
- ***New subsection 314A(2):*** *Outlines what sort of changes should be notified to the CAC.*
- ***New subsection 314A(4):*** *Can allow the CAC to exempt a C/NCSP from this requirement.*
- ***New section 314B:*** *Outlines assessment processes for notifications*
- ***New sections 314C, 314D and 314E:*** *Outlines the option for a C/NCSP to satisfy the notification requirement by submitting a security capability plan, and associated processes.*

Notification obligation

32. The notification requirement only applies to Carriers and NCPs (C/NCSPs). All C/NCSPs will be required to provide a notification to the CAC of planned changes to telecommunications services or systems that are likely to have a 'material adverse effect' on the ability of the C/NCSPs to comply with its obligation to protect its networks. It is not necessary for a 'material adverse effect' to have occurred, rather, that a proposed change is likely to have a 'material adverse effect'.

33. Subsection 313(1B) provides that the obligation to protect networks includes the requirement for the C/CSP to maintain competent supervision of or effective control over networks and facilities owned or operated by the C/CSP. Subsection 314A(2) of the Bill provides clarity for industry in identifying what types of changes to equipment may require notification – for example:

    - the engagement of a new billing supplier that would have access to sensitive customer information
    - upgrading core equipment requiring access or installation of software on equipment affecting law enforcement operations, or
    - data storage solutions with contractors not previously notified to government or outside Australia.[10]

34. The notification requirement formalises information sharing between C/NCSPs and government. This is triggered at the time the C/NCSP becomes aware of a proposed change. Consideration of the impact of a change has on the C/NCSPs ability to protect their networks and facilities should occur at the planning of proposed changes to networks and services, rather than following or close to implementation. There are two ways of notifying government of changes:

    - individual notifications – the CAC will have 30 days to respond, and
    - security capability plans – the CAC will have 60 days to respond.

[10] Section 314A(2) provides examples of other changes that require notification.

35. During the period of considering either the individual notification or the security capability plan, government will liaise with the notifying industry member about the notification. The CAC will respond by either:

    - requesting further information about the proposed change
    - notifying the C/NCSP that there is a risk of unauthorised access or interference that would be prejudicial to security and may set out measures to eliminate or reduce the identified risk, or
    - notify the C/NCSP that there is not a risk of unauthorised access or interference that would be prejudicial to security

36. Subsections 314A(4) and (5) authorises the CAC to exempt a C/NCSP from compliance with the notification requirement in section 314A. There is no legislative application process for C/NCSPs as exemptions will be granted on a case by case basis with further guidance on the process developed during the implementation period.

37. C/NCSPs that are unsure whether a proposed change may pose a national security risk (and therefore requires notification) can refer to the Administrative Guidelines, a live document that will continue to be developed in consultation with industry, and discuss their queries with the department.

Attorney-General's directions powers

38. The Bill introduces directions powers which will provide more proportionate options for managing national security risks to the telecommunications sector, where efforts to reach agreement cooperatively have failed. There are two types of directions powers:

    - a direction to cease a service, or
    - a direction to do or not do a specified thing.

Existing directions power – cease a service

Amendments to the Telecommunications Act:

- ***New section 315A****: the Attorney-General may direct a C/CSP to not use or supply, or cease using or supplying, a carriage service/s where the use or supply is, or would, be prejudicial to security.*

39. Existing section 581(3) of the Telecommunications Act allows the Attorney-General to direct a C/CSP to not use or supply, or cease using or supplying, a carriage service where the use or supply is, or would, be prejudicial to security. The Bill adds two additional safeguards to the exercise of this power by:

    - specifying that a direction to cease a service can only be made after an adverse security assessment in respect of the C/CSP has been given to the Attorney-General by the Australian Security Intelligence Organisation (ASIO), and

- introducing a review right under the *Administrative Decisions (Judicial Review) Act 1977* (ADJR Act) to increase transparency and accountability in the direction making process.

40. The existing power would only be used in extreme circumstances of high risk to national security. Prior to exercising the power, the Attorney-General is required to consult with the Prime Minister and Minister administering the Telecommunications Act (currently the Minister for Communications and the Arts). This consultation ensures that impacts on the C/CSP, end user, market and economy more broadly are considered before a direction is issued.

Directions power – to do or not do a specified act or thing

Amendments to the Telecommunications Act:

- ***New section 315B:*** *will give the Attorney-General powers to direct a C/CSP or carriage service intermediary to do, or refrain from doing, a specified act or thing if there is a risk to security from unauthorised access to, or interference with, telecommunications networks or facilities.*

41. The Attorney-General can only issue a direction:

    - if satisfied that there is a risk of unauthorised access or interference to telecommunications networks or facilities that would be prejudicial to security
    - if satisfied that reasonable steps have been taken to negotiate in good faith with the carrier, provider or intermediary to eliminate or reduce the risk, and
    - after an adverse security assessment (detailed later in this submission) in respect of the carrier, provider or intermediary is given to the Attorney-General by ASIO, and after consulting the Minister responsible for administering the Telecommunications Act.

42. This power must specifically direct action, or refraining from an action, that is 'reasonably necessary' to reduce or eliminate the risk of unauthorised access or interference which would otherwise result in a risk prejudicial to security. Noting the reforms are directed at better managing national security risks associated with the supply of equipment, services and support arrangements, the directions power is likely to be exercised to address vulnerabilities that arise through these arrangements. As outlined in paragraph 180 of the Explanatory Memorandum, this could include requiring certain access controls to be implemented to restrict third party access to sensitive parts of networks such as lawful interception systems.

43. In making the decision on whether to issue a direction, the Attorney-General must have regard to a range of matters including the adverse security assessment, the costs that would be likely to be incurred by the carrier, provider or intermediary, the potential consequences that any direction may have on competition in the telecommunications industry and the potential consequences that any direction may have on customers of the carrier, provider or intermediary. The Attorney-General must give the greatest weight to the adverse security assessment furnished by ASIO. The weighting is important to ensuring the reforms deliver on national security objectives of the Bill to better manage threats to the

telecommunications sector.

44. To enable flexibility in the engagement between government and industry, the Bill does not specify the types of things that the Attorney-General can direct a C/CSP to do or not do.

45. The requirement for the Attorney-General to be satisfied all reasonable steps have been taken to negotiate in good faith reflects an objective of the reform to encourage industry and government collaboration and partnership to protect networks and facilities against unauthorised access and interference. The good faith requirements ensure government agencies take genuine steps to engage with a C/CSP including working with them to develop reasonably necessary mitigation measures to reduce or eliminate risks of unauthorised interference or access to telecommunications networks or facilities. While the regulatory powers (and enforcement mechanisms) will provide mechanisms for addressing non-compliance, they are intended to operate as a last resort to address non-cooperative conduct rather than to penalise action and decisions taken in good faith.

46. The directions power under section 315B is to be exercised by the Attorney-General and will also be subject to judicial review under the ADJR Act to ensure transparency and accountability. Merits review has not been provided for the new directions power as the ASIO security assessment (upon which the decision to issue a direction is based) is already subject to merits review under the ASIO Act.

Adverse security assessments

47. An adverse security assessment would only be prepared in circumstances where ASIO or another relevant agency had informed a C/CSP of the security risks to the C/CSPs network and/or facilities and all reasonable attempts have been made to negotiate a cooperative outcome that reduces or eliminates the security risk. Subsection 315A(3) of the Bill provides that the Attorney-General cannot exercise the directions power without an adverse security assessment. In this circumstance, an adverse security assessment will set out ASIO's advice in respect of the requirements of security in regard to the exercise of the directions power in the relevant circumstances, including its recommendation that the power be exercised and the statement of grounds for its assessment in accordance with the ASIO Act.

48. As noted above, the Bill applies a threshold ensuring that any direction made is only issued in circumstances where ASIO has furnished an adverse security assessment. This provides an additional safeguard to C/CSPs when the directions power is exercised.

49. In accordance with Part IV of the ASIO Act, the C/CSP would be able to seek merits review of the ASIO security assessment in the Administrative Appeals Tribunal (AAT). The Attorney-General would be required to provide a copy of the security assessment to the C/CSP within 14 days after the day on which the assessment is furnished in accordance with subsection 38(1) of the ASIO Act.

Information gathering powers

Amendment to the Telecommunications Act:

- ***Section 315C:*** *will grant the Department's Secretary the power to obtain information and documents from C/CSPs and intermediaries, where that information is relevant to assessing compliance with the obligations imposed under subsections 313(1A) and (2A) of the Bill.*
- ***Section 315G:*** *the Secretary may delegate his or her information gathering power to the Director-General of Security, ASIO.*
- ***Section 315H:*** *sets out how information obtained may be shared and used.*

50. The information-gathering power is intended to formalise and extend the existing cooperative relationship of information exchange between government, and C/CSPs and intermediaries. The information-gathering powers will be most relevant where information is unable to be obtained on a cooperative basis. For example, where a C/CSP considers it is restrained from sharing information for contractual or other legal reasons.

51. Prior to exercising information gathering powers, the Secretary of the department will need to consider the potential cost, time and effort imposed on the C/CSP, or intermediary, in complying with the notice. The information that would be sought under these powers would be commercial in nature, such as procurement plans, network or service design plans, tender documentation, contracts and other documents specifying business and service delivery models and network layouts. Contrary to the suggestion made by the Australian Centre for Cyber Security in its submission, the Bill does not create any requirements to retain or provide access to metadata. Authorised agencies' access to metadata under the *Telecommunications (Interception and Access) Act 1979* is subject to strict controls and only available in limited circumstances.

52. Section 315H authorises the further use or disclosure of information obtained under the information gathering powers to persons other than the Secretary of the department or his or her delegate. The following safeguards are built into section 315H to protect commercially sensitive information:

    - disclosures are limited to the protection of security (as defined by the ASIO Act), and
    - a requirement for the removal of identifying information.

53. In practice, it is likely that information sharing may take place between relevant government agencies, such as the Department of Communications and the Arts or the Australian Signals Directorate. For example, information or documents may be shared in cases where technical expertise or assistance is required to assess risks to security.

Injunctions and enforcement powers

54. The directions powers granted to the Attorney-General and the information-gathering powers granted to the Secretary of the department by the Bill will be enforceable by virtue of the application of existing civil remedies provided for in the Telecommunications Act. The enforcement mechanisms in the Bill are intended to operate as a last resort to address non-cooperative conduct rather than to penalise action and decisions taken in good faith.

55. The Attorney-General can initiate proceedings in the Federal Court to seek civil remedies for non-compliance with the security obligation, a direction and/or a request for information – these include penalties, enforceable undertakings and injunctions. Consistent with all obligations under the Telecommunications Act, non-compliance with a direction or an information request would constitute a breach of carrier licence conditions or carriage service provider rules as these require compliance with the Telecommunications Act.

Other issues

Treatment of networks or facilities located overseas or outsourced

56. The regulatory framework applies to all C/CSPs within the meaning of the Telecommunications Act. This includes C/CSPs that have networks and facilities based in Australia, or based overseas which are used to provide services and carry and/or store information from Australian customers.

57. The Bill would require C/CSPs to do their best to protect sensitive parts of their networks and facilities from unauthorised interference and access. This would include those parts of networks and facilities which are of greatest security interest such as operations centres and any part of a telecommunications network that manages or stores information about customers. This obligation would apply irrespective of whether the location of that part of a C/CSPs operation is located in Australia, or overseas. C/CSPs would be expected to pay particular attention to identifying and addressing risks posed by higher risk service delivery models (such as outsourcing or 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 (as part of their requirement to demonstrate competent supervision and effective control).

Data storage

58. The Bill does not specify where or how data must be stored. The Bill supports a risk-based approach to managing national security concerns to the telecommunications sector, while also retaining flexibility in decision making for industry. The constantly changing nature of the telecommunications environment necessitates the need for industry to innovate and be in a position where they can retain flexibility to support their changing business needs and with minimal regulatory burden on their ability to conduct business internationally.

Access of suppliers to the Australian market

59. The Bill does not prevent specific suppliers from providing services or equipment in Australia, nor exclude suppliers on the basis of their country of origin. The proposed Bill will ensure that any risks associated with the supply chain are considered and managed by C/CSPs, with assistance from security agencies, where appropriate.

Retrospective application

60. C/CSPs will not be expected to retrofit all systems in order to comply with the security obligation to protect networks and facilities from unauthorised interference and access. Should there be a case where significant national security vulnerabilities are identified in an existing system, security agencies would

work collaboratively with the C/CSP to develop solutions to better manage the risks posed by the existing vulnerability.

Treatment of broadcast and content services

61. The Bill applies to the protection of telecommunications networks and facilities, irrespective of the type of service being provided over the networks. The Bill in its current form enables exemptions to be provided to a C/NCSP that offers a range of services from providing notifications in relation to a part of their business. As noted in the Explanatory Memorandum, an exemption could be made, for example, in relation to broadcasting or a subscription television service. However, the provider would still be required to notify of changes to other parts of their business that apply to the provision of other services, such as telephony and broadband access. The exemption process will be refined during the implementation phase, in consultation with industry.

Consultation

Public Consultation on Exposure Draft Legislation

62. The proposed reforms have been the subject of significant consultation with the telecommunications industry since 2012, including two rounds of public consultation on exposure draft legislation and associated documentation (in June – July 2015 and November 2015 – January 2016, respectively).

63. Significant amendments were made to the draft Bill and Explanatory Memorandum to address industry feedback including to:

- clarify and limit the scope of the security obligation to protect telecommunications networks and facilities by limiting it to networks or facilities owned operated or used by a C/CSP
- increase the threshold for the exercise of regulatory powers, i.e so that the Attorney-General may only give a direction where satisfied that they are 'reasonably necessary' to eliminate or reduce the security risk of unauthorised access or interference which is prejudicial to security
- allow companies (under information gathering powers) to provide copies of documents, and also be entitled to reasonable compensation for complying with a requirement to provide a copy of a document
- expand confidentiality requirements to protect the confidentiality of commercially sensitive information or documents provided in individual notifications or security capability plans
- increase the implementation period from six to 12 months, and
- provide an option for industry to determine whether to provide individual notifications or annual security capability plans depending on the method that better suits their business model.

Implementation arrangements

64. The Bill provides for a 12 month implementation period. This time will be used to engage further with industry to:

- facilitate processes to underpin the exchange of threat information between industry and government
- develop processes for the provision of individual notifications, security capability plans, and exemptions from the notification obligation; and
- further develop the Administrative Guidelines (Guidelines)

65. The current draft of the Guidelines were developed in November 2015 and made available on the department's website as part of the second public consultation process. The Guidelines are designed to aid compliance with the framework as introduced by the Bill. They include information about the sorts of business operating models that present higher risks and the parts of networks that are particularly vulnerable from a national security perspective. They also outline the sorts of controls and measures that can be implemented to manage these vulnerabilities. It is intended that the Guidelines will be a live document and subject to periodic review in order to capture changes to related legislation and security advice.

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.

UNCLASSIFIED

The department's answers to the two questions that were asked during the private hearing on 15 February are below.

Question One: What proportion of equipment is sourced from overseas companies of concern due to cost pressures?

The department does not have details of the proportion of equipment sourced from overseas companies of concern due to cost pressures. The department understands that providers take into account a range of factors when considering where to source their equipment from. These include cost, speed to market (availability of equipment, expertise and whether retrofitting of other equipment may be required) and longer-term issues such as support costs, staff training and interoperability with other equipment and services. In summary, the department understands that while initial costs are an important factor, having regard to cost impact of other factors, providers do not necessarily go with the cheapest option.

Question Two: What is the number of companies that off-shore metadata?

The department does not have this information as the law does not currently compel telecommunications providers to tell the government where retained data is stored. The data retention legislation includes an obligation on industry to protect and encrypt retained data and companies must also take reasonable steps to secure personal information to meet their obligations under the *Privacy Act 1988*.

The telecommunication sector security reforms are designed to better manage security risks, including risks posed by offshoring, and will provide greater protection not only for Australian metadata stored offshore, but also metadata stored in Australia that can be accessed offshore. The reforms will require providers to protect existing networks and systems and enable the department to obtain information, including on existing offshore arrangements. There is also a further obligation on providers to notify the department of any proposed changes that are likely to create a security risk.