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.