2016

THE PARLIAMENT OF THE COMMONWEALTH OF AUSTRALIA

SENATE

TELECOMMUNICATIONS AND OTHER LEGISLATION AMENDMENT BILL 2016

EXPLANATORY MEMORANDUM

(Circulated by authority of the

Attorney-General, Senator the Honourable George Brandis QC)

TELECOMMUNICATIONS AND OTHER LEGISLATION AMENDMENT BILL 2016

GENERAL OUTLINE

1. The Telecommunications and Other Legislation Amendment Bill 2016 (the Bill) will amend the *Telecommunications Act 1997* (the Telecommunications Act) and related legislation, including the *Telecommunications (Interception and Access) Act 1979* (the TIA Act), the *Administrative Decisions (Judicial Review) Act 1977* (the ADJR Act) and the *Australian Security Intelligence Organisation Act 1979* (the ASIO Act), to introduce a regulatory framework to better manage national security risks of espionage, sabotage and foreign interference to Australia's telecommunications networks and facilities.

2. The security and resilience of telecommunications infrastructure significantly affects the social and economic well-being of the nation. Government and business are increasingly storing and communicating large amounts of information on and across telecommunications networks and facilities. By their nature, telecommunications networks and facilities hold sensitive information. For example, lawful interception systems and customer billing and management systems which, if unlawfully accessed, can reveal sensitive law enforcement operations or the location of persons. This information presents a rich intelligence target for those who wish to harm Australian interests. Telecommunications networks, systems and facilities are also critical infrastructure and vital to the delivery and support of other critical infrastructure and services such as power, water and health.

3. For these reasons, the telecommunications networks and facilities of carriers, carriage service providers and carriage service intermediaries (C/CSPs) are attractive targets for espionage, sabotage and foreign interference activity by state and non-state actors. National security risks relate to possible:

- compromise or degradation of telecommunications networks
- compromise of valuable data or information of a sensitive nature, such as aggregate stores of personal data or commercial or other sensitive data
- impairment of the availability or integrity of telecommunications networks; or
- the potential impact on other critical infrastructure or government services (such as banking/finance, health or transport services).

4. A key source of vulnerability for espionage, sabotage and interference activity 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 further challenges in implementing controls to mitigate personnel, physical and information and communications technology (ICT) security risks in some locations and therefore make networks and facilities more vulnerable to unauthorised access and interference.

5. Advances in technology and communications have introduced significant vulnerabilities, including the ability to disrupt, destroy or alter telecommunications networks and associated critical infrastructure as well as the information held on these networks. Vulnerabilities in telecommunications equipment and managed service providers can allow

state and non-state actors to obtain clandestine and unauthorised access to networks. Such access could be used to extract information and disrupt or potentially disable networks.

6. While it is in the interest of all C/CSPs to secure their networks and facilities in order to comply with existing legislative obligations (for example to protect personal information under the *Privacy Act 1988* (the Privacy Act)) and to protect business continuity and reputation, these may be different to the requirements to protect national security interests. For example, some business delivery models may expose a telecommunications network, facility or service to high risks of espionage, sabotage and unauthorised interference and access, but may not otherwise affect the business continuity or general security of the network or facility. The reforms are intended to require C/CSPs to take into account a broader range of security risk factors when making investment decisions, to protect broader national security interests.

7. Currently national security risks to the telecommunications sector are largely managed through informal cooperative arrangements with industry. Security agencies have well established cooperative relationships with select carriers, and work collaboratively with these carriers to manage vulnerabilities on these networks. However, there are significant limitations to this approach. A voluntary or cooperative approach is only workable where companies are willing to give due consideration to national security and the public interest. . The industry is also dynamic and competitive and there are a number of market entrants and companies rapidly growing their market share that do not have established relationships with government. The rollout of the NBN magnifies the changes within the market.

8. There is an existing power in subsection 581(3) of the Telecommunications Act which authorises the Attorney-General to direct a C/CSP to cease operating its service where the proposed or continued operation of that service is, or would be, prejudicial to security. The power is an extreme measure and only appropriate for managing the most extreme national security risks given the potentially significant flow on consequences for the affected company's business, their customers, and possibly the broader Australian economy. For these reasons the power has not been exercised to date.

9. The absence of a comprehensive and proportionate security framework means security agencies do not have adequate levers (except in the most extreme circumstances) to engage those companies who choose not to engage on a voluntary basis with security agencies. Not only does this limit security agencies' visibility of potential vulnerabilities which could be exploited by malicious actors across a large part of the sector, it compromises existing cooperative relationships with carriers who seek a level playing field.

10. The security framework will formalise the relationship between Australian Government agencies and C/CSPs to achieve more effective collaboration on the management of national security risks. The aim is to encourage early engagement on proposed changes to networks and services that could give rise to a national security risk and collaboration on the management of those risks. While a more formal relationship is necessary to ensure appropriate management of national security risks, the regulatory objective is to achieve national security outcomes on a cooperative basis rather than through the formal exercise of regulatory powers. The Attorney-General's Department (AGD) and Australian Security Intelligence Organisation (ASIO) will work with C/CSPs to achieve more secure networks and facilitate the early identification of potential national security risks.

11. The Bill amends the Telecommunications Act to establish a comprehensive regulatory framework to better manage national security risks of espionage, sabotage and foreign interference, and better protect networks and the confidentiality of information stored on and carried across them from unauthorised interference and access. The amendments will supplement existing provisions including:

- the national interest obligations in section 313 of the Telecommunications Act, which require C/CSPs to do their best to protect networks and facilities from being used to commit offences;

- notification requirements in section 202B of the TIA Act concerning proposed changes to networks and services; and

- the existing directions power in subsection 581(3) to cease a service.

12. The Bill also implements the recommendations of two separate Parliamentary Joint Committees on Intelligence and Security (PJCIS). In 2013, the PJCIS recommended that the government progress measures to enhance the security and stability of Australia's telecommunications infrastructure. The recommended measures included the establishment of a security framework by way of amendments to Australia's telecommunications legislation (recommendation 19).

13. In its advisory report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014, the PJCIS further recommended that the government enact the proposed telecommunications sector security reforms prior to the end of the implementation phase of the data retention regime. This security framework would complement the data retention regime by improving the security of networks as a whole, thereby providing an additional layer of protection for retained data, as well as other information.

14. The Bill delivers on telecommunications sector security reform work recognised in the 2016 Australian Cyber Security Strategy.

Overview of legislative amendments

15. The Bill supports and gives meaning to existing provisions by:

- imposing a security obligation on C/CSPs requiring them to do their best to manage the risk of unauthorised access and interference to networks and facilities they own, operate or use to ensure the availability and integrity of networks and facilities and to protect the confidentiality of information stored on and carried across them

- imposing a notification requirement on carriers and some carriage service providers to notify of planned changes to systems and services that are likely to make the network or facility vulnerable to unauthorised access and interference, and providing for exemptions or partial exemptions from the requirement and the option to submit a Security Capability Plan to meet notification requirements

- providing the Secretary of AGD with an information gathering power to facilitate compliance monitoring and compliance investigation activity in relation to compliance with the security obligation

- providing the Attorney-General with a further directions power to direct a C/CSP to do or not do a specified thing (for example, alter a procurement assessed as giving rise to security risks), and

- providing enforcement mechanisms by extending the civil remedies regime provided for in Part 30 (injunctions), Part 31 (civil penalties), and Part 31A (enforceable undertakings) to address non-compliance with the security obligation, a direction, or notice to produce information or a document. The Attorney-General would be authorised to commence proceedings to seek these remedies.

16. The Bill also repeals and reinserts subsection 581(3) as new section 315A to place the national security related provisions within the same part of the Act. There are no substantive changes to the existing direction power, with the exception of clarifying that the power can only be exercised on the basis of an ASIO adverse security assessment and to remove the current exemption from review under the ADJR Act.

17. The regulatory framework is intended to promote a risk informed approach to managing national security risks of espionage, sabotage and foreign interference across telecommunications providers. For this reason, the national security obligation will apply to all C/CSPs. This will ensure that responsibility for managing national security risks to telecommunications infrastructure is more equitably managed across the industry. The approach is risk managed by requiring C/CSPs to "do their best" to manage the risk of unauthorised interference and access, which intends to impose a reasonableness test having regard to the particular circumstances of a C/CSP. In other words, what is required of a C/CSP to comply with the security obligation will be highly dependent on the risk profile of the provider.

18. On this basis, the notification requirement only applies to carriers and nominated carriage service providers (C/NCSPs) - NCSPs are companies that have been nominated under the TIA Act. The new notification requirement in section 314A of the Telecommunications Act is modelled on the existing notification provision in section 202B of the TIA Act. Section 314A will require C/NCSPs to notify the Communications Access Coordinator (CAC) within the AGD (as established under the TIA Act) of planned changes to telecommunications services or systems which are likely to have a material adverse effect on a C/CSP's ability to meet its duties under new sections 313(1A) and 313(2A) of the Telecommunications Act.

19. The Bill amends section 202B of the TIA Act to expressly exclude the application of section 202B to new sections 313(1A) and (2A) of the Telecommunications Act. Creation of a standalone notification provision within Part 14 of the Telecommunications Act will improve transparency of the new security framework. The new notification provision also clarifies the process for dealing with a notification once it is received by the CAC, and authorises the CAC to exempt a C/NCSP from compliance with the notification obligation either completely or in part.

20. New section 314A of the Telecommunications Act outlines the types of changes in arrangements that should be notified to the CAC, which include but are not limited to: outsourcing or offshoring arrangements affecting sensitive parts of a network and/or, procuring new equipment or services for sensitive parts of a network, and changes to the management of services. To streamline the notification requirement, C/CSPs will also have the option of submitting an annual Security Capability Plan which will facilitate bulk notification reporting.

21. The regulatory framework is intended to formalise and strengthen existing industry-government engagement and information sharing practices. The aim is that the new security obligation will operate to encourage engagement with government agencies on managing national security risks of espionage, sabotage and foreign interference. It will also provide industry with greater certainty about what is expected of them to protect national security interests and encourage greater consistency, transparency and proper accountability. The notification requirement is intended to trigger the consideration of national security when planning network or service delivery changes, particularly where services or network support is to be outsourced. A key area of interest for the government is changes to networks and systems that introduce risks to their security and the appropriate mitigations that would address these.

22. The security framework is not intended to prevent the use of particular equipment vendors or service suppliers. Additionally, it is a commercial reality that most C/CSPs will already have some component of outsourcing and offshoring in their business service delivery and support models. The framework only applies to C/CSPs within the meaning of the Telecommunications Act. This includes companies which have networks and facilities based in Australia, or networks or facilities located or managed offshore that are used to provide services and carry and/or store information from Australian customers. For global companies based in Australia, this means that to the extent networks, facilities and services are operated and managed in other countries, and do not have an Australian link, they are not required to ensure those networks and facilities comply with requirements under the framework.

23. The notification requirement is also not intended to replace existing direct engagement with security agencies. Rather it will provide greater clarity about the types of changes to network operations and service delivery that are likely to give rise to national security considerations and encourage targeted collaboration between C/NCSPs that have a high risk profile and security agencies to ensure these risks are adequately managed. While enforcement mechanisms and the regulatory powers 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. In considering whether C/CSPs are meeting their obligation (to do their best to manage the risk of unauthorised access and interference to networks and facilities that they own, use or operate), regard will be had to existing arrangements that C/CSPs already have in place when the provisions come into effect. Consideration will be given to existing arrangements when assessing compliance; however, this does not prevent the exercise of the directions powers to address an existing security risk. For example, if ASIO assessed that existing arrangements posed an immediate and unacceptable security risk to the confidentiality of information or the availability and integrity of networks and systems, ASIO may recommend implementing measures to mitigate the risk.

24. Importantly, the framework will be implemented and enforced on a good faith basis with the core objective to encourage industry and government collaboration and partnership to harden networks and facilities against unauthorised access and interference. However, there may be circumstances when a C/CSP wants the protections against civil and criminal liability which would be afforded through the exercise of the direction or information gathering powers. In some circumstances it may be in the interests of a company to request a direction to provide a clearer mandate for its board in making investment decisions.

25. Implementation of the legislative frameworks will be facilitated through non-binding administrative guidelines and the provision of threat information to assist C/CSPs to understand which parts of networks and facilities are particularly vulnerable to unauthorised access and interference, what is required of them to meet their legislative requirements and possible control measures and mitigations.

FINANCIAL IMPACT

26. The ongoing costs of resourcing and administering the scheme by ASIO and AGD are estimated to be $1.6m annually. These additional costs will be due to increased engagement with C/CSPs and to review notifications of proposed changes to telecommunications systems and services.

REGULATION IMPACT STATEMENT

The regulation impact statement appears at the end of this explanatory memorandum.

STATEMENT OF COMPATIBILITY WITH HUMAN RIGHTS

Prepared in accordance with Part 3 of the Human Rights (Parliamentary Scrutiny) Act 2011

Telecommunications and Other Legislation Amendment Bill 2016

27. This Bill is compatible with the human rights and freedoms recognised or declared in the international instruments listed in section 3 of the *Human Rights (Parliamentary Scrutiny) Act 2011*.

Overview of the Bill

28. The Telecommunications and Other Legislation Amendment Bill 2016 (the Bill) will establish a risk-based framework to effectively manage national security risks to Australia's telecommunications infrastructure. The Bill will implement recommendation 19 of the June 2013 PJCIS' *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation*.

29. Recommendation 19 of the PJCIS's 2013 report was that the government amend the the Telecommunications Act to create a security framework that would provide a telecommunications industry-wide obligation to protect infrastructure and the information held on it, or passing across it, from unauthorised interference. The PJCIS also recommended the security framework include a requirement for industry to provide information to government to assist in the assessment of security risks to telecommunications infrastructure, in addition to powers of direction and a penalty regime to encourage compliance.

30. The Bill will also implement a recommendation from the PJCIS in its advisory report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 that the government enact the proposed telecommunications sector security reforms prior to the end of the implementation phase of the Data Retention Bill.

31. The Bill will implement each of these recommendations through amendments to the Telecommunications Act. The amendments will impose a new security obligation on the telecommunications industry, including carriers, carriage service providers and carriage service intermediaries (C/CSPs). C/CSPs will be required under new sections 313(1A) and (2A) to do their best to protect networks and facilities they own, operate or use from unauthorised access and interference for the purposes of security. This will complement the existing scheme in subsections 313(1) and (2) of the Telecommunications Act which requires C/CSPs to do their best to prevent their networks and facilities from being used to commit offences.

32. New section 315B of the Bill will give the Attorney-General powers to direct a C/CSP to do, or refrain from doing, a specified act or thing if there is a risk to security. This is in addition to the current power of the Attorney-General to provide a direction to C/ CSPs not to use or supply, or to cease using or supplying, carriage services if the use or supply is, or would be, prejudicial to security under existing section 581(3) of the Telecommunications Act (this Bill will move this power to new section 315A). The Attorney-General's directions powers under new section 315B will complement the existing power by providing a mechanism for a more proportionate and graduated response to managing security risks and promoting compliance with the security framework.

33. New section 315C of the Bill will grant the Secretary of AGD the power to obtain information and documents from C/CSPs, where that information is relevant to assessing compliance with the obligations imposed under subsections 313(1A) and (2A) of this Bill.

34. Under existing section 202B of the TIA Act, C/NCSPs have a requirement to notify the CAC of any changes to their systems or services which could have a material adverse effect on their ability to meet their obligations under section 313 of the Telecommunications Act. A new notification provision, section 314A, modelled on section 202B, will be created in Part 14 of the Telecommunications Act. The new provision will require carriers and carriage service providers nominated under the TIA Act (C/NCSPs) to notify the CAC of proposed changes to networks and services which could have a material adverse effect on the C/NCSPs ability to comply with the new security obligation in sections 313(1A) and 313(2A). The CAC will also be vested with the power to exempt C/NSCP's from compliance with the notification requirement in full or in part. It is envisaged that the CAC would grant an exemption based on a recommendation from ASIO that considered the security risk profile of a company or aspects of a company's business. C/NCSPs will also be provided with the option of submitting an annual Security Capability Plan (SCP) forecasting multiple proposed changes to their systems and services in lieu of individual notifications, and setting out matters that describe the company's security policies and practices and how it proposes to meet its new security obligation.

35. The ASIO Act will also be amended to include the directions power of the Attorney-General under section 315B within the definition of prescribed administrative action within Part IV. Currently, in respect of the existing direction power under subsection 581(3) the Attorney-General is not required to obtain advice from ASIO, but if he does and wishes to rely on such advice it must be in the form of a security assessment. Following amendment of the Telecommunications Act, the Attorney-General will be required to obtain an adverse security assessment from ASIO before he or she can exercise the existing directions power (new section 315A which replaces existing section 581(3)).

Human rights implications

36. The Bill engages the following human rights:

- the right to privacy (Article 17 of the International Covenant on Civil and Political Rights (ICCPR));
- the right to freedom of expression (Article 19 of the ICCPR);
- the right not to incriminate oneself (Article 14 of the ICCPR); and
- the right to a fair trial (Article 14 of the ICCPR).

Right to privacy – Article 17 of the ICCPR

37. Article 17 of the ICCPR provides that no one shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful attacks on his or her honour or reputation, and that everyone has the right to the protection of the law against such interference or attacks.

38. Interferences with privacy may be permissible, provided that they are authorised by law and not arbitrary. In order for an interference with the right to privacy not to be arbitrary, the interference must be for a reason consistent with the provisions, aims and objectives of the ICCPR and be reasonable in the particular circumstances.[1] The United Nations Human Rights Committee (the HRC) has interpreted 'reasonableness' in this context to mean that 'any interference with privacy must be proportional to the end sought and be necessary in the circumstances of any given case'.

39. The following measures in the Bill engage the right to privacy under Article 17 of the ICCPR:

- obligations for C/CSPs to protect networks and facilities from unauthorised access and interference under new subsections 313(1A) and (2A) of the Telecommunications Act; and

- information gathering powers granted to the Secretary of AGD under new section 315C.

Obligations of C/CSPs to protect networks and facilities

40. The new obligations for C/CSPs to protect networks and facilities from unauthorised access and interference under new subsections 313(1A) and (2A) of the Telecommunications Act will promote the right to protection against arbitrary and unlawful interferences with privacy in Article 17 of the ICCPR.

41. New subsection 313(1A) of the Telecommunications Act will require C/CSPs to do their best to protect telecommunications networks and facilities they own, operate or use from unauthorised interference or unauthorised access to ensure the confidentiality, availability and integrity of communications. New subsection 313(2A) will apply this obligation to networks and facilities used to supply carriage services by carriage service intermediaries. These measures seek to protect the increasing amounts of information, including personal information, stored electronically in telecommunications facilities and passed across networks. Information and networks are becoming increasingly vulnerable to interference and disruption by malicious actors. It is essential that legislation reflects and meets those new and advanced risks with protection of critical infrastructure and telecommunications data.

42. The Bill responds to the advances in the technologies available to state-based and non-state based actors with malicious intent toward sabotage and espionage that can expose the personal information of users. The Bill promotes the right to privacy under Article 17 by providing additional protections under law from interference with personal information through improved protection of telecommunications infrastructure to prevent unauthorised access.

43. The obligations for C/CSPs to protect networks and facilities under new sections 313(1A) and (2A) will also promote the privacy of telecommunications customers by strengthening the protection of telecommunications data retained under the data retention regime established by the *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015*. The new obligations will complement the data retention regime by

[1] *Toonen v Australia*, Communication No. 488/1992, U.N. Doc CCPR/C/50/D/488/1992 (1994) at 8.3.

improving the security of networks as a whole, thereby providing an additional layer of protection for retained telecommunications data. This Bill will implement recommendation 36 of the PJCIS in its advisory report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014, which was that the government enact the proposed telecommunications sector security reforms prior to the end of the implementation phase of the data retention regime to better protect telecommunications data.

Information gathering powers granted to the Attorney-General's Secretary and notification requirements

44. The right to privacy under Article 17 of the ICCPR will also be engaged by the notification requirements under sections 314A to 314D and the information gathering powers granted to the Secretary of AGD under new section 315C of the Telecommunications Act.

45. New sections 314A to 314D of the Telecommunications Act provide that C/NCSPs must notify the CAC of changes to their systems or services if they become aware that the changes are likely to have a material adverse effect on their ability to protect telecommunications networks and facilities from unauthorised access and interference.

46. New section 315C of the Telecommunications Act will provide that the Secretary of AGD may obtain from C/CSPs information and documents relevant to assessing compliance under new subsections 313(1A) and (2A). New section 315E enables the Secretary of AGD to inspect a document produced under section 315C and may make and retain copies as necessary. New section 315F empowers the Secretary of AGD to take possession of the original documents and keep them for as long as he or she deems necessary.

47. The information sought under new section 315C or provided under sections 314A to 314D will primarily be of a commercial nature and unlikely to interfere with the privacy of telecommunications customers in most cases. This information may include procurement plans, network or service design plans, tender documentation, contracts and other documents specifying business and service delivery models and network layouts. Subsection 315C(1) specifies that the information must be relevant to an assessment of the C/CSP's compliance with subsections 313(1A) or (2A). This requirement that the information must be relevant increases the likelihood that information obtained will be commercial. Information collected of a personal nature will be minimal and purely incidental to the key objective of assessing compliance. Information about end-users will be similarly incidental to the collection of commercial information under sections 314A to 314D or 315C, and in any event, these sections are not intended to target end-users.

48. To the extent that new sections 314A to 314D and 315C may result in the incidental collection of personal information, it will limit the right to privacy in Article 17. However, any collection of personal information would be lawful, would not be arbitrary and would be reasonable, necessary and proportionate to achieving a legitimate objective.

49. The requirements under new sections 314A to 314D and the power in new section 315C are necessary to ensure that the government will have the information needed to make an assessment regarding the C/CSP's compliance with its obligations. It is also necessary for the assessment of the risk to security, including the confidentiality of communications carried on, and of information contained on, telecommunications networks and the availability and integrity of telecommunications networks and facilities.

50. The power in new section 315C is reasonable and proportionate, as it is limited to the collection of information or documents that are relevant to the duties imposed on C/CSPs under new subsections 313(1A) and (2A) to do their best to protect networks and facilities from unauthorised access and interference. Subsection 315F(2) ensures that the person otherwise entitled to possession of a document that is taken is entitled to be supplied with a certified copy as soon as practicable. In addition, subsection 315F(4) provides that until a certified copy is supplied, the Secretary of AGD must permit the person (or a person authorised by the person) to inspect and make copies of the document.

51. Further, safeguards for the protection of personal information specified in the Australian Privacy Principles (APPs) under the the Privacy Act will apply to information gathered under sections 314A to 314D and 315C for any incidental personal information collected by the Secretary of AGD. This includes requirements regarding the security of personal information specified under Australian Privacy Principle 11 and requirements regarding use or disclosure under Australian Privacy Principle 6.

52. Under section 315G the Secretary of AGD may delegate his or her information gathering power to the Director-General of Security, ASIO. This delegation power is necessary to facilitate more efficient implementation of the regime. The power is reasonable and proportionate as it is limited to the Director-General, who will provide the appropriate seniority and expertise necessary to exercise this function.

53. In accordance with usual administrative law practices, the delegation must be in writing and specify to whom, or to what position the power is delegated. Also in accordance with administrative law practices, the Secretary of AGD may revoke the delegation at any time. Subsection 315G(2) contains a further protection in the exercise of the information gathering power by a delegate by enabling the Secretary of AGD to specify how the delegate is to exercise the power. The delegate must comply with any directions issued by the Secretary of AGD otherwise the exercise of the power will be invalid.

54. New section 315H of the Telecommunications Act will provide that a person who obtains information or a document under sections 314A to 314D and 315C may provide that information to another person under certain circumstances. Subsection 315H(1) provides that information may be shared either for the purpose of assessing the risk of unauthorised interference with, or unauthorised access to, telecommunications networks or facilities and to assess any such risk to security or for the purposes of security. To the extent that this information may include personal information, this provision also limits the right to privacy.

55. It is necessary that the Secretary of AGD be able to consult with officials in AGD, ASIO, and other relevant government agencies such as the Department of Communications and the Arts and the Australian Signals Directorate where technical expertise or assistance is required to assess risks to security. It may also be necessary to disclose information to the Attorney-General or other relevant Ministers for the purpose of exercising the Attorney-General's directions power in new section 315A (previously subsection 581(3)), new section 315B), or more broadly for the purposes of security.

56. Information obtained under sections 314A to 314D and 315C can also be shared for the purposes of security. 'Security' is defined in the ASIO Act, and includes the protection of the Commonwealth, states, territories and the people of Australia from espionage, sabotage, politically motivated violence, promotion of communal violence, attacks on Australia's defence system, or acts of foreign interference, as well as the protection of Australia's border

integrity. The ability to share the information for the purposes of security ensures that information can be shared with appropriate agencies to address identified security issues. It parallels the operation of the communication provisions contained in the ASIO Act, which authorise ASIO to communicate information it obtains for purposes relevant to security. This provision authorises the Secretary of AGD or their delegate (i.e. the Director-General of ASIO) to share this information for security purposes without first consulting or notifying the C/CSP. The fact that the information was relevant for security purposes would likely be highly sensitive and protected information in itself.

57. New section 315H also contains important protections governing how the information and documents obtained under either sections 314A to 314D and 315C (original purpose) and section 315H (secondary disclosure) is to be treated. Subsection 315H(3) provides that information and documents are to be treated as confidential. This would operate to complement the high standard for protecting information which government agencies already operate under including compliance with requirements under the Privacy Act regarding use, disclosure and destruction of personal information and secrecy obligations in the *Crimes Act 1914*. Importantly, subsection 315H(2) also prevents information which would identify the affected C/CSP from being disclosed to anyone who is not a Commonwealth Officer (as defined by subsection 315H(4)). This means that sensitive information about the company would be protected and only threat information relevant to protecting Australia's security interests will be shared.

58. The restrictions in section 315H will not override existing legislative provisions that authorise ASIO to communicate information obtained in the performance of its functions. Parliament has already set out the circumstances in which it is considered appropriate for an agency such as ASIO to be able to communicate information collected as part of the performance of its functions, including personal and other information collected under warrant.

Right to freedom of expression – Article 19 of the ICCPR

59. Article 19(2) of the ICCPR sets out the right to freedom of expression, including the right 'to seek, receive and impart information and ideas of all kinds' and extends to any medium, including written and oral communications, the media, public protest, broadcasting, artistic works and commercial advertising.

60. The following measures in the Bill engage the right to freedom of expression under Article 19 of the ICCPR:

- existing directions powers of the Attorney-General under subsection 581(3) of the Telecommunications Act (moved to new section 315A); and

- new directions powers of the Attorney-General under new section 315B of the Telecommunications Act.

61. Under existing section 581(3) the Attorney-General may direct a C/CSPs not to use or supply, or to cease using or supplying, a carriage service if he or she considers it is prejudicial to security. Item 12 of the Bill will amend the Act to move that power in its current form to section 315A of the Act. This is a technical amendment which does not change the substantive nature of the provision with the exception of adding an additional safeguard to remove the current exemption from review under the ADJR Act. Furthermore, it

will now also be clear on the face of the provision that a pre-requisite to the Attorney-General exercising the power to cease a service is the provision by ASIO of an adverse security assessment. These two changes will ensure consistency with the operation of the new direction power in section 315B.

62. Notwithstanding the fact that the Attorney-General's directions powers under new section 315A have not changed substantially (except to provide an additional safeguard and clarity) from the existing subsection 581(3), it is important to note that this power engages the right to freedom of expression under Article 19(2) as the ability of the Attorney-General to shut down a communications service may limit the right to freedom of expression in Article 19 of the ICCPR as it could reduce the availability of communications mechanisms to individuals.

63. Article 19(3)(b) of the ICCPR states that the exercise of the right to freedom of expression may be subject to certain restrictions if provided by law and if necessary for the protection of national security or public order. Existing subsection 581(3) of the Telecommunications Act, now moved to new section 315A, is provided by law and is necessary for the protection of national security and public order. It may only be exercised when the Attorney-General, after consultation with the Prime Minister and the Minister for Communications, considers that the proposed or continued use or supply of that carriage service would be or is prejudicial to security. 'Security' is defined in the ASIO Act to include the protection of the Commonwealth, states, territories and the people of Australia from espionage, sabotage, attacks on Australia's defence system, and acts of foreign interference. 'Prejudicial to security' is intended to have the same meaning as the term 'activities prejudicial to security' which is set out in the *Attorney-General's Guidelines in relation to the performance by the Australian Security Intelligence Organisation of its function of obtaining, correlating, evaluating and communicating intelligence relevant to security (including politically motivated violence).* The term is defined to mean activities that are relevant to security and which can reasonably be considered capable of causing damage or harm to Australia, the Australian people, Australian interests, or to foreign countries to which Australia has responsibilities.

64. The power of the Attorney-General to suspend supply of a carriage service is reasonable and proportionate as it has been designed for use in exceptional or extreme cases only to prevent harm to Australia's interests. In its existing form in subsection 581(3), the power to cease a service has never been used by the Attorney-General, in recognition of the potential impact on C/CSPs and end users. The Bill will amend subsection 581(3) to clarify that the power cannot be exercised unless it is on the basis of an adverse security assessment from ASIO. Subsection 581(3) is already included within the definition of prescribed administrative actions in subsection 35(1) of the ASIO Act which may be the subject of an ASIO qualified or adverse security assessment. The Bill will now effectively restrict the type of ASIO assessment that can be relied upon by the Attorney-General to suspend a carriage service to an adverse security assessment and expressly include the requirement within the provision vesting the Attorney-General with the power to cease a service (now section 315A). This will have the effect of increasing the threshold for exercising the power and make the requirement transparent on the face of the provision.

65. Further, introduction of the new power of the Attorney-General to give directions to C/CSPs in new section 315B is intended to reduce the need to rely on the existing powers under subsection 581(3) of the Telecommunications Act. This new power enables the Attorney-General to take a more proportionate response to a security risk posed by a C/CSP.

Section 315B provides the Attorney-General with the option to give a written direction requiring a C/CSP to do, or refrain from doing, a specified act or thing within the period specified in the direction.

66. The power in 315B is intended to be used in a cooperative way alongside engagement with industry. While it is an intrusive power, a number of protections and safeguards have been included to ensure that it is only used where absolutely necessary (including in circumstances where the C/CSP itself requests a direction) and the threshold for its exercise is high.

67. Subsection 315B(1) provides that the Attorney must be satisfied that there is a risk of unauthorised access or unauthorised interference and that the risk is *prejudicial* to security. As noted above, prejudicial is associated with a concept of harm or damage to Australia's security interests.

68. Second, the power cannot be exercised without an adverse security assessment or negotiating with the relevant C/CSP in good faith. Both sections 315A and 315B require the Attorney-General to obtain an adverse assessment prior to exercising the relevant power, which ensures that he or she is provided with specific security advice in making a decision, and that ASIO makes a recommendation that adverse action should be taken. An adverse security assessment is defined in section 35 of the ASIO Act and means a security assessment made by ASIO in respect of a person (including a company) that:

- contains any opinion or advice, or any qualification of any opinion or advice, that is or could be prejudicial to the interests of the person, and

- recommends that prescribed administrative action be taken or not taken in respect of that person (e.g. the exercise of one of the listed legislative powers in relation to the affected person), which would of be prejudicial to the interests of that person.

69. Third, subsection 315B(5) clarifies that the exercise of the directions power is to be a measure of last resort where all efforts to reach agreement cooperatively have failed. The Attorney-General must not give a C/CSP a direction unless the Attorney-General is satisfied that all reasonable steps to negotiate measures to reduce or eliminate the risk have been negotiated in good faith. The requirement to act in good faith means that attempts to reach agreement must be genuine. Government agencies will need to have taken adequate steps to engage the C/CSP, listen to the C/CSP's concerns and work with the C/CSP to develop mitigation measures reasonably necessary for addressing the risk.

70. In addition, subsection 315B(5) limits the purpose for which the Attorney-General can issue a direction to be for the purpose of reducing or eliminating the risks identified in subsection 315B(1). The direction must therefore specifically direct action that seeks to reduce or eliminate the risk of unauthorised access or interference which would otherwise result in a risk to security.

71. There are also a number of safeguards included to ensure that the exercise of the power does not unnecessarily impinge the right to freedom of expression and is not exercised arbitrarily. These include:

- Listing the matters which the Attorney-General must have regard to when exercising the power. Section 315B stipulates that the Attorney-General may only issue a direction to a C/CSP if he or she has had regard to the cost and impact on the C/CSP of implementing the direction, as well as the impact on customers, the market, competition and innovation. This is an inbuilt protection for customers using telecommunications networks in that their market choices are no more restricted than is necessary.

- Imposing mandatory consultation requirements. The Attorney-General will be required to consult both the Minister for Communications and the affected C/CSP. Consultation with the Minister will further ensure that security considerations do not unnecessarily impede market innovation and business autonomy. The requirement to consult the affected C/CSP will further ensure the direct impact on the C/CSP is taken into account and the C/CSP is given a voice to explain their position on why they cannot agree to implement ASIO's security advice.

Right not to incriminate oneself – Article 14 of the ICCPR

72. Article 14 of the ICCPR provides for the right to a fair hearing and includes in 14(3)(g) the right of protection against self-incrimination. The right to be free from self-incrimination may be subject to permissible limitations provided that the limitations are for a legitimate objective, and are reasonable, necessary and proportionate to that objective.

73. New subsection 315D(1) of this Bill abrogates the privilege against self-incrimination as it provides that a person is not excused from giving information or a document under new section 315C on the ground that the information or document might tend to incriminate the person or expose the person to a penalty.

74. The information gathering powers under section 315C of this Bill are modelled on similar powers under section 521 of the Telecommunications Act. The existing powers also abrogate the privilege against self-incrimination under section 524.

75. Abrogation of the privilege in this circumstance is necessary as there are no other appropriate avenues for collecting the information needed by the regulator to assess compliance with the obligation to protect networks and facilities under subsections 313(1A) and (2A). The information-gathering powers of the Secretary of AGD under section 315C form a core part of the telecommunications security framework that will be established by this Bill and would be significantly impaired if persons were excused from providing self-incriminating information.

76. However, subsection 315D(2) will provide both a use and derivative use immunity to the individual who provides information or documents under section 315C. As such, the information and documents obtained through this mechanism will be inadmissible, as well as any evidence obtained as a direct or indirect consequence of the documents or information being provided, in any criminal proceedings against the person (except proceedings under sections 137.1 and 137.2 of the Criminal Code), or civil proceedings, with the exception of a proceeding to enforce the information gathering power itself. These are very narrow exceptions to an otherwise broad immunity. In this regard, section 315D is reasonable and proportionate for monitoring compliance with the duty in subsections 313(1A) and (2A). The common law privilege against self-incrimination only extends to natural persons, not to bodies corporate. This is well-established in common law, as outlined in the

Attorney-General's Department's 2011 *A Guide to Framing Commonwealth Offences, Infringement Notices and Enforcement Powers.*

77. Subsection 315C(3) will deem it mandatory for a person to comply with the information gathering power under section 315C. Section 570 of the Telecommunications Act provides that pecuniary penalties may be issued against a person for contravention of the Act, including new subsection 315C(3). Hence only when the proceedings at hand arise directly from the refusal or failure to provide information, would that information be admissible as evidence against that person. This is a similarly narrow exception.

78. The protections in Article 14(3) of the ICCPR include minimum guarantees that are applicable in criminal proceedings. However, in some cases it is possible for a civil penalty which subjects a person to a high penalty and is intended to be punitive or deterrent in nature to constitute a 'criminal charge' for the purposes of the prohibition on the right to be free from self-incrimination under Article 14(3). The Secretary of AGD may institute a proceeding for the recovery of a pecuniary penalty relating to a contravention of subsection 315C(3) regarding compliance with a written notice given to a C/CSP to give the Secretary of AGD information or documents. The pecuniary penalties for contraventions of civil penalty provisions are specified in section 570 of the Telecommunications Act, which is that the maximum amount that could be payable would be $10m for a body corporate and $50 000 for a natural person.

79. The threshold for exercising the information gathering power is relatively high. Espionage and sabotage through cyber-attacks targeting Australia's telecommunications networks and facilities have the potential to cause considerable damage to Australia's national interest. This includes damage to businesses and individuals where commercially sensitive information or personal information is accessed.

80. The Secretary of AGD must have reason to believe the C/CSP has information relevant to assessing compliance with the duty. This is to protect against general fishing expeditions, by imposing a state of mind test and a relevance test. Monitoring compliance is critical as the impact of non-compliance can have significant national security implications.

81. The penalties are also reasonable and proportionate measures to encourage compliance as they are consistent with the existing penalties for non-compliance by carriers and carriage service providers under the Telecommunications Act. The threshold of $10m applies to a breach of any carrier licence condition or service provider rule, which includes a breach of the Telecommunications Act. Enforcement action and the penalty regime will only be activated as a last resort, where national security outcomes are not able to be achieved through cooperative engagement.

Right to a fair trial – Article 14 of the ICCPR

82. The right to a fair trial is protected in Article 14 of the ICCPR and is aimed at ensuring the proper administration of justice by upholding, among other things, the right to a fair hearing.[2] The Bill engages and supports the right to a fair trial through the availability of judicial review of all decisions and merits review of ASIO security assessments.

[2] UN Human Rights Committee, General Comment No 13 (1984).

83. This Bill will remove an existing exemption of the Attorney-General's directions powers under subsection 581(3) of the Telecommunications Act (new section 315A) from review under the ADJR Act.

84. The Bill does not seek to limit the principles of procedural fairness within administrative law, available as recourse to a C/CSP by virtue of the new and existing directions power of the Attorney-General. The legislation will require the Attorney-General to consult the affected C/CSP before a direction is issued, notifying it of the proposed direction and providing a minimum of 28 days (unless circumstances are urgent) to provide a written response which must be taken into account in issuing a direction.

85. Further, there are a number of other thresholds and safeguards built in to the exercise of the directions power. These are set out above in paragraphs 67 to 71. As noted in paragraph 68 the directions powers can only be exercised in circumstances where ASIO has provided an adverse security assessment. Not only does this increase the threshold for the exercise of the powers, it also attracts the accountability protections associated with a security assessment in Part IV of the ASIO Act, which provide for merits review of the assessment in the Security Appeals Division of the Administrative Appeals Tribunal (AAT).

86. Part IV also provides notification obligations which require the recipient of the assessment, in this case, the Attorney-General, to provide the affected party with a copy of the security assessment within 14 days. In accordance with section 38A of the ASIO Act, the security assessment might be redacted to remove information that would be prejudicial to the interests of security before being provided to the affected party. The security assessment must be accompanied by an unclassified statement of grounds setting out the information ASIO has relied upon and a written notice informing the affected party (the C/CSP) of its right to apply to the AAT for merits review of the security assessment.

Conclusion

87. The Bill is compatible with human rights because it will promote rights and, to the extent that the Bill may also limit rights, those limitations are reasonable, necessary and proportionate to the objective of ensuring telecommunication networks and facilities are appropriately protected.

NOTES ON CLAUSES

Clause 1 – Short title

88. Clause 1 provides for the short title of the Act to be the *Telecommunications and Other Legislation Amendment Act 2016*.

Clause 2 – Commencement

89. Clause 2 sets out when the various parts of the Act will commence as described in the table.

90. Item 1 in the table provides that sections 1 to 3, which concern the formal aspects of the Act, will commence (i.e. come into effect) on the day the Act receives Royal Assent.

91. Item 2 in the table provides that Schedule 1, which amends the *Telecommunications Act 1997* (Telecommunications Act), the *Telecommunications (Interception and Access) Act 1979* (TIA Act), the *Administrative Decisions (Judicial Review) Act 1977* (ADJR Act) and the *Australian Security Intelligence Organisation Act 1979* (ASIO Act) will commence 12 months after the date of Royal Assent.

Clause 3 – Schedules

92. Clause 3 provides that each Act specified in a Schedule to this Act is amended or repealed as set out in the Schedule. Any other item in a Schedule to this Act has effect according to its terms. This is a technical provision to give operational effect to the amendments contained in a Schedule.

SCHEDULE 1 - AMENDMENTS

PART 1 – MAIN AMENDMENTS

Overview of measures

93. Part 1 of Schedule 1 will insert new provisions into Part 14 of the Telecommunications Act which concerns national interest matters. In particular:

- a new security obligation will be added to the existing law enforcement obligation in section 313 of the Telecommunications Act to require carriers, carriage service providers and carriage service intermediaries (C/CSPs) to protect networks and facilities they own, operate or use from unauthorised access and interference;

- a notification requirement, modelled on section 202B of the TIA Act, will be created in Part 14 which will oblige carriers and some carriage service providers to notify of proposed changes to systems and services which are likely to have a material adverse effect on the carriers and nominated carriage service providers' (C/NCSPs) ability to comply with the new security obligation in sections 313(1A) and 313(2A) (in other words, to protect network and facilities from unauthorised access and interference). Provision is also made for a C/NSCP to be exempted, in full or in part, from the notification requirement based on ASIO's assessment of

the risk profile of the C/NCSP or aspects of the C/NCSP's business. C/NCSPs will also be provided with the option of submitting a SCP forecasting multiple proposed changes to their systems and services in lieu of individual notifications, and setting out matters that describe the company's security policies and practices and how it proposes to meet its new security obligation. It would provide a greater degree of certainty for the company that it is meeting the government's national security expectations (although would not amount to approval of policies or immunity from any obligations);

- the Secretary of AGD will be vested with an information gathering power to facilitate compliance monitoring and investigations of the new security obligation;

- the Attorney-General will be provided an additional directions power to direct a C/CSP to do or not do a specified thing (for example, alter a procurement that has been assessed as giving rise to security risks);

- additional safeguards will be added to the Attorney-General's existing directions power in subsection 581(3) and the provision will be relocated within the Act to place the national security related provisions within the same part of the Act; and

- the existing civil remedies regime provided for in Part 30 (injunctions), Part 31(civil penalties), and Part 31A (enforceable undertakings) will be made available for taking enforcement action to address non-compliance with the security obligation, a direction, or notice to produce information or a document. The Attorney-General would be authorised to commence proceedings to seek these remedies.

94. The TIA Act will be amended so that the notification requirement in section 202B of that Act will not be invoked by the new obligations in subsections 313(1A) and 313(2A) of the Telecommunications Act.

95. The ASIO Act will be amended so that the exercise of the new directions power in section 315B will be included in the list of prescribed administrative actions in subsection 35(1) of the ASIO Act. This will enable ASIO to provide security assessments in respect of the exercise of the new directions power to the Attorney-General. The definition of prescribed administrative action in the ASIO Act will also be amended to reflect the repeal of subsection 581(3) to relocate it in new section 315A.

Item 1 – Section 5

96. Section 5 provides a simplified outline of the Telecommunications Act. Item 1 amends Section 5 by including a reference to the new security obligations to protect networks from unauthorised interference or unauthorised access in the simplified outline for the Act.

Item 2 – Section 7

97. Item 2 inserts new definitions for the following eight terms into section 7 for the purpose of the new security scheme: adverse security assessment, Attorney-General's Department, Attorney-General's Secretary, Director-General of Security, nominated carriage service provider, notifiable equipment, telecommunications service and telecommunications system. The definitions are self-explanatory. An adverse security assessment is defined in

section 35 of the ASIO Act and means a security assessment made by ASIO in respect of a person (including a company) that contains:

- any opinion or advice, or any qualification of any opinion or advice, that is or could be prejudicial to the interests of the person, and

- a recommendation that prescribed administrative action be taken or not taken in respect of that person, being a recommendation the implementation of which would be prejudicial to the interests of the person.

Item 3 – After subsection 105(5A)

98. Item 3 provides that the telecommunications regulator (the Australian Communications and Media Authority (ACMA)) is not required to monitor or report each financial year to the Minister on the operation of the provisions in this Bill (instead the Secretary of AGD will report annually on the operation of the provisions). It does so by providing that paragraph 105(5A)(a) does not apply in relation to Part 14 of the Act to the extent that it has been amended by this Bill and by inserting new section 315J.

Item 4 – Before section 311

99. Item 4 inserts the heading 'Division 1–Simplified Outline' into 'Part 14 – National interest matters' of the Telecommunications Act to apply consistent drafting conventions.

Items 5 and 6 – Section 311 and at the end of section 311

100. Section 311 outlines the key provisions in Part 14 of the Act. Items 5 and 6 amend section 311 to also include a reference to the new security obligations, as well as the directions powers of the Attorney-General and the information-gathering powers of the Secretary of AGD.

Item 7 – Before section 312

101. Item 7 inserts the heading 'Division 2–Obligations of ACMA and carriers and carriage service providers' to apply consistent drafting conventions.

Item 8 – After subsection 313(1)

102. Item 8 inserts a new subsection (subsection 313(1A)) into section 313 to establish a new obligation for C/CSPs to protect telecommunications networks and facilities they own, operate or use from unauthorised interference or access for the purposes of security. Section 313 already imposes obligations on C/CSPs to: (1) do their best to prevent networks and facilities being used to commit offences; and (2) to provide reasonable assistance to authorities for the purposes of enforcing criminal and pecuniary laws, protecting public revenue and safeguarding national security.

103. The new security obligation will also apply universally to all C/CSPs to require all network operators and service providers to actively manage security risks to telecommunications services and infrastructure. The obligation to do their best to protect networks and facilities from unauthorised access and interference is limited to protecting Australia's national security interests. In other words, the inclusion of the words 'for the purposes of security' in subsection 313(1A) clarifies that the purpose of the obligation is to

protect the integrity and availability of networks and facilities and the confidentiality of information stored and carried across them from threats such as espionage, sabotage, and foreign interference. The note under section 313(1A) clarifies that that the terms 'unauthorised access' and 'unauthorised interference' are to be read within the meaning of 'security' as defined in the ASIO Act with particular reference to security threats of espionage, sabotage and interference. This in no way limits the scope of the meaning of 'security' as defined in the ASIO Act, rather it highlights the security threats of most relevance.

104. The obligation is framed in terms of the C/CSP doing 'its best' to protect networks from unauthorised interference or unauthorised access. This is consistent with the existing obligations in section 313 and avoids imposing an absolute obligation. In other words, compliance with the obligation requires C/CSPs to take all *reasonable steps* to prevent unauthorised access and interference for the purpose of protecting the confidentiality of information 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.

105. It encourages a risk based approach to managing risks of espionage, sabotage and foreign interference rather than imposing absolute liability. For example, the cost of implementing controls should be balanced against the harm to security interests if the risk is not adequately managed. Security threats and risks are ever evolving, as are the capabilities of those who wish to gain access to sensitive parts of telecommunications systems and undertake activities contrary to our national interest or law. Despite best efforts, it may not be possible to prevent every instance of unauthorised access and interference. As such, evidence of unauthorised access to, or interference with, a network would not necessarily constitute a breach of the security obligation.

106. Importantly, while the obligation applies universally to all C/CSPs, the requirement to do their best imposes a subjective element which means that what is required to comply with the obligation will differ according to the risk profile of the C/CSP. Not all networks and facilities will pose the same level of risk to security or will be as actively targeted by malicious actors. However, it is important that all parts of the sector take proactive steps to secure the networks and facilities they own, operate or use from unauthorised access and interference to harden the entire Australian telecommunications network against security threats, such as espionage, sabotage and foreign interference activities. The following factors will contribute to whether a C/CSP is more likely to be actively targeted and therefore have an increased risk from espionage, sabotage or foreign interference:

- percentage of market share – the larger the customer base the greater the aggregated data;

- sensitivity of customer base – some customers will have more information of a sensitive nature being communicated and held on networks and facilities than others – including government and critical service providers, science and research organisations, large or significant commercial organisations, and large healthcare provider organisations (or their suppliers and business partners); and

- criticality of the network – for example, where the telecommunications network or service supports the delivery of other critical services, such as power, water, health, banking or where it provides services to critical customers.

107. Not all parts of networks and facilities are equally vulnerable to national security risks. Some parts of networks and facilities are generally considered to be more sensitive and at a greater risk of intrusion and interference than other parts because they either house or carry sensitive communication and information (e.g. billing systems and lawful interception systems) or because they affect the availability and integrity of the network (e.g. operations support systems). These areas of greater security interest are:

- network operation centres, including infrastructure used to facilitate support of the network;
- lawful interception equipment or operations;
- any part of a telecommunications network that manages or stores:
    - aggregated information about customers
    - aggregated authentication credentials of a significant number of customers
    - administrative (privileged user) authentication credentials for the network or related systems
- any place in a telecommunications network where data belonging to a customer or end user aggregates in large volumes, being either in transit or stored data; and
- any additional area as advised in writing, in response to changes in threat, technology and business practices.

108. The parts considered more vulnerable are likely to change over time due to changes in the way networks and services are operated and delivered. For this reason, administrative guidelines will outline what is expected of C/CSPs to comply with the security obligation based on whether they have a low, medium or high risk profile and the parts of networks and facilities considered most vulnerable to national security risks. This advice and guidance will assist C/CSP to implement a risk managed approach to meeting the security obligation.

109. In terms of compliance, a C/CSP will be expected to be able to demonstrate that it has implemented effective security practices and measures to manage risks of unauthorised access and interference to protect the confidentiality of communications stored on and carried across networks (i.e. manage the risk of espionage) and ensure the availability and integrity of networks (i.e. guard against sabotage activity). For example, a C/CSP would need to take reasonable steps to ensure that intrusions or breaches do not occur within networks or facilities that they own, use or operate, and that the potential for malicious activity is minimised, demonstrable by the security controls in place. This will be particularly relevant where activity, left unchecked, could provide opportunity to compromise the confidentiality, availability or integrity of telecommunications infrastructure or information carried by, or across it.

110. While the security obligation will have immediate effect from the expiry date of the implementation period, existing networks and facilities in place at the time the security obligation comes into effect that are non-compliant will not be subject to civil penalties for non-compliance with the security obligation to protect networks and facilities under

subsections 313(1A) and (2A). C/CSPs are not expected to retrofit all 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 seek to work with the provider to develop cost effective solutions to better manage the risks posed by the existing vulnerability. Subject to how serious the security risk is and how willing the C/CSP is to collaborate with government to manage the risk, the Attorney-General could issue a direction requiring mitigation measures to be implemented.

111. The Bill does not prescribe what technical solutions a C/CSP should use to secure networks to protect information or the integrity and availability of the network, as this will be highly dependent on factors specific to each network and business delivery model. Mitigation measures required to secure networks will be particular to each network. There will be degrees of risk that vary across networks and providers. However, as specified in subsection 313(1B), from a compliance perspective a C/CSP will be expected to demonstrate *effective control* and *competent supervision* over the networks and facilities that are owned or operated by the C/CSP, targeted at addressing vulnerabilities that can arise through equipment supply, outsourcing and offshoring arrangements. Subsection 313(1B) is not intended to otherwise limit the potentially broad scope of the obligation to just addressing risks that arise through ineffective control and incompetent supervision arrangements.

112. The term 'competent supervision' means the ability of a C/CSP to maintain proficient oversight of its networks and facilities and could include arrangements to maintain:

- visibility of network and facility operations;
- visibility of key data flows and locations;
- awareness of parties with access to network infrastructure; and
- the ability to detect security breaches or compromises.

113. The term 'effective control' in this context means the ability of the C/CSP to maintain direct authority and/or contractual arrangements which ensure that networks, facilities, infrastructure and information stored or transmitted within networks, is protected from unauthorised interference. This would include authority over all parties with access to network infrastructure and data. It could include the ability to:

- direct actions to ensure the integrity of network operations and the security of information carried on them;
- terminate contracts without penalty where there has been a security breach or data breach reasonably attributable to the contracted services or equipment;
- address issues of data sovereignty;
- 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 unauthorised access has occurred (for example to confirm accuracy of information or data holdings).

114. A key vulnerability for unauthorised access and interference arises through the telecommunications supply chain. Therefore, the concepts of effective control and competent supervision are largely directed at ensuring C/CSPs build security considerations into their arrangements with suppliers of equipment, services and support arrangements, particularly where data and/or service delivery operation or support is to be provided from offshore locations. For example, if a C/CSP is using a supplier or managed service arrangement, or has outsourced elements of its enterprise such as data hosting, the C/CSPs will need to consider the controls it has in place, or is proposing to put in place, to manage who can access and control sensitive parts of the network. If a C/CSP is engaged in offshore arrangements, one of the key risks it would be expected to consider is the legislative environment in the particular country and whether offshoring particular parts of their business may mean that personal information about Australians, as well as sensitive commercial information or communications, may have to be provided to a foreign government under a lawful request. These reforms are not about preventing offshoring. However, C/CSPs would be expected to take a risk based approach to considering which parts of networks, facilities, systems and operations should be offshored.

115. More broadly, demonstrating best efforts to secure networks would include as a minimum, ensuring mechanisms for facilitating corporate awareness of the broad national security vulnerabilities and risks posed to telecommunications networks and embedding security considerations in to business decision-making and business delivery models. In this regard, the obligation is intended to encourage C/CSPs to regularly and proactively engage with ASIO and AGD to inform themselves of these risks and develop strategies for managing those risks. Further guidance on particular areas of vulnerability and possible measures and controls to mitigate associated risks will be provided in the form of administrative guidelines to be developed in consultation with C/CSPs. It is expected that C/CSPs will familiarise themselves with the guidance material and, where in doubt, seek advice from the AGD and/or ASIO.

116. Paragraph 313(1A)(c) requires C/CSPs to protect the confidentiality of information carried across and stored on telecommunications networks and facilities, through the protection of those networks and facilities themselves. Many C/CSPs are already required to comply with the obligations in the APPs contained in the Privacy Act, including APP6 regarding use or disclosure of personal information, APP8 regarding cross-border disclosure of personal information and APP11 which requires that they take reasonable steps to protect personal information they hold from misuse, interference and loss, and from unauthorised access, modification or disclosure. While there are similarities between C/CSPs' obligations under APP11 and the obligation under paragraph 313 (1A)(c), there are a number of differences, including:

- subsection 313(1A) has as its objective the protection of all information, not just personal information, to ensure that sensitive government and commercial information is also protected; and
- the steps a C/CSP will be required to take under subsection 313(1A) focus on protecting the information 'for the purposes of security', whereas APP11 is concerned with protecting individual's privacy.

117. Importantly, while there may be overlap between the steps that a C/CSP might take under subsection 313(1A) and APP 11, steps taken to comply with one obligation will not necessarily mean that the C/CSP has complied with the other obligation. For example, while subsection 313(1A) is focused on protecting a broader range of information from threats such as espionage, sabotage, and foreign interference through the protection of a C/CSP's networks and facilities, APP11 is focused only on personal information, but requires C/CSPs to consider broader sources of risks to information – a C/CSP must take reasonable steps to protect it from any misuse, interference and loss and from any unauthorised access, modifications or disclosure.

118. Guidance produced by agencies such as ACMA and the Office of the Australian Information Commissioner to assist entities comply with their obligations to protect the security of personal information will also assist C/CSPs to meet their obligations to protect the confidentiality of information under paragraph 313(1A)(c). However, C/CSPs will also need broader approaches to protect all categories of information, such as commercial-in-confidence and sensitive government information.

Item 9 – After subsection 313(2)

119. Item 9 mirrors the obligation under Item 8, although new subsection 313(2A) applies specifically to carriage service intermediaries. This is consistent with the application of existing obligations in section 313 and ensures that all parts of the telecommunications sector are taking responsibility for protecting telecommunications networks and facilities.

120. Item 8 does not include a similar provision to subsection 313(1B) in recognition of the fact that not all carriage service intermediaries would be able to demonstrate effective control and competent supervision of networks and facilities. Similarly to Item 8, the obligation for carriage service intermediaries to 'do their best' to protect telecommunications networks and facilities will depend on what steps are reasonable in particular circumstances (taking into account the extent that an intermediary can influence security outcomes in a particular situation). For example, an intermediary may be given access to services that may provide them with information about security vulnerabilities. They would therefore be expected to have appropriate procedural, governance and contractual arrangements to secure this type of information so that this knowledge of security vulnerabilities cannot be accessed by other parties and exploited.

Items 10 and 11 – Paragraph 313(5)(a) and at the end of subsection 313(5)

121. Items 10 and 11 extend the operation of the existing protections in subsection 313(5) of the Telecommunications Act to actions undertaken by a C/CSP to comply with the new security obligation in sections 313(1A) and 313(2A) and/or with a direction issued by the Attorney-General under either sections 315A or 315B. This means that a C/CSP is not liable to any action or proceedings for damages for an act done or omitted in good faith, if that act or omission was in the performance of a duty imposed by the new obligation of subsection 313(1A) or 313(2A) or in compliance with a direction issued by the Attorney-General.

122. In other words, the provision provides a C/CSP with a broad protection from any liability to a third party for any damage caused by negligence or breach of contract arising from the C/CSP acting or not acting in the course of performing its duties under the security

obligation or pursuant to a direction given by the Attorney-General under new sections 315A or 315B. The most likely remedy that would be sought in such circumstances is damages.

123. Subsection 313(6) provides that this protection extends to all officers, employees and agents of a carrier/carriage service provider.

124. Although the immunity would not prevent third parties from commencing an action or proceedings for damages, the C/CSP would be able to rely on the protections under subsections 313(5) and (6) to defeat an alleged liability.

Item 12 – After section 314

Division 3 – Notification of changes to telecommunications services or telecommunications systems relating to obligation under subsections 313(1A) or (2A)

125. Item 12 will insert the heading Division 3 after an existing provision in Part 14, section 314 to apply consistent drafting conventions.

Subdivision A – Individual notifications

126. Section 314A will insert a new notification requirement in the Telecommunications Act. Section 314A will oblige C/NCSPs nominated under the TIA Act to notify the CAC of planned changes to telecommunications services or systems which the C/NCSP has become aware are likely to have a material adverse effect on the capacity of the C/NCSP to meet its security obligation under the new subsections 313(1A) and (2A) of the Telecommunications Act to protect telecommunications networks and facilities from unauthorised access and interference. '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 TIA Act.

127. Section 314A is modelled on the existing notification requirement in section 202B of the TIA Act, which requires C/NCSPs to notify the CAC of planned changes to telecommunications systems and services which are likely to have a material adverse effect on the ability of the C/NCSP to meet its obligations under the TIA Act or section 313 of the Telecommunications Act. This Bill will exclude the new security obligations under subsections 313(1A) and (2A) of the Telecommunications Act from operation of the existing notification requirement in section 202B of the TIA Act so there is no duplication between the notification requirements.

128. The notification requirement is one method of formalising information sharing between C/NCSPs and the government and is triggered at the time of planning proposed changes to networks and services, rather than following implementation. Although the legislation does not specify when a C/NCSP should notify government of changes, it is in the C/NCSP's best interests to notify of a proposed change as early as possible in the design and planning stage and prior to finalising arrangements to implement the change. For example, the stage at which a detailed business case is being prepared for the company Board for decision might provide a guide for the appropriate time in the planning process for notifying the CAC. This will allow security considerations to be built into the proposal in the most cost effective manner and provide the Board with a more realistic understanding of all aspects of the proposal and associated security costs. Administrative guidelines will provide detailed

advice on when a C/NCSP should notify of proposed changes. Early, close and regular engagement with security agencies will also assist C/NCSPs to assess the types of changes that must be notified and at what stage of the planning and decision making process.

129. Even the most informed C/NCSP is unlikely to have access to the most up to date threat information available to ASIO. Early engagement with government during the planning and design stage of changes to networks may help the C/NCSPs to mitigate security risks in the most cost-effective manner. Further, notification early in the procurement process can avoid unnecessary delay in the progress of procurements and minimise costs associated if procurement plans need to be modified to address security concerns.

Kinds of changes

130. The requirement to notify arises only from a change to a system or service, not from existing operations. Section 314A outlines the types of changes in arrangements that should be notified to government, which include but are not limited to: outsourcing or offshoring arrangements affecting sensitive parts of a network and/or procuring new equipment or services for sensitive parts of a network, and changes to the management of services. This is not an exhaustive list and may include other types of changes.

131. Like section 202B of the TIA Act the requirement to notify is only triggered where a proposed change is likely to have a 'material adverse effect'. This means that the proposed change may have an actual or measurable negative impact on the ability of the C/CSP to comply with the duties in subsections 313(1A) or 313(2A) to protect networks from risks of unauthorised access and unauthorised interference.

132. The notification requirement is only triggered where the C/NCSP 'becomes aware' that the implementation of a proposed change is likely to have a material adverse effect on the capacity of the C/NCSP to protect telecommunications networks and facilities. This is in recognition of the fact that C/NCSPs are well-placed through their practices and processes to identify risks associated with proposed changes. However, C/NCSPs would be expected to also make themselves aware of guidance issued by AGD and information provided by security agencies, as appropriate, when assessing whether a proposed change is likely to have national security implications.

133. Not all parts of networks and facilities are equally vulnerable to security risks. Some parts of networks and facilities are generally considered to be more sensitive and at a greater risk of intrusion and interference than other parts because they either house or carry sensitive communication and information (e.g. billing systems and lawful interception systems) or because they affect the availability and integrity of the network (e.g. operations support systems).

134. In particular, C/NCSPs would be expected to notify the CAC when they are planning changes to these more sensitive or vulnerable parts of networks. The parts considered more vulnerable are likely to change over time due to changes in the way networks and services are operated and delivered. Administrative guidelines will outline what is expected of C/CSPs to comply with the notification obligation under section 314A.

Exemptions

135. 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 application process for C/NCSPs – instead the CAC will decide if and when to grant any exemption and write to the affected C/NCSP advising of the decision to grant the exemption. The exemption may be a complete exemption from the operation of this section made under subsection 314A(4) (i.e. the C/NCSP does not have to notify the CAC of any planned changes to telecommunications systems or services) or a partial exemption made under subsection 314A(5). For example, a partial exemption may be given in relation to certain categories of changes or in respect of particular parts of the C/NCSP's business. For instance, a large carrier which offers a number of different types of services, may be exempted from providing any notifications in relation to a part of their business (for example, a subscription television service), but would still be required to notify of changes to other parts of their business. The details of a partial exemption would be specified in a notice provided to the C/NCSP.

136. In practice, the CAC's decision to grant a full or partial exemption will be based on advice from ASIO that takes into account the security risk profile of a company. ASIO's assessment of security risk will be based on a number of factors such as:

- percentage of market share – the larger the customer base the greater the aggregated data;

- sensitivity of customer base – some customers will have more information of a sensitive nature being communicated and held on networks and facilities than others – including government and critical service providers, science and research organisations, large or significant commercial organisations, and large healthcare provider organisations (or their suppliers and business partners); and

- criticality of the network – for example, where the telecommunications network or service supports the delivery of other critical services such as power, water, health, banking or where it provides services to critical customers.

137. While the process for issuing an exemption will be by way of issuing individual exemptions, it is envisaged that classes of providers may be exempt from the notification requirement on the same grounds, for example, exemptions may relate to a particular type of low risk service or network operator based on the factors identified above.

138. The CAC may revoke or amend an exemption made under subsections 314A(4) or (5) in line with subsection 33(3) of the *Acts Interpretation Act 1901,* which specifies that the power to make an instrument of a legislative or administrative character also includes the power to vary or revoke that instrument. Again, a decision to vary or revoke an exemption will likely be based on advice from ASIO having regard to any changes to security risks and services offered by the C/NCSP and the national security threat environment.

139. The statement in subsection 314A(7) that an exemption granted under subsections 314A(4) or (5) is not a legislative instrument is declaratory of the law and included to assist the reader. It does not represent a substantive exemption from the requirements of the *Legislative Instruments Act 2003*.

Assessment of proposed change

140. Section 314B specifies the assessment processes for proposed changes following notification under subsection 314A(3). When the CAC receives a notification under this section he or she will generally consult ASIO for the purposes of assessing any potential security risks associated with the proposed change.

141. In all circumstances following notification the C/NCSP will receive one of the following notices from the CAC:

- request under subsection 314B(1) for further information about the planned change so the CAC can assess whether there is a risk of unauthorised access to, or interference with, telecommunications networks or facilities; or

- notice under subsection 314B(3) advising the C/NCSP of a risk associated with the planned change of unauthorised access to, or interference with, telecommunications networks that is prejudicial to security; or

- notice under subsection 314B(5) advising that the CAC is satisfied there is not a risk from the planned change of unauthorised access to, or interference with, telecommunications networks or facilities that is prejudicial to security.

142. Subsection 314B(6) provides that a C/NCSP will be provided with a notice under subsection 314B(3) or (5) within 30 days of notifying the CAC of a proposed change. However, if the CAC has sought further information under subsection 314B(1), the C/NCSP will be provided with a notice as soon as practicable and within 30 days of providing the further information.

143. There are no penalties associated with non-compliance with a request for further information made under subsection 314B(1). Therefore if a C/NCSP did not comply with a request made by the CAC under this section, the Secretary of AGD may consider use of his or her new information gathering powers under section 315C of the Telecommunications Act.

144. The provision does not prevent a C/NCSP from implementing the proposed change within the 30 day period specified for the CAC to assess the proposed change or following a notice provided to the C/NCSP by the CAC under subsection 314B(3). However, as inferred in paragraphs 314B(3)(d) and (e), if a proposed change poses security risks and is implemented without any steps taken to manage this risk the C/NCSP will be potentially acting in contravention of its duties in subsections 313(1A) and (2A).

145. In circumstances where the CAC notifies the C/NCSP that a proposed change poses security risks, the CAC (on advice of ASIO) may also advise the C/NCSP of the types of measures and mitigations that could or should be implemented to manage the security risk. It is likely that ASIO will have already directly engaged with the C/NCSP on any proposed change that gave rise to security risks and the notification from the CAC will simply formalise this advice. In any event, ASIO and government agencies would seek to engage the relevant C/NCSP on the proposed change and provide advice on possible control measures and mitigations to reduce or eliminate the risk in circumstances where a proposed change did give rise to security risks (i.e. unauthorised access and interference) that are prejudicial to security.

146. The CAC cannot force the C/NCSP to implement this advice, however, again as inferred by paragraphs 314B(3)(d) and (e), if a proposed change poses security risks and is implemented without any steps taken to manage this risk the C/NCSP will be potentially acting in contravention of its duties in subsections 313(1A) and (2A).

147. However, ultimately if the C/NCSP chose to ignore this advice and implementation of the change resulted the C/NCSP operating in breach of the security obligation the Attorney-General could apply to the Federal Court for a civil remedy such as a civil penalty or an injunction to penalise non-compliance. The Attorney-General could also consider issuing a direction under section 315B (or section 315A in extreme circumstances) requiring the C/NCSP to implement mitigation or remedial measures to address the security risk. A direction could also be issued before the proposed change is implemented (i.e. before there is an actual breach of the security obligation) to prevent a breach of the security obligation, if the circumstances warranted this action.

148. The notice provided to the C/NCSP under subsection 314B(5) advising of a security risk with a planned change will specifically alert the C/NCSP to the fact that the failure to mitigate the security risk could mean the C/NCSP is in breach of the obligations under subsection 313(1A) and (2A) and that this could give rise to the Attorney-General issuing a direction or enforcement action being taken to penalise the C/NCSP for non-compliance with the security obligation.

Subdivision B – Security capability plans (SCPs)

149. Item 12 will also add new sections 314C to 314E to Part 14 of the Telecommunications Act, which will allow C/NCSPs to submit a SCP to the CAC. The SCP could facilitate a C/NCSP meeting its notification requirement more efficiently and provide it with an opportunity to outline proposed changes within the context of the company's approach to security management.

150. Section 314C will enhance the new notification requirement under section 314A by clarifying that a C/NCSP can choose to meet the notification requirement through the submission of a SCP. The SCP would be in lieu of individual notifications under section 314A. Section 314E will clarify that if a change is included in a SCP further notification is not required unless there is a modification to a previously proposed change (subsection 314E(2)). Furthermore any further change/s not included in the original SCP would need to be separately notified under section 314A. For clarity submission of a SCP would not operate to exempt the C/NCSP from the notification requirements in section 314A, where the SCP failed to adequately notify of a planned change or changes.

151. The submission of a SCP would be optional and would provide a mechanism for a C/NCSP to notify all or multiple proposed changes to systems and services within a defined period. Subsection 314C(8) limits the number of SCPs which can be submitted by a C/NCSP in any 12 month period to one. This is to avoid administrative burden on government agencies to consider detailed plans on an ad hoc and frequent basis and promote the efficient and effective operation of the SCP process. As noted above, section 314E clarifies that if a proposed adverse change included in a SCP is later modified following the CAC's consideration of the change, it will be necessary for the C/NCSP to treat the modification as

if it were a new change and formally notify of the change (if it is likely to have a material adverse effect on the ability of the C/NCSP to meet its obligations to protect networks and facilities from unauthorised access and interference) unless advised otherwise by the CAC. For example, if a notification was made to locate a core control system in one country and the proposal changed to locate the system in a different country then the proposal would need to be notified again under section 314A.

152. The benefits of submitting a SCP include facilitating more holistic engagement with security agencies on investment planning and decision making, and assisting security agencies to understand more comprehensively the C/NCSP's arrangements with suppliers and its service delivery model for operating and managing key components of its network and service. For this reason, a SCP may also outline the C/NCSP's general approach to managing risks of espionage, sabotage, disruption and interference and what measures or mitigation it proposes to apply to each proposed change (subsections 314C(6) and (7)). Subsection 314C(7) allows the C/NCSP to detail any current or proposed mitigation measures or controls to reduce the risk of unauthorised access or interference. For example, this may include access controls in systems or oversight arrangements that are proposed to be built into contracts with third parties. These additional details will help expedite the assessment of the security plan by reducing the need to request additional information from a C/NCSP about the likely operation of a proposed change.

153. Early engagement and notification of changes to networks will enable any security risks associated with a proposed business model to be identified early and mitigation measures built into the design stage. Early incorporation of security controls from the design stage will be easier and more cost effective for C/NCSPs than if measures are added late in the process.

154. Inclusion of information about a C/NCSP's security polices, practises and strategies could facilitate more targeted engagement between the C/NCSP and government agencies on the C/NCSP's approach to the performance of its duties under the security obligation in subsections 313(1A) and (2A). It could also streamline the process of assessing the security risks associated with each proposed change and ultimately provide the CAC (and ASIO) with sufficient information to assess whether proposed changes can be implemented without further engagement with government agencies. Importantly, the submission of a SCP is not intended to remove the need to engage with ASIO where this is already occurring or where ASIO considers it necessary to ensure compliance with the security obligation.

Kinds of changes

155. The SCP provisions are intended to complement and supplement the new notification provisions in section 314A. For example, a SCP should only capture those changes the C/NCSP is planning to implement that are likely to have a material adverse effect on the provider's ability to meet its requirements. This applies the same test as section 314A. The phrase 'material adverse effect' includes any change which could have an actual or measurable negative impact on the ability of the C/CSP to comply with the duties in subsections 313(1A) or 313(2A).

156. Section 314C sets out the matters that may be included in a SCP if a C/NCSP chooses to submit a SCP. There is no particular date on which a SCP may be submitted (for example there is no requirement it be submitted by the end of the financial year). However, it should

be noted that any changes that require consideration before the expiry of the 60 day period may need to be notified separately under section 314A, which specifies a 30 day period for CAC consideration.

157. This includes specifying that the kinds of changes that should be included in the SCP include (but are not limited to) the changes listed in new section 314A of the TIA Act, which are outsourcing arrangements, offshoring equipment or services, changes to services, procuring new equipment, and changes to the management of services. Greater clarity on what should and should not be notified and included or not included in a SCP will also be provided in administrative guidelines.

Assessment process following notification

158. Section 314D outlines the administrative process following submission of a SCP to the CAC. Under subsection 314D(6) the CAC has 60 days to assess all of the proposed changes in the SCP. In this timeframe, the CAC (in consultation with ASIO as necessary) will consider whether there is sufficient information about each proposed change to assess the potential security risks and whether proposed mitigations (if included) are adequate to manage the risk. If there is insufficient information, the C/NCSP will be contacted in writing and requested to provide further information under subsection 314D(1). Subsection 314D(6) further provides that if the CAC requests further information under subsection 314D(1), the C/NCSP will be provided with a notice as soon as practicable and within 60 days of providing the further information.

159. Like the process for individual notifications under section 314A, the C/NCSP will receive a notice from the CAC regarding each specific change in the SCP (the only difference being that the notification will be made within 60 days). This may be either a:

- request under subsection 314D(1) for further information about a planned change so the CAC can assess whether there is a risk of unauthorised access to, or interference with, telecommunications networks or facilities;

- notice under subsection 314D(3) advising the C/NCSP of a risk associated with a planned change of unauthorised access to, or interference with, telecommunications networks that would be prejudicial to security; or

- notice under subsection 314D(5) that the CAC is satisfied there is not a risk from a planned change of unauthorised access to, or interference with, telecommunications networks or facilities that would be prejudicial to security.

160. The effect of section 314D is that each change included in a SCP is assessed individually. For example, a C/NCSP may receive a notice that there is a risk of unauthorised access or interference that would be prejudicial to security with two out of the ten changes listed in the plan and the C/NCSP would be encouraged to engage with ASIO on mitigation measures for these particular changes. The notice would then specify that no risks have been identified with the remaining eight changes and no further consultation on these changes is required.

161. Like section 314A, this provision does not contain a power to enforce compliance with mitigation advice. Instead, ASIO and government agencies would seek to engage the

relevant C/NCSP on the proposed change and advice on possible control measures and mitigations to reduce or eliminate the risk in circumstances where a proposed change did give rise to security risks (i.e. unauthorised access and interference) that are prejudicial to security.

162. Failure to address potential security risks and cooperate to implement security advice could lead to ASIO furnishing an adverse security assessment relating to the C/CSP's ability to meet its obligation to secure networks and facilities to support the Attorney-General in exercising the new directions powers in section 315B. Further, in circumstance where failure to implement mitigation advice resulted in a breach of the security obligation, the Attorney-General could also take enforcement action in the Federal Court to pursue civil remedies such as a civil penalty or an injunction. The notice provided to the C/NCSP under subsection 314D(3) advising of a security risk with a planned change will clarify that a failure to mitigate security risks could mean the C/NCSP is in breach of the obligations under subsections 313(1A) and (2A) to protect telecommunications networks and facilities from unauthorised access and interference and could result in enforcement action or the Attorney-General issuing a direction under section 315B (or section 315A in extreme cases).

163. The purpose of the notification process is to avoid network operational and management changes being implemented without proper regard to the potential national security vulnerabilities that the change could expose the network to. It will help to ensure that C/CSPs have proper regard to their obligation to protect networks and facilities from unauthorised access and interference under subsections 313(1A) and (2A) of the Telecommunications Act. As noted with respect to individual notifications under section 314A, ASIO will have access to the latest threat information concerning espionage, sabotage, and foreign interference activity. Particular outsourcing arrangements, especially when combined with sensitive parts of the network and facilities, can increase the vulnerability of a network or facility to exploitation. For higher risk C/NCSPs (i.e. those networks likely to be more targeted by malicious actors) the notification process and/or submission of SCPs will be supported by ongoing engagement to proactively manage risks on networks and ensure proposals are modified as appropriate to reduce or eliminate these risks.

164. There is no exemption process associated with SCPs as they are not mandatory. However, any C/NCSP exempted under section 315A from making individual notifications for planned changes to telecommunications systems and services would also be expected not to submit a SCP.

165. Item 12 will also insert the heading 'Division 4 – Carriage service provider may suspend supply of carriage service in an emergency' to apply consistent drafting conventions.

Item 13 – After section 315

Division 5 – Directions by Attorney-General

166. Item 13 inserts new Division 5 into Part 14 to co-locate the existing directions making power of the Attorney-General (new section 315A) and the new directions making power of the Attorney-General (section 315B).

Attorney-General's direction power to cease a service

167. Item 13 relocates repealed subsection 581(3) as new section 315A, which is the Attorney-General's direction making power to not use or supply, or cease using or supplying, carriage services where use or supply is considered to be prejudicial to security. Subsection 581(3) of the Telecommunications Act is repealed under Item 27 of the Bill.

168. The Bill does not change the operation or effect of the existing power vested in the Attorney-General to direct a C/CSP to cease its services on security grounds, with the exception of adding a requirement that ASIO must have issued an adverse security assessment before the Attorney-General can exercise the power. An adverse security assessment is subject to the accountability requirements contained in Part IV of the ASIO Act, including the provision of notice of the adverse assessment to the subject of the assessment, and the availability of review in the AAT. The Bill will also remove a current limitation on judicial review of a direction under the ADJR Act.

169. The new section 315A is intended to be used in the most extreme circumstances where the continued operation of the service would give rise to such serious consequences that the entire service needed to cease operating. 'Security' is defined within the ASIO Act to include the protection of , and of the people of, the Commonwealth, States, and Territories from espionage, sabotage, politically motivated violence, promotion of communal violence, attacks on Australia's defence system, or acts of foreign interference, as well as the protection of Australia's border integrity. The threshold for exercising the power is that the security risk is prejudicial to security. The term 'prejudicial' should be given the same meaning as 'activities prejudicial to security' which is defined within the *Attorney-General's Guidelines in relation to the performance by the Australian Security Intelligence Organisation of its function of obtaining, correlating, evaluating and communicating intelligence relevant to security (including politically motivated violence),* to mean activities relevant to security and which can reasonably be considered capable of causing damage or harm to Australia, the Australian people, or Australian interests, or to foreign countries to which Australia has responsibilities.

170. The creation of the new directions power in section 315B is intended to supplement this existing power with a regulatory tool which will enable other action to be taken to address a security risk where the circumstances do not require the complete shut-down of the service. The power to cease a service will remain the ultimate protection measure where action needs to be taken immediately to protect Australia's security interests. For these reasons, some of the additional requirements and protections included in the new directions power under section 315B, for example the Attorney-General must be satisfied all reasonable steps have been taken to reach agreement and consult the affected C/CSP in good faith, are not replicated in the existing provision. However, alternative safeguards are provided for use of the power under section 315A through the requirement to consult the Prime Minister, in addition to the Minister responsible for administering the Telecommunications Act, the Minister for Communications.

171. The Bill will now provide further safeguards by increasing the threshold for exercising the power to circumstances where ASIO has furnished an adverse security assessment. While subsection 581(3) was already included in the list of prescribed administrative actions which could be the subject of an ASIO security assessment, Item 13

will now impose a requirement on the Attorney-General to obtain an adverse security assessment from ASIO prior to using the power in subsection 315A(2).

172. The adverse security assessment triggering the use of the directions power will be issued by ASIO in accordance with Part IV of the ASIO Act and will set out in writing ASIO's advice in respect to the exercise of the directions power by the Attorney-General. In practice a security assessment under Part IV will be prepared by ASIO, following engagement with the affected C/CSP about potential security risks posed to the C/CSPs' network and/or facilities and providing advice on possible mitigation or remedial measures. If the C/CSP is unwilling to cease the service or take other remedial measures voluntarily, then an adverse security assessment would be prepared by ASIO for the purpose of recommending the Attorney-General issue a direction under section 315A.

173. In accordance with the accountability provisions contained within Part IV of the ASIO Act, the C/CSP would be able to seek merits review of the ASIO security assessment in the AAT. The Attorney-General would be required to provide a copy of the security assessment to the C/CSP within 14 days. The security assessment would be accompanied by an unclassified statement of grounds that would set out the information ASIO has relied upon and a written notice informing the C/CSP of its right to apply to the AAT for merits review of the security assessment.

174. The Bill (Item 32) also amends the ADJR Act to remove the current exemption from judicial review under the ADJR Act. Currently, while judicial review of a direction to cease a service would likely be available through the High Court's original jurisdiction, the process is more complicated and does not provide as many grounds of review. Removing the current exemption will enable a C/CSP to seek judicial review under the ADJR Act and therefore increase the transparency and accountability of the direction process. It will also align with the review rights provided under the new directions power in subsection 315(2) which will also provide for judicial review under the ADJR Act.

The Attorney-General's power to direct a C/CSP to do or refrain from doing something

175. The Bill will vest an additional directions power in the Attorney-General (section 315B) to provide a more proportionate and graduated power of intervention and enforcement to achieve national security outcomes where this cannot be done on a cooperative basis. Noting that the framework is premised on cooperative engagement and collaboration, it is expected this power will be used only as a last resort to achieve compliance. The intention is that government agencies and C/CSPs continue to operate in the current environment of cooperative engagement and exchange of information, but if national security outcomes cannot be achieved on a cooperative basis, the Attorney-General can consider requiring compliance through the issue of a formal direction.

176. Alternatively, there may be circumstances in which a C/CSP would prefer the certainty of a formal direction. For example, implementing security measures may increase the cost of a particular investment option and other less secure options may be more commercially attractive. Fiduciary duties to shareholders can operate as a disincentive to invest in security measures for the purpose of protecting national security interests. For these reasons, a company board may prefer a clear mandate to govern its decision making.

177. Section 315B provides the Attorney-General with the power to give a written direction requiring the C/CSP to act, or refrain from an act. Before issuing a direction, the Attorney-General must be satisfied that there is a risk of unauthorised interference or access (subsection 315B(1)) that would be prejudicial to security having reference to the meaning of 'security' in the ASIO Act (subsections 315B(1) and 315B(13)). In other words, the Attorney-General would only be authorised to issue a direction where there was a risk of unauthorised interference or access and it threatened the confidentiality of information contained on or carried across telecommunications networks and/or facilities or the availability and integrity of telecommunications networks and facilities and this was prejudicial to security.

178. As noted above, 'security' is defined within the ASIO Act to include the protection of the Commonwealth, States, Territories and the people of Australia from espionage, sabotage, attacks on Australia's defence system, or acts of foreign interference, as well as the protection of Australia's border integrity. The threshold for exercising the power is the same threshold as the existing directions powers under section 315A: it must pose a risk that is prejudicial to security. The term 'prejudicial' should be given the same meaning as 'activities prejudicial to security' which is defined within the *Attorney-General's Guidelines in relation to the performance by the Australian Security Intelligence Organisation of its function of obtaining, correlating, evaluating and communicating intelligence relevant to security (including politically motivated violence),* to mean activities relevant to security and which can reasonably be considered capable of causing damage or harm to Australia, the Australian people, or Australian interests, or to foreign countries to which Australia has responsibilities.

179. The types of things the Attorney-General can direct a C/CSP to do or not do are not specified or limited, with the exception of the limitation imposed in subsection 315B(3). Subsection 315B(3) limits the purpose for which the Attorney-General can issue a direction to do, or refrain from doing, specified acts or things that are 'reasonably necessary' for reducing or eliminating the risks identified in subsection 315B(1). In other words, the direction 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.

180. Noting that the security framework is 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. For example, 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. Again, the aim of the framework is that C/CSPs will engage with ASIO and AGD when developing procurement plans to outsource capability or network support to a supplier (third party) and if required, mitigation measures would be developed and agreed on a cooperative basis. Where there is disagreement about the need to implement mitigation measures, or an actual failure to implement ASIO recommended mitigation measures, or a C/CSP seeks a more formal request to empower its Board of Executives, the Attorney-General can issue a direction compelling the C/CSP to implement the mitigation measures.

181. A direction would be based on addressing a security risk as set out in an ASIO adverse security assessment. The circumstances where this might arise could also include potential risks associated with planned changes to networks, facilities or services which are

notified under new section 314A of the Telecommunications Act. For example, while those provisions themselves identify mechanisms for how the CAC might respond to a notified change that gave rise to a risk of non-compliance with the security obligation, it is possible that where the affected C/CSP failed to implement recommended mitigation measures through that process ASIO would prepare an assessment recommending the Attorney-General issue a direction.

182. Subsection 315A(3) of the Telecommunications Act 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. An adverse security assessment would normally be prepared in circumstances where ASIO or another relevant agency had informed a C/CSP of the security risks to the C/CSP's network and/or facilities and tried to work with the C/CSP to develop control measures and mitigations but the C/CSP was uncooperative and/or refused to implement ASIO's advice. The adverse security assessment would be prepared by ASIO for the purpose of recommending the Attorney-General issue a direction under section 315B.

183. In accordance with the accountability provisions contained within Part IV of the ASIO Act, the C/CSP may seek merits review of the ASIO security assessment in the AAT. The Attorney-General is required to provide a copy of the security assessment to the C/CSP within 14 days of receiving the assessment. The security assessment must be accompanied by an unclassified statement of grounds setting out the information ASIO has relied upon and a written notice informing the C/CSP of its right to apply to the AAT for merits review of the security assessment.

184. In addition to making an adverse security assessment a pre-condition to the exercise of the directions power in section 313B, the Attorney-General will also have to be satisfied that reasonable attempts have been made to negotiate an outcome between government agencies (for example, ASIO and AGD) and the C/CSP that reduces or eliminates the security risk. The requirement in subsection 315B(5) has the effect of placing an obligation on government agencies to ensure that they have acted in good faith in engaging the C/CSP to alert them to the risk, the consequences of not managing the risk and sought to work collaboratively with the C/CSP to develop appropriate measures that reduces the risk to security and no more. Likewise, the C/CSP will be under an obligation to engage in good faith and seek to work with ASIO and government agencies to address security risks.

185. Good faith in this context is intended to impose a requirement that engagement is genuine and solutions-focussed and all reasonable options for addressing the risk are considered by both parties. This provision is intended to underpin the entire objective of the security framework which is to facilitate cooperative and collaborative government and industry partnership to manage national security risks to the telecommunications sector.

186. Subsection 315B(6) outlines the types of factors the Attorney-General should have regard to in determining whether it is reasonable to issue a direction having regard to all the circumstances of the case and what should be included in that direction. Factors that the Attorney-General must consider include: the risk to security and other considerations such as the potential costs associated with implementing the proposed direction, the potential impact for competition in the sector and potential impacts for end-users. The harm to security is to be

given the greatest weight in this balancing exercise to ensure that Australia's security interests are properly safeguarded despite potential impacts on the C/CSP, competition and end-users. The requirement to have regard to other factors, in addition to the risk to security, will ensure that a direction is proportionate and reasonable in all of the circumstances and guard against imposing directions that would possibly address security risks but have an unnecessary crippling effect on the C/CSP's business or impede market innovation and competition. Subsection 315B(7) clarifies that the matters listed in subsection 315B(6) are not intended to limit or prescribe the matters to which the Attorney can have regard when exercising the power.

187. To ensure that the directions power is exercised in an objective manner and complies with procedural fairness requirements, mandatory consultation requirements have been imposed on the exercise of the directions power. Paragraph 315B(8)(a) imposes mandatory consultation with the Minister administering the Telecommunications Act (the Minister for Communications) to ensure that the exercise of the power takes into account broader communications policy considerations, for example, any potential impact on the telecommunications sector, including effects for competition. This requirement is in addition to the requirement in subsection 315B(6) specifying that the Attorney-General must have regard to the potential consequences of a direction on industry competition and on the C/CSP and its customers. This requirement imposes a high degree of scrutiny and accountability on the Attorney-General's exercise of this power. Mandatory consultation with the Minister for Communications highlights the significance of the decision and will ensure a range of views inform the Attorney-General's exercise of the directions power and the Attorney-General takes into account factors such as the potential impact for the affected C/CSP, end-users and the economy more broadly.

188. Paragraph 315B(8)(b) imposes mandatory consultation with the affected C/CSP. The Attorney-General is required to write to the C/CSP and notify them of his or her intention to issue a direction, set out the terms of the proposed direction, and provide the C/CSP the opportunity to make written representations about the proposed direction. In practice, the Attorney-General will generally provide the C/CSP with a copy of draft direction at the time he/she provides the ASIO security assessment (as required under the ASIO Act).

189. Subsection 315B(9) sets a minimum timeframe in which the Attorney-General can require the C/CSPs to provide written representations, which is at least 28 days from the date the notice is given. The exception is where a shorter timeframe is required because the circumstances require action to be taken quickly to address a threat, for example where the risk of espionage, sabotage or foreign interference was high and required urgent resolution. The provision does not by implication prevent the Attorney-General from providing a C/CSP longer than 28 days in which to make representations. In fact a notice might seek to provide a timeframe for making representations in the event the C/CSP decided to seek merits review of the security assessment through the AAT which might have the effect of staying the process for issuing a direction. Subparagraph 315B(8)(b)(iii) provides that the Attorney-General is only required to take into account representations made within the specified timeframe. This qualification will ensure that directions can be issued and implemented within a timely manner.

190. Subsection 315B(8) does not specify the form in which representations should be made other then they must be in writing. Given the Attorney-General is required to consider factors such as the potential cost and impact on the C/CSP and their customers, it would be

desirable if representations were able to address these matters. C/CSPs should also set out their reasons as to why the C/CSP does not agree to implement ASIO's advice.

191. Subsection 315B(10) clarifies that subsection 315B(8) does not operate to restrict the Attorney-General from consulting other persons. This could include other Ministers with an interest, such as the Minister for Foreign Affairs and Trade where there are international sensitivities. A direction would also likely be informed by the advice of other security agencies and relevant government agencies through consultations by AGD.

192. Subsection 315B(11) requires the Attorney-General to provide the telecommunications regulator, the ACMA, with a copy of any direction that is issued under new subsection 315B(1). This is a notification only to the ACMA and does not require intervention by the ACMA.

193. Subsection 315B(12) is intended to make clear that a breach of a direction given by the Attorney-General under section 315B gives rise to the enforcement regime in the Telecommunications Act. A direction must be complied with by a C/CSP. Non-compliance is one trigger for further action, as provided for in the Bill under Items 15-29. Neither subsection 315B(12) nor subsection 315A(5) preclude enforcement actions being taken against a C/CSP which has breached the obligations in section 313 of the Telecommunications Act (including the new obligation of this Bill) without that C/CSP having been issued with a direction.

194. Given the potential implications of a direction to the operations of a C/CSP, the Attorney-General's power to issue directions under sections 315A or 315B cannot be delegated (unlike the Secretary of AGD's information-gathering powers under section 315C which may be delegated to the Director-General of Security– see notes on Division 6 below). There is also no implied power to authorise an official to exercise the power to issue directions on the Attorney-General's behalf.

Division 6 – Attorney-General's Secretary's information-gathering powers

195. Item 13 inserts Division 6, which sets out the Secretary of AGD's new information-gathering powers under sections 315C-315H.

196. The Secretary of AGD is empowered to request information from C/CSPs under section 315C where that information is relevant to assessing their compliance with the obligation to protect networks and facilities under subsections 313(1A) and (2A). In exercising the power the Secretary of AGD must have the belief that the C/CSP has information or documents that would assist the Secretary of AGD to assess compliance with the duties in subsections 313(1A) and (2A). It is not necessary that the Secretary of AGD be satisfied that a breach has occurred before exercising the information gathering power. The information gathering power has been drafted with reference to the Administrative Review Council's twenty best practice principles for implementing and exercising information gathering powers in its 2008 report on the *Coercive Information Gathering Powers of Government Agencies*. In particular, the information gathering power is limited to obtaining material directly relevant to monitoring compliance with the proposed security obligation.

197. Paragraph 315C(2)(c) provides that the Secretary of AGD may exercise his or her information gathering power in respect of copies of documents or information, rather than

original versions of requested documents, including electronic documents and applications. Subsection 315C(8) provides that if a C/CSP provides copies of documents in compliance with a requirement under paragraph 315C(2)(c), the C/CSP will be entitled to be paid reasonable compensation by the Commonwealth. Paragraph 315C(2)(c) will operate in a similar manner to the information gathering powers granted to the ACMA in paragraphs 521(2) (b) and (c) of the Telecommunications Act.

198. Subsection 315C(4) requires the Secretary of AGD to consider the potential cost, time and effort imposed on the C/CSP in complying with the notice. In practice, government agencies will likely engage the C/CSP prior to issuing a notice to discuss the terms of the notice. The purpose of this discussion will be to ensure the notice targets the information sought and does not put the C/CSP to unnecessary expense. There may be circumstances where it is not feasible or necessary to engage the C/CSP prior to issuing the notice. A failure to engage or consult does not affect the validity of the notice as it is not a pre-condition for issuing the notice.

199. The information-gathering power is intended to formalise and extend the existing cooperative relationship of information exchange between government and C/CSPs. The new power is not intended to replace these existing practices, but instead would be exercised in circumstances where a C/CSP considers it is restrained from sharing information for contractual or other legal reasons, or for some other reason refuses to cooperate. There may be instances where C/CSPs are reluctant to provide information because of commercial-in-confidence reasons or because it is potentially self-incriminating. The powers are modelled on the ACMA's existing information-gathering powers in Part 27 of the Telecommunications Act and include existing protections against self-incrimination.

200. The information-gathering power in section 315C (combined with the provision on self-incrimination in new section 315D) will operate to override reasons for non-disclosure and compel the provision of information or documents. The compulsion element has the effect of authorising the disclosure of personal information under the Privacy Act (i.e. the disclosure is authorised by law) and offers a statutory protection for breach of confidentiality provisions in contracts.

201. Subsection 315C(3) clarifies that a C/CSP issued with a notice to produce information or documents must comply with that notice. Furthermore, subsection 315D(1) clarifies that a notice under section 315C must be complied with even if it exposes the person (an individual or a body corporate) to criminal or civil liability. Subsection 315D(1) reflects section 187 of the Commonwealth *Evidence Act 1995,* which abolishes the privilege against self-incrimination for bodies corporate, including where the body corporate is required to answer a question, give information or produce a document under a law of the Commonwealth.

202. Subsection 315D(2) provides broad protections for individuals against criminal or civil proceedings if the information is self-incriminating. For example, it clarifies that the documents or information cannot be used in evidence in any criminal or civil proceedings against the individual with the exception of Commonwealth criminal proceedings for providing false or misleading information or documents or civil proceedings to recover a penalty for non-compliance with the exercise of the information gathering power itself. The common law privilege against self-incrimination only extends to natural persons, not to bodies corporate. This is a well-established principle in common law, as outlined in AGD's

2011 *A Guide to Framing Commonwealth Offences, Infringement Notices and Enforcement Powers.*

203. Non-compliance with a notice to provide information or documents will constitute a breach of the Telecommunications Act and will attract the operation of the civil remedies regime in Part 30 (injunctions), Part 31 (civil penalties) and Part 31A (enforceable undertakings) of the Telecommunications Act. The Bill authorises the Attorney-General to bring proceedings to enforce these remedies for non-compliance with a notice issued under section 315C.

204. The information to be sought under subsection 315C(2) is likely to be of a commercial nature, rather than personal information. It is very unlikely that this information would relate to end-users. Rather it would likely fall into the category of procurement plans, network or service design plans, tender documentation, contracts and other documents specifying business and service delivery models and network layouts.

205. Subsection 315C(4) sets out the requirements for a notice issued by the Secretary of AGD under subsection 315C(2). Subsections 315C(2) and 315C(4) have the effect of requiring the Secretary of AGD to make any request for information and documents by written notice which sets out when the information or documents are required, the form in which they are required to be provided or produced, and outline the effect of provisions relevant to C/CSPs concerning compliance with the Telecommunications Act and offences under the Criminal Code for providing false or misleading information. This ensures C/CSPs understand the consequences of failure to comply with a notice issued under section 315C, including the criminal consequences for providing misleading or false information.

206. Given the potential sensitivities of information required to be provided to the Secretary of AGD (or his or her delegate, see new subsection 315G) under section 315C, and given that self-incrimination does not excuse non-compliance with a notice issued under subsection 315(2) (see new section 315D), the Bill inserts a number of provisions to clarify the use, retention and further disclosure of the information to other persons.

207. Section 315E clarifies that the Secretary of AGD may inspect a document produced under section 315C and may make and retain copies as necessary. Section 315F empowers the Secretary of AGD to take possession of the documents obtained under section 315C (including original documents) and keep them for as long as he or she deems necessary. Noting that section 315H enables the further disclosure of that document for other purposes (as specified by section 315H), the document could be retained for a period beyond the purpose of the initial request. Confidentiality of retained documents would be protected under existing legislative requirements governing the use and disclosure of documents and information held for official purposes, including secrecy obligations and storage requirements under the *Archives Act 1983*. It is important to note that the type of information or documents that can be required to be provided is however limited by relevance to the security obligation imposed in subsections 313(1A) and (2A). Section 315F imposes requirements on the Secretary of AGD (or his or her delegate) to provide a certified copy of the original documents to the person who is entitled to possess the document that was produced pursuant to the notice and otherwise provide reasonable access to inspect or copy the document.

208. Section 315G allows the Secretary of AGD to delegate any of the information-gathering powers referred to in new sections 315C, 315E and 315F to the

Director-General of Security. The purpose of this delegation power is to counter protracted engagement processes and in particular to enable the Director-General, whose Organisation is likely to be directly engaging with C/CSPs, to obtain relevant information for the purpose of assessing the risk of unauthorised access and interference. In accordance with usual administrative law practices, the delegation must be in writing and specify to whom or to what position the power is delegated. Also in accordance with administrative law practices, the Secretary of AGD may revoke the delegation at any time. Subsection 315G(2) contains a further protection in the exercise of the information gathering power by a delegate by enabling the Secretary of AGD to specify how the delegate is to exercise the power. The delegate must comply with any directions issued by the Secretary of AGD otherwise the exercise of the power will be invalid.

Division 7 – Information sharing and confidentiality

209. Item 12 inserts Division 7, which sets out how information obtained under sections 314A, 314B, 314C, 314D, 315C and 315H may be shared and disclosed.

210. Section 315H authorises the further use or disclosure of information or documents obtained under sections 314A, 314B, 314C, 314D, 315C and 315H to persons other than the Secretary of AGD or their delegate. Disclosure must be either for the purpose of assessing compliance with a C/CSP's obligation to protect networks and facilities from unauthorised access or interference, or for broader security purposes (paragraphs 315H(1)(a) and (b)). In practice it is likely that information sharing may take place between relevant government agencies, such as with 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. It may also be used to inform the Attorney-General or other relevant Ministers for the purpose of exercising the Attorney-General's power in new section 315A (previously subsection 581(3), or more broadly for the purposes of security. 'Security' is defined by reference to the ASIO Act. The powers would therefore also potentially authorise sharing of information or documents with state authorities and international partners, pursuant to the ASIO Act and formal information sharing arrangements with those countries.

211. While section 315H allows an expanded number of people to access the information or document required to be provided, this is limited to the protection of security. For example, a document or information may also be relevant in assessing the vulnerability of another Australian network to unauthorised access or interference. It is important that government agencies are not prevented from relying on a piece of information or document that reveals or addresses other security threats and risks. Again, the information and documents that are captured by this information sharing provision are likely to be commercial in nature and restricted to being relevant to the duty in subsections 313(1A) or 313(2A).

212. Safeguards are built into section 315H to protect commercially sensitive information provided by C/CSPs. Subsection 315H(2) requires the Secretary of AGD, the Director-General of Security or other Commonwealth officers who have access to the information or documents to remove from the information or documents information that identifies the C/CSP before sharing them outside of the Australian Government. In practice, information would only likely be shared outside Commonwealth Government officials for reasons of providing threat information and intelligence to foreign partners in support of reciprocal information sharing arrangements. Australia is dependent on intelligence provided

under these arrangements to support preparation of its own threat advice to Australian companies. C/CSPs will not be advised when information is shared with foreign partners as this could potentially compromise national security by identifying the types of issues considered by security agencies and the nature of sharing arrangements.

213. Only information that does not identify the C/CSP (i.e. the threat-based information) would be shared in these circumstances and information shared in these circumstances is protected through formal arrangements such as a Memorandum of Understanding. In practice this would involve removing the identifying details of the C/CSP such as company name and logo before the information or documents are shared. As outlined above, information or documents would be shared with other security agencies and foreign intelligence partners to better protect national security. It would not be shared with a C/CSP's competitors or with other stakeholders who may gain a commercial advantage from seeing this information. Subsection 315H(3) also imposes a confidentiality obligation on people who obtain information or documents. This would include protection of information and documents in line with Australian Government policies and procedures and only disclosing the information or documents for the purposes of section 315H or where otherwise provided for other under other legislation.

214. Australian Government agencies subject to the Privacy Act are required to protect, use, disclose and destroy personal information in line with the requirements of the Privacy Act. Section 315H is intended to allow information to be shared for reasons of providing threat information and intelligence to foreign partners in support of reciprocal information sharing arrangements. Information or documents would therefore generally be de-identified prior to being shared to remove personal information, unless information about a particular person needs to be shared for the purposes of security (such as where information about an individual is directly relevant to a security threat).

215. The restrictions in section 315H will not override existing legislative provisions that authorise ASIO to communicate information obtained in the performance of its functions. Parliament has already set out the circumstances in which it is considered appropriate for an agency such as ASIO to be able to communicate information collected as part of the performance of its functions, including personal and other information collected under warrant.

216. The ASIO Act provides the authority for ASIO to seek information from, and provide information to, authorities in other countries that is relevant to Australia's security, or the security of the foreign country. In general, the types of foreign authorities that are approved by the Attorney-General perform broadly similar functions to ASIO, and include security and intelligence authorities, law enforcement, immigration and border control, and government coordination bodies.

217. ASIO has internal guidelines that govern the communication of information about Australians and foreign nationals to approved foreign authorities. These guidelines impose an internal framework for assessing and approving the passage of such information.

218. In addition to these safeguards, the activities of ASIO (including intelligence sharing activities) are reviewed by the independent statutory office of the Inspector-General of Intelligence and Security (IGIS). The IGIS publicly reports each year about inquiries or inspection activity conducted during that year.

219. Although there are no express consequences for a breach of the confidentiality requirements in subsections 315H (2) or (3), disciplinary action would be available under existing legislation for Australian Government employees who breach these provisions. Under the *Public Service Act 1999* Australian Public Service employees must comply with all applicable Australian laws and could face disciplinary action for any breaches. Section 70 of the *Crimes Act 1914* applies criminal sanctions to unauthorised disclosure of information by current or former Commonwealth officers. Many Australian state and territories have similar offences for unauthorised disclosure of information by public officials.

Division 8 – Annual report

220. Section 315J obliges the Secretary of AGD to provide an annual report to the Attorney-General on the operation of the provisions in this Bill. Subsection 315J(3) obliges the Attorney-General to cause a copy of this report to be laid before each House of the Parliament within 15 sittings days of that House after receiving the report.

Item 14 – Before section 316

221. Item 14 will insert the heading 'Division 7 – Generality of Part not limited' before the existing section 316 of the Telecommunications Act to separate this section from the new sections added by this Bill.

Item 15– Subsections 564(1) and (2)

222. The directions powers granted to the Attorney-General and the information-gathering powers granted to the Secretary of AGD by this Bill will be enforceable by virtue of the application of existing civil remedies provided for in the Telecommunications Act. These are located in Part 30 (injunctions), Part 31 (civil penalties) and Part 31A (enforceable undertakings) of the Act. These provisions provide remedies to penalise breaches of obligations under the Act and to prevent a breach.

223. It is expected that the Attorney-General (supported by AGD) would manage all compliance and enforcement action with respect to provisions in this Bill and the ACMA would not act as a regulator with respect to the provisions in this Bill to ensure there is no duplication of roles. However, this Bill does not expressly preclude the ACMA from taking separate and independent action with regard to these new provisions given their roles as regulator for the communications sector.

224. Item 15 has the effect of vesting the Attorney-General with the same powers vested in the Communications Minister, the ACMA and the Australian Competition and Consumer Commission (ACCC), to apply to the Federal Court of Australia for an injunction to restrain a C/CSP from engaging in conduct that contravenes the Telecommunications Act. The Attorney-General may also apply for an injunction requiring a C/CSP to take action (paragraphs 564(1)(a) and (b)). For example, the Attorney-General may wish to seek an injunction where information has been obtained that a C/CSP is about to enter into a contract which poses a risk to security in the form of unauthorised access or interference.

Item 16 – After subsection 564(3)

225. The standing of the Attorney-General to apply for an injunction in the Federal Court of Australia is limited by subsection 564(3) of the Telecommunications Act. Item 16 inserts subsection 564(3A) which has the effect of limiting the standing of the Attorney-General to apply for injunctive relief to address non-compliance with the security obligation (new sections 313(1A) and 313(2A)), a direction issued under new subsection 315A(5) or 315B(12) or notice to provide information or a documents under new subsection 315C(3). Any one of these types of breaches has the potential to give rise to an application by the Attorney-General for an injunction.

226. C/CSPs are encouraged to notify the CAC, where appropriate, of changes to systems and services under section 314A and 314C and engage early before entering into contractual arrangements. The ability for the Attorney-General to apply to the Federal Court for an injunction is designed to encourage this early engagement with government. Injunctions and other enforcement powers will only be used as a last resort following engagement between government and C/CSPs and attempts to address security risks cooperatively.

Item 17 – Before subsection 564(4)

227. Item 17 inserts the heading 'Definition' before subsection 564(4) of the Telecommunications Act to clarify an existing subsection within Division 6 relating to the *Telecommunications (Consumer Protection and Service Standards) Act 1999* and regulations under that Act.

Item 18 – Subsection 571(1)

228. Section 570 of the Telecommunications Act provides that pecuniary penalties are payable for contraventions of civil penalty provisions. The Communications Minister, the ACMA or the ACCC may institute a proceeding in the Federal Court of Australia for the recovery of those penalties (subsection 571(1)). Item 18 grants the Attorney-General that same ability.

Item 19 – Before subsection 571(3)

229. Item 19 inserts the heading 'Limit on standing of the ACMA' before existing subsection 571(3) of the Telecommunications Act, which identifies provisions under which the ACMA is not entitled to institute a proceeding for the recovery of a penalty.

Item 20 – At the end of section 571

230. Like the limitation imposed on the standing of the Attorney-General to seek injunctive relief, Item 20 inserts new subsection 571(4) into the Telecommunications Act to limit the standing of Attorney-General to recover pecuniary penalties provided for in Part 31 of the Telecommunications Act to address non-compliance with the security obligation (new subsections 313(1A) and 313(2A)), a direction issued under new subsection 315A(5) and 315B(12) or notice to provide information or a documents under subsection 315C(3). Any one of these types of breaches has the potential to give rise to an application to the Federal Court of Australia by the Attorney-General for the imposition of a pecuniary penalty.

Item 21 – Section 572A

231. Item 21 enables the Attorney-General to enter into enforceable undertakings with C/CSPs provided for in Part 31A of the Telecommunications Act. This is achieved by extending the operation of section 572A to refer to the Attorney-General along with the ACMA as being authorised to accept an undertaking.

Item 22 – Subsections 572B(1), (3) and (4)

232. The Attorney-General will have a role in the operation of enforceable undertakings equivalent to that played by the ACMA under the current legislation. A C/CSP which has been identified as being in breach of its obligations under section 313 of the Telecommunications Act, or in breach of new subsections 315A(5), 315B(12) or 315C(3), may make a formal commitment to the Attorney-General to remedy that breach. The commitment may be to take action, refrain from taking action, or to ensure that the Telecommunications Act is not contravened in the future. The undertaking may only be withdrawn by the C/CSP, with the consent of the Attorney-General.

Item 23 – At the end of subsection 572B(5)

233. Item 23 authorises (but does not oblige) the Attorney-General to publish the undertaking on the Attorney-General's Department's website.

Item 24 – After subsection 572B(5)

234. Item 24 limits the Attorney-General's authority to accept an undertaking to an undertaking which addresses compliance with the security obligation (new subsections 313(1A) and 313(2A), a direction issued under new subsections 315A(5) or 315B(12) or notice to provide information or a documents under new subsection 315C(3) of the Telecommunications Act. These circumstances are the same as those which enable the Attorney-General to institute proceedings in the Federal Court of Australia to apply for an injunction or to recover pecuniary penalties.

Item 25 – Subsection 572C(1)

235. Item 25 extends the operation of subsection 572C(1) of the Telecommunications Act to apply to the Attorney-General, in addition to the ACMA. The effect of this is to give the Attorney-General standing to apply to the Federal Court of Australia to enforce an undertaking that the Attorney-General entered into with a C/CSP in circumstances where the C/CSP has failed to comply with the terms of the undertaking.

Item 26 – At the end of section 572C

236. Item 26 has the effect of clarifying that the authority which the ACMA and the Attorney-General have to bring proceedings in the Federal Court of Australia to enforce an undertaking only exists for those undertakings they are authorised to accept. In other words, the Attorney-General can only bring proceedings to enforce undertakings he or she has accepted that relate to compliance with the security obligation (new subsections 313(1A) and 313(2A), a direction issued under new subsections 315A(5) or 315B(12) or notice to provide information or a document under new subsection 315C(3).

Item 27 – Subsections 581(3) and (3A)

237. Item 27 repeals subsections 581(3) and (3A) of the Telecommunications Act relating to the Attorney-General's power to direct a C/CSP to cease using or supplying a service. These sections are reinserted in section 315A (Item 12 above).

Item 28 – Subsection 581(4)

238. Item 28 removes reference to repealed subsection 581(3) of the Telecommunications Act in existing subsection 581(4). The effect of this amendment is that Part 34 only relates to the powers of the ACMA to give a direction to carriers and service providers.

Item 29 – Subsection 581(5)

239. Item 29 repeals subsection 581(5) of the Telecommunications Act to remove the definition of 'security' as this relates specifically to the Attorney-General's powers under Part 34 which have been repealed. The definition of security appears in new subsection 315A(6).

PART 2 – OTHER AMENDMENTS

Telecommunications (Interception and Access) Act 1979

Item 30 and 31 – Subparagraph 202A(a)(ii) and at the end of paragraph 202B(1)(b)

240. Item 30 will amend the TIA Act to exclude the new obligations to protect networks and facilities from unauthorised access and interference in subsections 313(1A) and (2A) of the Telecommunications Act from the purpose of Part 5-4A of the TIA Act.

241. Item 31 will amend the TIA Act so that the notification requirement in section 202B of that Act will not be invoked by the new obligations in subsections 313(1A) and 313(2A).

242. This exclusion from Part 5-4A of the TIA Act is to ensure there is no duplication of reporting requirements between the existing notification obligations in section 202B of the TIA Act and the new specific notification obligation that will be created by this Bill under section 314A of the Telecommunications Act.

Administrative Decisions (Judicial Review) Act 1977

Item 32 – Paragraph (daa) of Schedule 1

243. Item 32 omits the reference to repealed subsection 581(3) in Schedule 1 to the ADJR Act. This is not substituted with a reference to new subsection 315A (the Attorney-General's power to direct that a C/CSP cease using or supplying a service) to give effect to the decision to now allow review under the ADJR Act.

Australian Security Intelligence Organisation Act 1979

Item 33 – Subsection 35(1) (subparagraph (d)(ii) of the definition of *prescribed administrative action*)

244. Item 33 repeals the reference to existing subsection 581(3) in the definition of prescribed administrative action and substitutes a reference to the Attorney-General's directions power under new sections 315A and 315B. The inclusion of these powers in the definition of prescribed administrative action will enable ASIO to provide advice in respect of the exercise of these powers to the Attorney-General in the form of a security assessment. This security assessment will attract the accountability obligations contained in Part IV of the ASIO Act, for example notification requirements and review rights.

Item 34 – Paragraph 38A(1)(b)

245. Item 34 repeals paragraph 38A(1)(b) which references the Attorney-General's direction making powers and substitutes reference to the new sections 315A and 315B.

PART 3 – TRANSITIONAL AND SAVING PROVISIONS

Item 35 – Transitional and saving provisions

246. New subsection 315A(1) will have the same purpose and effect as existing subsection 581(3), which will be repealed under Item 27 of these amendments.

247. Item 35 provides that any directions made by the Attorney-General under the existing subsection 581(3) will continue to operate upon repeal of that provision as if they were a direction in force under section 315A of the Act.

248. Item 35 also provides for the assessments made under subsection 38A(1) of the ASIO Act in relation to existing subsection 581(3) of the Telecommunications Act to continue to have effect upon the commencement of new subsection 315A.

249. Item 35 will also mean that the exemption from review under the ADJR Act of any directions issued under subsection 581(3) will continue upon repeal of this subsection by this Bill.

REGULATION IMPACT STATEMENT

Table of Contents

Purpose

This Regulatory Impact Statement (RIS) considers four options for addressing the ongoing management of national security concerns in the Australian telecommunications sector. Specifically, it relates to the need for Carriers, Carriage Service Providers and Carriage Service Intermediaries (together referred to as C/CSPs) to protect their networks and facilities from unauthorised access and interference. The need for reform and options for reform are considered having regard to industry's preference for a framework that:

- provides a level playing field for protection of networks and facilities for all industry players and does not disproportionally burden some companies over their competitors;
- provides industry with clarity, certainty and flexibility to assist with their commercial decision-making, including to meet their broader operational and commercial requirements in the context of global links;
- allows greater access to, and sharing of, security information between government and industry; and
- gives careful consideration to the regulatory impacts on both C/CSP operations and customers, including removing onerous and/or duplicated processes and obligations on industry.

This document has been prepared by the Attorney-General's Department (AGD) in consultation with Australian Government security agencies; and the Department of Communications. Much of the classified information in the RIS has been provided by security agencies. The RIS has also been developed in consultation with the Office of Best Practice Regulation (OBPR) and the Department of the Prime Minister and Cabinet (PM&C) in accordance with the government's requirements for assessing regulatory impacts of proposed reforms.

The net benefit analysis is largely qualitative rather than quantitative due to limited industry data and case studies to highlight and compare the costs associated with mitigating national security risks. For example, it has not been possible to quantify cost implications of a failure to mitigate a national security risk or the cost of taking remedial or mitigating action. There is not an equivalent industry proxy to substitute the lack of industry data. For this reason, the RIS focusses on transaction costs to industry and not costs associated with potential implications of reduced competition in the supply market or costs of mitigation where legacy systems are replaced or upgraded.

Introduction

In 2004, the *Telecommunications Act 1997* was amended to provide a power for the Attorney-General, in consultation with the Prime Minister and Minister for Communications, to direct a person to prevent or cease the supply of a telecommunications service on national security grounds. Since its enactment, the power has not been exercised. It is an extreme power, and while there have been incidents that have necessitated the power being considered to address

potential national security risks posed by the actions of individual C/CSPs, no Attorney-General has yet issued a direction under section 581(3).

To date, national security risks to telecommunications networks and facilities have been managed through cooperative relationships with the highest risk C/CSPs, relying on their goodwill to implement security advice. Security agencies rely on the power in section 581(3) as a basis for engagement and encouraging cooperation. This approach is risky for numerous reasons (detailed below) and involves often lengthy and costly engagement (for both government and industry) on a case-by-case basis. While section 581(3) provides an ultimate mechanism to address national security risks, there would be wide reaching and significant impacts on market and the community. This calls into question whether it could be used. Security agencies' concern that the current framework is ineffective and inefficient to manage the national security threat to telecommunications infrastructure necessitates consideration of improvements to the current framework.

In late 2011 the AGD considered, in consultation with other agencies, a range of risk management measures to mitigate national security risks to Australia's telecommunications infrastructure. The government agreed to explore a risk-based regulatory framework as a means to improve the way national security risks are managed in the telecommunications sector. As part of this exploratory process, AGD undertook targeted consultation with C/CSPs to inform its assessment of resource implications and the impacts on industry. Industry provided limited information and data which has made analysis and quantification of those impacts challenging.

In 2013, the Parliamentary Joint Committee on Intelligence and Security (PJCIS) undertook a review of three national security reforms and published its report 'Inquiry into Potential Reforms of Australia's National Security Legislation' in June 2013. Following a broad public consultation process, the PJCIS recommended that government amend the Telecommunications Act by establishing a security framework to mitigate security risks to Australia's telecommunications infrastructure (recommendation 19) to provide:

- a telecommunications industry-wide obligation to protect infrastructure and information held on it or passing across it from unauthorised interference;
- a requirement for industry to provide the government with information to assist in the assessment of national security risks to telecommunications infrastructure; and
- powers of direction and a penalty regime to encourage compliance.

The PJCIS further recommended that in developing such a framework government should have regard to the regulatory impacts, particularly on competition, and matters such as how such a framework would interact with existing corporations' law and protections (such as an indemnity against civil action) for service providers who have acted in good faith.

The PJCIS also noted 'warm, if cautious, support of most industry submitters' and supported the introduction of a security framework in their public inquiry. The rationale for recommendation 19 provided by the PJCIS was the potential for misalignment of commercial

interests with national interest where national security is threatened and industry sometimes does not act on the advice of government.[3]

The current proposal for reform was developed taking into account the findings of the report, the feedback the PJCIS received during its consultation processes, and further feedback received from industry through additional consultation on the proposal undertaken as part of the RIS process in 2014. Consultation processes and the industry feedback received are detailed at pages 43 to 46.

This RIS and the proposed reforms aim to respond to the PJCIS inquiry and consider different options for how the existing regulatory framework may be improved.

1 What is the policy problem?

1.1 The Security Problem

Australia's national security, economic stability, prosperity and social wellbeing are increasingly dependent on telecommunications networks and infrastructure that connect us to the Internet. Government and business have increasing amounts of information and records of communications that are stored electronically in telecommunications networks and facilities. At the same time, these systems are becoming more connected to, and dependent on, the Internet to move information nationally and internationally. The telecommunications systems and the information networks to which they are connected are essential parts of our national infrastructure. *[redacted text]*

Australian citizens, businesses and public entities rely on C/CSPs to handle their communications and electronically stored information securely. The C/CSP networks and infrastructure that hold and transmit communications data have become vital to our national interest. However, at the same time, these networks and infrastructure have become attractive targets for those who wish to harm Australian interests. *[redacted text]* The recent hacking of telephone voicemail systems in the UK illustrates the broader implications of an unsecure network – in that case, hacking did not require the expertise and well-resourced capability of a hostile foreign intelligence agency.

[redacted text]

The threats come from a variety of sources: other national states acting in their own national interest; criminal syndicates (in particular well-resourced organised crime networks); business corporations seeking commercial advantage over competitors; political or other issue-specific groups; cyber-vandals and 'hacktivists'.

A key source of vulnerability for telecommunications networks and systems 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

[3]Paragraphs 3.45 and 3.46 of the Parliamentary Joint Committee on Intelligence and Security's Final Report, 'Inquiry into Potential Reforms of Australia's National Security Legislation'.

from foreign countries. This can create further challenges in implementing controls to mitigate personnel, physical and information and communications technology (ICT) security risks in some locations and therefore make networks and facilities more vulnerable to unauthorised interference. *[redacted text]*

[redacted text]

1.2 The Australian Market

Size and composition of the Telecommunications Industry

The telecommunications sector is an important part of the Australian economy, providing employment to over 54 000 Australians and generating revenue of approximately $43.7b (2013-14).[4] In 2010, investment figures for the telecommunications industry totalled approximately $10b with a projected growth to $15b in 2014.[5] Australia's telecommunications sector comprises of approximately 200 licensed carriers (organisations that own networks or facilities used to provide telephony or internet services to the public), and approximately 1360 CSPs (entities that use, but do not own, infrastructure used to provide telephony or internet services to the public). The majority of the telecommunications market in Australia is represented by a small number of larger carriers. The three largest carriers (Telstra, Optus and VHA) account for over 90 per cent of revenue in the telecommunications market and the remaining 10 per cent is dominated by around five C/CSPs. *[redacted text]*

The telecommunications sector forms the backbone to other critical infrastructure sectors in Australia (such as energy, banking and finance). These sectors are increasingly dependent on the telecommunications sector. A serious compromise of the telecommunications sector would have a cascading effect on other critical infrastructure sectors and significantly impact the Australian economy. *[redacted text]*

Developments in the telecommunication market

C/CSPs have benefitted from advances in digital technology, the structural separation of Telstra, the national rollout of 4G networks by various service providers, greater reliance on outsourcing and cloud computing.[6]

Increasingly vendors are offering C/CSPs services which provide all elements for a C/CSP to perform a particular function, such as operations support and business systems, and is sold as a complete bundle. This is often referred to as a 'turnkey solution' and can be a source of vulnerability to unauthorised access and interference making it difficult for C/CSPs to implement controls to mitigate security concerns. *[redacted text]*

[4]IBISWorld Industry Report – *Telecommunications Services in Australia,* March 2014.
[5]Deloitte Access Economic Study, *Large capital projects – defining Australia's investment challenge*, 24 April 2012 published by the Business Council of Australia.
[6]Cloud computing where data is held across international jurisdictions introduces questions about sovereignty. This also introduces architecture vulnerabilities in terms of who has potential access to the data.

Convergence of technology is boosting competition and changes in the market, driving investment in infrastructure and expansion of operating network environments. The NBN rollout will further transform the Australian telecommunications sector, with changes to the telecommunications market's structure and functionality creating new opportunities for C/CSPs to access the Australian market.

[redacted text] Potentially the greatest threats to the security of the telecommunications sector are focused on *[redacted text]* high priority C/CSPs. *[redacted text]* However, the dynamic and fluid nature of the market is driving dynamic change across all levels of the industry. *[redacted text]*

Investment trends suggest most C/CSPs operate on a three to five year business cycle. To keep pace with rapid technological developments, C/CSPs will replace more sensitive parts of their networks and facilities in their entirety at least once during this cycle. *[redacted text]*

There is growing reliance by the telecommunications industry on customer data management programs which use data analytic techniques to increase profit. Industry has been investing heavily in operation support systems and business support systems to develop an understanding of customer requirements and preferences. *[redacted text]*

While C/CSPs have a general commercial incentive to provide customers with a secure environment, this incentive is usually limited to providing business continuity rather than extending to protect against national security threats. Threats to national security may not manifest as a risk to business continuity and most customers, with the exception of government and large corporate accounts, may not have an awareness of these risks to seek assurance. *[redacted text]*

As well as technical and market changes, intense cost pressure is being applied to C/CSPs in the Australian market. In the past ten years significant changes in technology have altered the shape of the telecommunications market. *[redacted text]* With C/CSPs under greater pressure to minimise costs, there is a commercial motivation to accept higher risk propositions for the supply of equipment and services. Fiduciary duties on company boards and directors can operate as a disincentive to consider national security risks when making procurement decisions.

1.3 Current Regulatory Framework

The regulatory framework for managing national security risks in the telecommunications sector places responsibility for managing those risks on C/CSPs and not suppliers or other parts of the sector. The current telecommunications legislative framework relies on three key provisions.

- Section 313 of the Telecommunications Act requires carriers and nominated CSPs to do their best to prevent networks and facilities from being used in the commission of an offence under Commonwealth, State or Territory laws. Carriers and nominated CSPs must provide help as is reasonably necessary to government to help safeguard

national security through the operation of networks or facilities or supply of carriage services.

- Section 202B of the *Telecommunications (Interception and Access) Act 1979* (TIA Act) requires carriers and nominated CSPs to notify government (through the Communications Access Coordinator) of material changes to their networks and facilities that could affect their ability to assist safeguarding national security under section 313 of the Telecommunications Act.
- Section 581(3) of the Telecommunications Act provides the Attorney-General with the power to issue a direction to cease a service that is prejudicial to security.

Under the Telecommunications Act, C/CSPs are also regulated by licence conditions and service provider rules respectively. There are however, no levers to require C/CSP engagement and information sharing. While section 202B of the TIA Act provides a formal mechanism for notification of material changes to networks and facilities, it does not currently operate to support early engagement and notification around potential changes to networks and procurement plans. The TIA Act does not specifically address supply chain risks, hardware and software vulnerabilities or security risks to the confidentiality, integrity and availability of telecommunications infrastructure.

Security agencies rely on section 313 to require C/CSPs to engage where security agencies become aware of a potential security threat posed to a network or facility. However, this provision only allows for limited information to be proactively shared and relies heavily on a cooperative relationship and the goodwill of C/CSPs.

There is a large legislative gap between the obligations on C/CSPs in section 313 of the Telecommunications Act and 202B of the TIA Act and the ultimate use of the power to cease a service under section 581(3) of the Telecommunications Act. The power in section 581(3) was designed for extreme circumstances, reflected by the fact that the Attorney must first consult the Prime Minister and Minister for Communications before exercising such a power. The majority of the Australian market is serviced by a small number of carriers, Telstra, Optus and VHA – if a part or whole of a service was directed to cease, it would have a significant impact on the market. There have been circumstances in which the government has considered exercising the power, however, the broad and, potentially, significant implications of issuing such a direction means that it has never been exercised to date.

Currently, there is an absence of effective levers to encourage industry to engage with security agencies about potential national security risks arising through procurements, or to incorporate security considerations into business and investment decisions at an early stage. Management of security risk relies heavily on *[redacted text]* corporate goodwill and the threat of the potential use of section 581(3) to encourage engagement, information sharing and cooperation. *[redacted text]*

Growth and rapid changes to the telecommunications sector mean it is increasingly unsustainable to risk manage national security outcomes in this way for both the market and government. Some large carriers acknowledged this during the PJCIS inquiry, expressing warm, if cautious support for a regulatory framework to better guide security risk management

in the telecommunications sector. Consultation processes and the industry feedback received are detailed at pages 34 to 37.

[redacted text]

2 Why is government action needed?

[redacted text]

There are compelling reasons why government intervention is necessary to enhance the current framework for managing telecommunications national security risks.

2.1 National security

[redacted text] The pace of technological change presents serious challenges to the security of telecommunications data – risks can arise from hardware vulnerabilities, accidental misconfiguration, external hacking and trusted insiders. The implications of these threats and risks are significant.

Australian Government agencies have been the victim of cyber intrusions – in one case the loss of sensitive intellectual property was significant. Globally, data breaches of major commercial entities (such as Target in the United States) reduce business confidence and that of the community in online transactions. The cyber security breach into Target (US) in 2013 shows the extensive costs to business of unsecure networks – that breach is estimated to have cost Target $148m.[7] There were flow on costs to customers who had their credit card details stolen, and other businesses such as banks which had to reissue credit cards**.**

In Australia, security agencies are seeing an increasing number of attempts to gain unauthorised access to government systems. In 2013, the Australian Signals Directorate's Cyber Security Operations Centre recorded 2168 serious cyber incidents, up 21 per cent on 2012 when there were 1790 reported incidents and 1259 in 2011. These were reported incidents: there are likely to be thousands of additional incidents that go unreported. As highlighted in the Target example, remediation costs associated with a serious cyber event can be very costly for businesses.

Australian businesses, individuals and government rely on the ability of C/CSPs to store and transmit their data safely and securely and protect it from potential national security threats.

[7] *Target Provides Preliminary Update on Second-Quarter Expenses Related to the Data Breach and Debt Retirement*, 5 August 2014, <http://pressroom.target.com/news/target-provides-preliminary-update-on-second-quarter-expenses-related-to-the-data-breach-and-debt-retirement>.

Although telecommunications infrastructure is privately owned and managed, the broad scale implications of any compromise to the security of those networks means that government must ensure that those networks are appropriately managed and protected.

2.3 Inefficiency and ineffectiveness of existing regulation

The current regulatory framework is ineffective and inefficient to manage the increasing threat posed to telecommunications infrastructure.

While section 581(3) of the Telecommunications Act provides government with a mechanism to intervene to shut down a service where the operation of that service presents national security risks, it is such an extreme measure that it has never been used. The 'blunt instrument' nature of section 581(3) is not a reasonable or proportionate response to manage all but the most severe security risks. The consequence of a complete shut-down of a service, say a 4G network, would be dire for customers. Consequently, there is growing uncertainty for industry and security agencies as to if and when the power will ever be used, and the threshold that would need to be met to warrant the exercise of the power.

The current approach to managing national security relies on the goodwill of industry to cooperate with security agencies. While cooperative partnerships between industry and government are critical to effective management of security risks in the telecommunications industry, relying on good will and cooperation alone means that processes for managing risks are uncertain, protracted and inefficient. In the absence of a clear statement of government expectations, there are no effective levers for security agencies to manage national security risks.

Security agencies need timely access to industry information to assess potential national security risks and threats and provide advice to C/CSPs on the management of those risks. *[redacted text]*

Currently, C/CSPs are not required to provide information to security agencies. The absence of clear obligations results in ad hoc, reactive and delayed approaches to address any potential concerns. *[redacted text]* Rapid changes in market dynamics and technologies increases opacity – C/CSPs initially considered to present low risk can suddenly present a high risk due to factors such as rapid expansion in market share or expansion of services. *[redacted text]*

In addition to ad hoc and ineffective information sharing mechanisms, addressing any security concerns relies on effective cooperative relationships. *[redacted text]*

The existence of fiduciary duties obligating company directors and boards to act in the financial interest of the C/CSP presents a real challenge to having national security advice taken into account when designing and procuring networks and capabilities. No matter how good the partnership between government and industry, if implementing security advice presents a cost or the loss of a business opportunity, directors and board members may choose to ignore it and prioritise the commercial interests of the company.

[redacted text] Continued reliance on the goodwill of a subset of industry is unsustainable due to the commercial pressure from shareholders to compete in a relatively small market. *[redacted text]* It is risky to rely on C/CSPs to act altruistically in the absence of clear legal obligations to actively protect networks from national security risks.

The lack of certainty around government security expectations means that efforts to manage national security risks that do arise are delayed, complex, inefficient and costly to both parties. *[redacted text]* Clearly, as the threat increases and greater cooperation is required to address national security risks, it is unmanageable to rely on Ministers and CEO's to become involved in long and protracted negotiations to manage national security risks.

[redacted text]

In some cases, contracts might be finalised and steps taken to implement changes to networks and facilities which cannot be undone or risks effectively mitigated in the future. *[redacted text]*

In summary, government action is needed because:

- current mechanisms rely on goodwill and cooperation which is not an appropriate mechanism for managing national security risks;
- there is lack of clarity for government agencies and industry on how national security risks are to be managed and enforcement action to be taken;
- industry does not have access to the threat picture to enable decisions to be informed by national security risks;
- industry is not currently required to take responsibility for protecting their networks and facilities from national security threats presented by suppliers of equipment and managed services; and
- the current patchwork of legislative provisions do not provide a comprehensive regime for the ongoing management of national security risks to telecommunications infrastructure.

2.4 Broader flow on impacts of secure telecommunications infrastructure

In addition to ensuring effective management of national security risks, protecting networks and facilities from unauthorised access and interference will help reduce the level of cyber-attacks. Ensuring C/CSPs are not using compromised equipment will make it harder for hostile actors to mount cyber-attacks against networks and facilities, reducing the level and severity of attacks. Reducing cyber-attacks has flow on cost benefits to the telecommunications sector and potentially other critical infrastructure sectors.

Likewise, protection of telecommunications infrastructure will enhance protection of equipment and managed services from data breaches that can occur as a result of less secure and reliable networks. Targeted consultation with industry in early 2012 highlighted that industry itself appreciated the importance of protecting the confidentiality, integrity and availability of their networks.

3 Objective

The objective of the proposed reform is to provide a more effective and efficient framework for managing national security risks to telecommunications networks and facilities posed by suppliers of equipment and managed services.

An efficient security framework would be achieved by:

- timely information sharing by industry on material changes to networks or facilities to enable the assessment of national security risks;
- timely provision of threat information to industry by security agencies;
- effective and timely mitigation of security risks; and
- reduced burden, cost and effort on industry through early engagement and clarity about government's expectations.

In achieving this objective the framework should:

- build on the collaborative and cooperative relationships in place between industry and government to achieve national security outcomes;
- engage C/CSPs in actively managing national security risks – C/CSPs are considered best placed to manage the risk as part of their commercial decision-making and ultimately responsible for ensuring their infrastructure does not pose national security risks;
- provide flexibility for how a C/CSP protects its infrastructure from unauthorised interference and; and
- focus on managing security risks in high value C/CSPs and in the core and sensitive parts of their networks and facilities.

4 What policy options have been considered?

As noted above, in 2013 the PJCIS considered the issue of reform of the current regulatory regime to manage national security risks to telecommunications networks. Following a process of broad consultation, it considered further government regulation was the best option for managing these risks. In particular, amending the Telecommunications Act to create an enhanced framework comprised of three key components: an industry-wide obligation to protect telecommunications infrastructure from unauthorised interference, an obligation on industry to provide information to government; and direction powers and a penalty regime to encourage compliance. A **regulatory option** consistent with the PJCIS recommendation is considered at Option 3.

To meet best practice regulatory requirements, three other options are also considered. Option 1 considers retaining the **status quo**. As outlined above, the current framework comprises of a mix of regulation and self-regulation.

Option 2 considers the development and registration of an **industry code** (a Code) under Part 6 of the Telecommunications Act. There are two approaches to developing a Code – a self-

regulatory model or a quasi/co-regulatory model. Only a quasi/co-regulatory approach is considered in this RIS.

During consultation processes, the development of a voluntary Code was suggested by some C/CSPs as an alternative to further regulatory reform. However, to date industry has not elected to pursue this option nor seems likely to proactively do so.

In addition to the direct regulatory approach considered in Option 3, a more comprehensive direct regulatory option is explored in Option 4. Option 4 adds an extra layer of regulation to Option 3, imposing an industry-wide obligation to produce **annual investment plans**. This approach is modelled on the more comprehensive regulatory approach adopted by New Zealand to manage security risks in the telecommunications sector.

The option of de-regulation by removing the existing national security provision is not considered viable and is not explored. While the existing regulation is reactive and best suited to extreme levels of national security risk, AGD and the PJCIS engagement with industry reflected broad acceptance of the importance of the management of national security risks to Australia's telecommunications infrastructure.

4.1 Option 1 – Retaining the status quo

As detailed in section 1.3 Current Regulatory Framework, the existing regulatory framework for managing national security risks in the telecommunications industry relies on three key provisions and cooperative engagement with security agencies.

Broad objectives of the Telecommunications Act include that telecommunications be regulated in a manner that 'promotes the greatest use of industry self-regulation'.[8] Maintaining the status quo would allow industry to continue to self-manage national security risks until they reach a point where the risk posed to national security engages regulatory action under section 581(3).

As noted above, it has been ten years since the enactment of section 581(3), which has provided sufficient opportunity to examine the effectiveness of the current regime. While to date the current framework has met the objective of addressing perceived security risks to the sensitive and core parts of telecommunications infrastructure, the process by which this is achieved is not considered to be effective. As detailed above, under the existing arrangements there are no relevant levers to require industry to provide information. *[redacted text]*

For both industry and government there is a lack of transparency, clarity and accountability. *[redacted text]*

Under the status quo, while ultimately the government can address security risks by exercising the power to cease a service in s 581(3) of the Telecommunications Act, there is no certainty as to the threshold at which the government would exercise this power. As such, there is a lack of clarity about the responsibility C/CSPs are expected to exercise in operating and managing

[8]Section 4 of the *Telecommunications Act 1997*.

their infrastructure to protect it from national security risks and how proactive government expects industry to be. Without clear rules and graduated enforcement measures, the process of engagement can be unpredictable and costly. The competitive state of the market is resulting in significant cost pressure and the status quo is not always effectively influencing behaviour, particularly where national security risks are not clearly visible to members of industry.

4.2 Option 2 – Industry Code (Quasi/Co-regulation)

An industry Code could be developed and registered under Part 6 of the Telecommunications Act. Part 6 provides a mechanism for the development of Codes by industry and a process for registration and enforcement.

If ACMA is satisfied that an Industry Code is necessary or convenient to regulate C/CSPs performance to achieve national security outcomes, it can issue a written notice to an industry representative body such as the Communications Alliance to develop an Industry Code and present it for registration (section 118 of the Telecommunications Act). Industry, through the representative body, would then be responsible for developing and drafting a Code with appropriate rules and provisions that sought to clarify government's expectations in relation to national security.

Subject to subsection 115(1) of the Telecommunications Act, Code provisions could be drafted to impose industry-wide obligations to protect telecommunications infrastructure from interference and require industry to provide information to government.[9] A Code, developed with significant technical expertise of security agencies, could clarify government's expectations about national security management, draw on existing recognised principles in security management and set out when and how C/CSPs should engage with security agencies. For example, a Code could specify when and how a C/CSP needs to provide information about potential procurements.

If the Code satisfied the objective of providing a mechanism for the efficient management of security risks, and additional requirements under sections 112 and 117 of the Telecommunications Act,[10] the ACMA could register it under section 136 of the Telecommunications Act.[11] Registration is regarded as a critical step to the effectiveness of an industry Code under Option 2. It provides legislative support for the enforcement of a Code and attracts ACMA's enforcement powers to issue a Direction to Comply (section 121) and give Formal Warnings (section 122). Failure to comply with an ACMA direction may attract civil penalty provisions.

If ACMA became aware that a C/CSP was operating in breach of a Code provision it could investigate the matter, gather evidence and then determine whether or not to take enforcement

[9] Section 115(1) provides that an industry Code has no effect to the extent to which compliance with the Code is likely to have the direct or indirect effect of requiring customer, equipment, customer cabling, a telecommunications network or a facility to have particular design features or meet particular performance requirements.
[10] Section 112 'Statement of Regulatory Policy' and section 117 'Registration of industry Codes'.
[11] 'ACMA to maintain Register of industry codes and industry standards'.

action. Security agencies are more likely to be aware of any non-compliance with the Code than ACMA and trigger the investigation process. However, as ACMA is an independent authority it will not instigate an investigation unless it is satisfied that the matter requires investigation. The usual timeframe for investigations into complaints of non-compliance with Code provisions can take approximately six months.

The ACMA and Communications Alliance have indicated the period of development for a complex Code can take around two years. Before presenting a Code for registration, the draft Code must undergo a period of industry and public consultation. ACMA cannot register a Code unless it is satisfied that there has been adequate consultation and that consideration has been given to the feedback received. Consultation processes can take several months. The registration process itself usually takes approximately two months (this includes mandatory consultation with the Information Commissioner).

In the event that industry does not provide a Code for registration or the Code does not meet regulatory objectives and/or the requirements of registration, ACMA can develop an Industry Standard. Without registration, there are no legislative enforcement mechanisms and compliance remains voluntary. Compliance with a registered Industry Standard is compulsory – it would operate much like the proposed regulatory option set out in Option 3 and for this reason an Industry Standard has not been separately considered.

4.3 Option 3 - Amending existing legislation to introduce a security framework

A risk-based security framework could be established for all C/CSPs by strengthening the existing national security provisions in the Telecommunications Act.

The framework would consist of several high-level key obligations on industry with details contained in supporting guidelines. Such a framework would codify informal relationships to provide industry with clarity about government's expectations of the management of risks to national security. In particular a framework would go beyond the current obligation to provide assistance to safeguard national security and focus on the ability of a C/CSP to manage the security of its infrastructure and the information held on it. The aim of such a regulatory framework would be to promote risk informed management of security in the telecommunications sector.

This could be achieved by amending the Telecommunications Act to:

- require all C/CSPs to their protect networks and facilities from unauthorised access or interference – this would be achieved by demonstrating 'competent supervision' and 'effective control' over a C/CSP's networks (defined below);
- empower government to require C/CSPs to provide information to facilitate security agencies developing threat assessments;
- facilitate provision of threat information from security agencies to industry; and
- ensure industry's cooperation in managing national security risks by imposing proportionate and graduated compliance and an enforcement regime consisting of powers of direction and civil (financial) penalties.

Competent supervision – would require a C/CSP to maintain technically proficient oversight (either in-house or through a trusted third party) of: the operations of their network; location of data; and parties with access to network infrastructure. It also involves a C/CSP maintaining a reasonable ability to detect security breaches or compromises.

Effective control – would require a C/CSP to maintain direct authority and/or contractual arrangements which ensure that its infrastructure and the information held on it are protected from unauthorised interference. This could include arrangements to: cease contracts where there has been a security breach; undertake mitigation or remedial actions; monitor, document and remedy security breaches; and reclaim customer data and network systems where unauthorised interference to a network has occurred.

Government would provide guidance, through administrative guidelines and provision of advice from security agencies, to assist industry to understand and meet its obligation and to inform C/CSPs how they can maintain competent supervision and effective control over their networks. Guidance would be tailored to C/CSP service types (for example internet service providers (ISP), backhaul service providers, and mobile virtual network operators) and distributed to C/CSPs prior to commencement of a security framework.

The framework would provide government a graduated suite of enforcement measures (including the power of direction) to provide industry with greater incentive to engage cooperatively with government. For example, first government would provide advice and guidance to encourage risk informed management of security concerns. Second, where potential issues of concern are identified, the preferred approach would be to engage with the relevant C/CSPs to establish whether national security concerns can be cooperatively addressed. Third, in cases where engagement with C/CSPs proves to be ineffective, or there is a disregard of security information that jeopardises the government's confidence in the security and integrity of Australia's telecommunications infrastructure, powers of direction could provide a proportionate means to achieve compliance. There may be instances in which a C/CSP seeks a direction to provide its board with a clear mandate to guide commercial decision making.

Directions could involve targeted mitigation or remediation of security risks, including modifications to infrastructure, audit, and ongoing monitoring, with costs to be borne by the relevant C/CSP. Grounds for directing mitigation or alternative actions would ultimately be determined by security agencies, based on an assessment of risk following their engagement with a C/CSP. The powers of direction would serve as a means to support the existing powers in the Telecommunications Act relating to national interest matters. Based on the frequency of major changes to core and sensitive parts of networks that are likely to give rise to national security risks, it is anticipated that directions will be issued infrequently.

4.4 Option 4 - Amend existing legislation to introduce security framework and require annual investment plans

This option builds on the security framework outlined at Option 3 with the additional requirement for C/CSPs to provide government with an annual investment plan. Investment Plans would provide a multi-year outlook of C/CSP's planned procurements.

The requirement to provide an investment plan would be modelled on the provisions in the TIA Act to provide annual interception capability plans (ICPs) to the Communications Access Coordinator by carriers and nominated CSPs although it would be broadened to cover all material business decisions and procurements. Around 200 carriers and nominated CSPs already provide ICPs to the Communications Access Coordinator each year and have dedicated teams to manage this process.

Additional investment plans could be managed in a similar way, although the scope would potentially increase substantially to include the additional 1360 CSPs, if applied universally. This would place a significant additional burden on the vast majority of low priority CSPs as well as low priority carriers.

Annual investment plans would provide security agencies with detailed information, in advance, of upcoming procurements and other changes to networks that might not already be captured in annual interception plans. This would adopt a regulatory approach similar to New Zealand which is considered to be one of the most comprehensive. It would enhance security agency capability to develop detailed threat assessments and better target engagement.

5 What is the likely net benefit of each option?

The net benefits of each option are assessed below in how they meet the reform objectives and outcomes outlined above in section 2.1.

The regulatory impact and costs associated with each proposed option for reform have been calculated using data and estimates provided by industry during the various consultation processes. The PJCIS noted the lack of detailed information in response to the question of the costs of regulatory impact on industry. Consequently, costs associated with implementation of a particular option have, to a large degree, been calculated having regard to the types of impacts and costs currently associated with engaging with government to manage security risks and concerns. Difficulties quantifying benefits of options means that the net benefit analysis necessarily focuses on risks associated with options and the significance of those risks to the overall effectiveness options and the achievement of national security outcomes.

A further complexity with calculating costs associated with compliance is that such costs are subject to the risk profile of a C/CSP and the level of risk presented by a particular procurement or operational decision affecting infrastructure and the action required to mitigate risk, at any given time. Each scenario is likely to be highly variable making any attempt to quantify the potential cost implications at an industry-wide level at each point in this process difficult, if not impossible.

A key assumption is that costs associated with implementing mitigation measures will be less costly to C/CSPs (and therefore possibly to suppliers and customers) than remedial work. *[redacted text]* An absence of industry data means it has not been possible to quantify the cost of mitigation or remedial measures, including addressing legacy system risks that arise during system upgrades. Any attempt would be purely speculative as there is not an appropriate proxy against which to estimate costs.

The current cost to industry under the status quo is business as usual and reflected as a nil cost. This provides a neutral benchmark for considering the impacts of proposed reform options. However, there are significant costs for industry associated with compliance under the status quo due to the resources that may need to be devoted to protracted engagement. *[redacted text]* A key change under each of the alternative options would be to impose these costs sector-wide on a risk basis – noting that that the costs would still be proportional to individual C/CSP risk profiles.

Consequently, each reform option presents a relatively low regulatory burden compliance cost (around $500 000 per year) above business as usual or the status quo and is likely to have the most impact on those C/CSPs that do not have any mechanisms in place for managing any security risk. A key assumption is that the costs to industry of implementing any of the proposed options are likely to be minimal in comparison with revenue generated and therefore unlikely to operate as a barrier to market-entry or competition. The benefits associated with the three options to reform the status quo are also considered modest. They are important in terms of efficiency in achieving security outcomes, with greater visibility for security agencies of potential national security risks, and more targeted advice from security agencies to prevent delays to C/CSP business plans.

Competition impacts – suppliers

The management of national security risks posed through the supply of equipment and services means that there will be some restrictions, where a service is, or is likely to be, prejudicial to security. However, these restrictions already exist under the status quo. *[redacted text]* While there is likely to be an increased impact on the supply market under options 2, 3 and 4 through a more effective mechanism to inform C/CSPs about risks, it is not possible to predict with accuracy the difference in the impact under each option.

[redacted text] It is anticipated the security framework will minimise competition impacts by encouraging C/CSPs to work with suppliers on how they can provide equipment and services enabling them to maintain competent supervision and effective control over their networks and facilities. *[redacted text]*

Impact on Customers

Restrictions and/or additional requirements being placed on business solutions for some C/CSPs could result in a cascading affect to the market-place with a portion of the higher costs passed onto customers (both individuals and business). A cost to a C/CSP of meeting existing

national security obligations of providing a service that is not prejudicial to security is likely to have only a marginal impact on consumers. The costs are likely to be nominal – in the range of a few cents per service due to the wide customer base and revenue stream compared to the relatively modest scale of costs against the sector's revenue. *[redacted text]*

In any event, if security risks are identified, remedial costs under the status quo could potentially have a significant impact on the customer. As noted above, costs associated with remediation or ceasing a service are likely to increase charges to customers or see services withdrawn (albeit at a likely low per-customer level).

The cost-benefit analysis for each option relies on the following broad assumptions:

- Options discussed below do not remove existing regulatory powers – the current power under subsection 581(3) of the Telecommunications Act would remain available for the most serious security breaches.
- Costs may arise if C/CSPs need to mitigate high risk network designs at a late stage or if more expensive but more secure supply options need to be chosen.
- *[redacted text]*

5.1 Option 1 – retaining existing regulation under the status quo

5.1.1 Costs of Option 1

Industry impact

Continuing the existing regulation would not result in additional administrative or compliance costs for industry or government. Under current engagement processes costs would continue to be incurred by industry in engaging in potentially lengthy negotiations on what constitutes a security risk and what constitutes appropriate mitigation action. *[redacted text]*

To date larger C/CSPs have been bearing any administrative and compliance costs associated with managing security risks through processes of engagement.

Regulatory Burden and Cost Offset Estimate – Option 1: Status quo

Average Annual Regulatory Costs (from Business as usual)				
Change in costs ($M)	**Business**	**Community Organisations**	**Individuals**	**Total change in cost**
Total by Sector	$0	$0	$0	$0
Cost offset ($M)	**Business**	**Community Organisations**	**Individuals**	**Total by Source**
Agency	$0	$0	$0	$0
Within portfolio	$0	$0	$0	$0
Outside portfolio	$0	$0	$0	$0
Total by Sector	$0	$0	$0	$0
Are all new costs offset? N/A **☐ yes, costs are offset**				
Total (Change in costs - Cost offset) ($M) $0				

5.1.2 Benefits of Option 1

[redacted text]

Additionally, C/CSPs benefit from the knowledge that the blunt regulatory instrument (use of section 581(3)) with far reaching consequences is unlikely to be used, enabling them to take some risks with a potentially unrestricted market of vendors of equipment and services and base decisions on commercial advantage.

This option also provides the greatest flexibility to industry as to when and how it engages with security agencies and matters concerning national security. Low risk C/CSPs are likely to be able to avoid putting in place mechanisms to effectively monitor and protect their networks from interference and access, without national security agency engagement.

5.1.3 Risks of Option 1

Without a clear principles-based security framework, uncertainty for industry and government will continue. Uncertainty for business usually results in greater costs in the longer term and could stifle innovation and investment in infrastructure development for some C/CSPs.

[redacted text]

Industry would continue to be pressured by shareholders to pursue lower cost procurements in the absence of clear government statements of national security risk management expectations. Where a C/CSP engages a supplier with potential risks *[redacted text]*, security agencies would not have the ability to ensure that mitigation measures are put in place to manage these risks.

[redacted text] Cost savings of proceeding with a cheaper supplier may end up causing significant future cost implications if remedial action is required to avoid a direction to cease the service under section 581(3). This is likely to result in increasing pressure on the Attorney-General to engage his or her formal power, while balancing this with competing impacts on competition, the market and consumers. *[redacted text]*

Option 1 does not meet the objective of providing a mechanism to proportionally manage risks. It leaves risk management in the hands of security agencies without effective levers to engage C/CSPs.

The consultation process and ongoing dialogue with industry *[redacted text]* indicates that the status quo is problematic for justifying why national security should take precedence over commercial imperatives. Industry seeks a clear mandate from government that they can provide to their boards, rather than the vague threat of invoking section 581(3). This certainty, that would enable business decisions and that gives appropriate regard and weight to security concerns, is not achievable under Option 1.

5.1.4 Summary of the Net Benefits of Option 1

This approach relies on the goodwill of industry along with some government targeted engagement *[redacted text]* managing to contain cyber security vulnerabilities. The status quo will not, however, provide for an effective response to the potential growing area of vulnerabilities as industry is not required to voluntarily provide information or have regard to security agency advice.

This has, however, resulted in delayed decision making and significant and avoidable demands on the time of senior executives in industry, as well as Ministers and senior officials in government. Timeliness is not an outcome of the status quo. *[redacted text]*

[redacted text]

There are no added regulatory costs associated with this option. However, existing costs remain uncertain and difficult to predict for industry given the potentially huge costs associated with any protracted engagement process. This option fails to adequately balance the costs to industry of commercial autonomy vis-a-vis the risk of national security threats. *[redacted text]*

5.2 Option 2 – Co-regulation

5.2.1 Costs of Option 2

Industry Impact

A Code option would attract greater compliance costs for industry. These additional costs, above existing regulatory obligations and business-as-usual activities, relate to ensuring that their management of national security risks aligned with the Code. The limited data provided by industry means these costs are estimates only and based on a break-down of possible administrative and compliance related activity.

Costs associated with developing a Code

There is potentially significant up-front costs associated with industry developing a Code (start-up cost estimated at $679 142 to fund staff to develop and communicate expectations for a Code and initial implementation across the sector) that does not arise under other options.

Responsibility for the development of a registered Code would likely reside with an industry association, such as Communications Alliance. As such, it represents a marginally higher administrative start-up cost to industry than guidelines developed by government with industry consultations. Establishment costs would arise from C/CSPs being required to provide resources to develop a Code followed by ongoing self-assessment to ensure their compliance.

Costs to industry associated with the establishment of a Code is based on a period of six weeks to develop the code (210 hours) from 20 C/CSP staff, coordinated by Communications Alliance over a two year period. Costs associated with registration processes include a minimum of 2 months including consultation processes.

Costs associated with implementation and compliance

The assumption for implementation of the Code has been estimated at three hours for each of the 1560 C/CSPs, which would involve reading and understanding a Code and self-assessing whether any changes to network and information security and resilience are required. While it has been assumed that the status quo involves a level of information security management, the codification would clarify this and spread the costs across industry.

The overall ongoing cost to industry each year is estimated at $292 100 which includes C/CSPs' maintenance, updating (every three years) and ensuring compliance with a Code. Maintenance and review of the Code has been factored to occur every three years to take into

account potential changes in technology and the market. Communications Alliance members would need to review, update and consult on any changes to code provisions which is estimated to require the equivalent of 35 hours for 20 C/CSPs per annum over three years (or 105 hours over three years).

Costs associated with compliance with Code provisions is difficult to quantify, as it will ultimately depend on the action required for a C/CSP to ensure its networks and facilities are secure and protected from unauthorised access and interference. This will vary across all C/CSPs.

The estimated cost for undertaking monitoring of networks and infrastructure to assess national security risks is the equivalent of at least two hours for each C/CSP per annum. This would involve taking into account the spectrum of effort depending on the exposure to national security risks and would range from engagement with security agencies on high national security risk propositions through to the vast majority of engagement to keep industry informed of emerging threats and risks.

Table 5.2 below breaks down the regulatory life-cycle costs of a Code from development to ongoing compliance. These relatively modest costs would likely be passed on to customers while potential enforcement action would be a matter to be resourced through the ACMA.

Table 5.2 – Industry Code Costs

Activity	Number of C/CSPs	Number of staff per C/CSP	Hours per staff member	Frequency	Cost
Establish an industry Code or standard	20	1	210	[start up]	$321 216
Incorporate industry Code or standards	1560	1	3	[start up]	$357 926
Update industry Code or standard	20	1	35	Every three years	$53 482
Compliance with an industry Code	1560	1	2	Each year	$238 618

Compliance costs would also include costs associated with meeting requirements in relation to C/CSP's complying with code provisions that place obligations to meet with security agencies

on a regular basis, providing information about networks, facilities and procurements. The costs would be similar to those under Option 3 assuming the Code incorporated similar requirements.

Costs to government

Participating in Code development is likely to involve officers from AGD, ACMA and security agencies. It is estimated this would take approximately two years to develop – these costs would be absorbed within existing functions and resources of relevant government agencies. The registration process and assessment of a Code would be undertaken by the ACMA as one of its functions under the Telecommunications Act.

There is an ongoing role for security agencies in engaging and monitoring compliance with the Code. Similar to the costs proposed under options 1 and 3, security agencies would be expected to engage with C/CSPs about national security risks under a Code, which would require up to five additional officers to meet demand from C/CSPs for national security assessments and advice ($700 000). These officers would also engage closely with the ACMA to escalate enforcement of non-compliance with provisions in a Code and advice to mitigate national security risks.

The additional oversight and enforcement functions for the ACMA (assumed to be three staff at $400 000) and costs associated with security agency monitoring and engagement would be expected to be cost recovered, consistent with the funding of existing regulatory functions. The ACMA has advised that to oversee and enforce compliance for national security purposes, if would require around $1m for capital costs to equip itself to protect information. The estimated total costs of $2.1m to establish and administer the Code are likely to be passed to industry through the Annual Carrier Licence Charge.

Regulatory Burden and Cost Offset Estimate – Option 2: Co-regulation

Average Annual Regulatory Costs (from Business as usual)				
Change in costs ($M)	**Business**	**Community Organisations**	**Individuals**	**Total change in cost**
Total by Sector	$0.360	$0	$0	$0.360
Cost offset ($M)	**Business**	**Community Organisations**	**Individuals**	**Total by Source**
Agency	$0	$0	$0	$0

Average Annual Regulatory Costs (from Business as usual)				
Within portfolio	$0	$0	$0	$0
Outside portfolio	$0.578	$0	$0	$0.578
Total by Sector	$0.578	$0	$0	$0.578
Are all new costs offset? **☐ yes, costs are offset**				
Total (Change in costs - Cost offset) ($M) -$0.218				

The regulatory cost of offsets noted in the above table have been identified within the Communications portfolio. The cost offsets are taken from the cost savings arising from the removal of retail price controls in telecommunications (costs have been agreed with OBPR and reported in Q1 2015).

5.2.2 Benefits of Option 2

A Code would be supported by some members of industry who would prefer to develop their own rules and obligations. This too would align with the general objective of the Telecommunications Act, to promote the greatest use of self-regulation (noting this is a quasi-regulatory option).

A Code would meet the objective of clarifying the expectations of government. It would promote greater transparency and accountability using a self-regulatory approach which sought to continue security agencies' focus on engagement and developing cooperative relationships with industry. A Code could also set out government's expectations about triggers for engagement with security agencies on potential national security threats and requirements in relation to information sharing and rules. This would ensure sensitive information provided by government to industry is appropriately managed and protected.

One of the key factors affecting the current framework is that C/SCPs lack a proper understanding of the risks and threats some suppliers provide. A Code could provide a proper framework for the exchange of information held by security agencies (where a Code provided rules for the handling of sensitive information). Provision of more detailed information by security agencies would enable industry participants to make informed decisions about their procurements and outsourcing material.

If a Code was drafted on the basis of imposing industry-wide obligations to protect and control networks, it could clarify that responsibility for protecting telecommunications infrastructure

rests with C/CSPs and provide an enforcement regime to penalise non-compliance. It could also assist with information sharing by clearly outlining what is expected.

5.2.3 Risks of Option 2

Section 115 of the Telecommunications Act poses a risk to the effective operation of a Code dealing with how C/CSPs are to manage and protect their networks and facilities. Section 115 provides that a Code has no effect to the extent that compliance is likely to have the effect (whether direct or indirect) of requiring customer cabling, a telecommunications network or a facility to have particular design features or to meet particular design requirements. It is foreseeable that in seeking to address a potential security risk provided by a particular supplier or managed service that a Code provision may directly or indirectly engage section 115. This casts significant doubt around whether a Code can be used to put in place enforceable obligations of the type that might be required to manage telecommunications infrastructure security. The Telecommunications Act could be amended to remove the restrictions in section 115 for Codes dealing with management of national security risks. However, such an amendment would require careful consideration, given the potential wider implications for the use of Codes, because it could broaden the matters that have been deemed appropriate to be regulated through a Code.

The enforcement mechanisms do not provide for a quick and targeted resolution of non-compliance. In particular the direction power is linked to compliance with particular Code provisions which may not adequately target action to address the particular security risk. The effectiveness of a direction to secure national security outcomes is dependent on the effectiveness of the Code provisions to address specific national security risks. For example, the security concern may relate to failure to implement advice of security agencies – unless the Code contained broad provisions that required compliance with advice of security agencies (noting that such a provision may not be enforceable according to the current operation section 115), a direction to comply may not achieve a particular security outcome.

The processes involved in exercising enforcement powers would be less efficient than processes under Option 3. For example, if a C/CSP is non-compliant with obligations under the Code which presented a national security risk, security agencies would request the ACMA to issue a direction to comply with the Code. As an independent statutory agency, the ACMA would need to develop its own brief of evidence before taking regulatory action rather than just relying on external advice from security agencies on national security risks.[12] If compliance is still not achieved following the direction the ACMA could issue a formal warning and seek the imposition of a pecuniary penalty through the Federal Court. Both of these processes can be lengthy, costly and ultimately delay the achievement of national security outcomes.

As with the status quo, delay in achieving security outcomes could increase risk and cause delay to business decisions. C/CSPs could potentially use these processes to ‘game’

[12] Since the Telecommunications Consumer Protections Code (TCP) commenced in April 2010 the ACMA has issued 109 warnings, 10 directions to comply and infringement notice.

government. The risk or threat could also increase over the period of enforcement to the point that it may not be able to be managed effectively or that remediation is no longer possible (i.e. once infrastructure or capability is moved offshore it is almost impossible to reverse or mitigate).

The ACMA advises compliance and enforcement actions under a Code are better suited to minor Code breaches and for dealing with companies that are cooperative and based in Australia. The enforcement regime relies on civil penalty sanctions to penalise behaviour and provide commercial incentives to comply. It is possible that C/CSPs would be willing to bear a civil penalty if the money they would save by proceeding with a low cost procurement covered the cost of the civil penalty. A direction may not have the effect of directing mitigation action.

A further potential risk to the effectiveness of the compliance regime is that it relies on the ACMA to take enforcement action at the request of security agencies. The ACMA does not have expertise in national security matters or capabilities to detect and monitor security risks. Consequently, ACMA would need to develop a new capability on national security.

A significant risk is that a Code will be drafted by industry that does not meet government objectives. Government can assist industry to draft the Code and is best placed to articulate its expectations about security threats and risks. However, as it is developed by industry it is likely to reflect commercial interests foremost. In the event that a Code presented to the ACMA was deficient or could not be registered or enforced, the ACMA could develop a Standard. However, this would further delay addressing risks associated with the status quo and would face the same challenges as a Code with respect to being focussed on technical rules rather than broad national security outcomes.

A further significant risk is that the process for developing a Code would significantly delay implementation of this option. Codes require industry cooperation and engagement and significant lead in times. The Code development process is a lengthy process consisting of several phases of public comment, content approval and process approval, to enable registration with ACMA. It also requires stakeholder representatives to reach a consensus on the matters that will be included which can take considerable time and resources. Consensus might be reached on a high level principles-based Code, however is likely to be more challenging in relation to a detailed rules-based Code concerning national security.

Finally, Codes are usually more effectively used as an industry driven mechanism to protect consumers and industry when appropriate sanctions can be imposed and where Code objectives are consistent with commercial interests. Public awareness of Code provisions and requirements are also usually an important mechanism for ensuring Code compliance and critical to achieving the objectives relating to matters of public interest. These factors are not likely to be present in the context of addressing national security concerns so it is questionable whether a Code is an appropriate fit.

5.2.4 Summary of Net Benefit of Option 2

Option two could go some way to meeting reform objectives and would be an improvement to the status quo. It would achieve the following policy objectives:

- Increased industry awareness about national security risks and implications and timely information sharing.
- Formalise and clarify the relationship between government and industry and government's expectations about industry's responsibilities in respect of managing national security risks.
- Provide greater certainty for industry in business decision making reducing costs.

However, Option 2 does not meet the overall objective of providing effective and efficient model to achieve security outcomes. There are a number of significant risks with this option that must be weighed against the benefits, these are:

- A Code is likely to take at least two years to develop, requiring investment of resources, time and money from government and industry and may not satisfy registration requirements and remain unenforceable.
- A Code may not be able to provide enforceable rules to achieve national security outcomes, (assuming the existing restrictions in section 115 were engaged).
- The enforcement mechanisms do not provide for a quick and targeted resolution of non-compliance. In particular the direction power is linked to compliance with particular Code provisions which may not adequately target action to address the particular security risk.
- Codes are usually appropriate for the protection of community safeguards where these can be appropriately balanced against C/CSPs business objectives and autonomy. National security objectives may require C/CSPs to put security interests above commercial interests – this would not meet the stated intention of the industry Code framework under Part 6.

The significant upfront costs for industry in developing the Code mean that this is not a low cost option for industry. However, the increased costs are still relatively low when compared with the size and value of the industry to the economy**.**

On balance, while the Code would achieve some reform objectives it does not provide sufficient assurance that a Code will be able to impose clear obligations on industry to implement security agencies advice and proactively protect networks and facilities. In particular the more arms-length nature of the relationship between industry and security agencies under this mechanism does not provide the certainty that security outcomes will be achieved.

5.3 Option 3 – Security Framework: Amending Legislation

5.3.1 Costs of Option 3

As with Option 2, there are additional costs associated with the compliance regime that would affect all C/CSPs. The limited data provided by industry means these costs are estimates only and based on a break-down of possible administrative and compliance related activity.

The obligation to ensure effective control will require C/CSPs to put in place a mechanism to ensure they can monitor security obligations. AGD's assessment of the additional costs suggests a modest increase to costs reflecting the fact that there is already national security regulation in place, although recognising that only a minority of C/CSPs with dominant market share are currently engaged.

Many larger C/CSPs already have staff designated to engage with government on matters of lawful interception and privacy obligations and these staff tend to also work on broader national security matters. These existing resources would manage their engagement with security agencies over potential national security risks, together with business-as-usual security assurance functions. While high priority C/CSPs are likely to have such mechanisms already in place, lower risk C/CSPs may have to develop this capability and maintain it, however, it would be proportionate to risk.

Industry impact

Of the costs associated with compliance, there will be costs associated with providing information or documents for government to assess the risks to national security. As with Option 2, a security framework would facilitate consistency in the government's approach, encouraging early engagement which could ultimately save C/CSPs time and money in terms of procurements. There is likely to be a small net increase in costs across the telecommunications sector, which are set out in the Table 5.3 below.

Table 5.3 – Security Framework

Activity	Number of C/CSPs affected	Number of staff	Hours	Frequency	Cost
Implementation of the security framework	1560	1	3	[start-up]	$357 926
Intensive engagement and information sharing	20	2	3	Yearly	$110 131

C/CSP notification and engagement on material changes to core systems / networks	20	1	35	1	$53 536
C/CSP escalated engagement over a Direction with AGD (as regulator)	3	2	35	1	$16 061
Low priority C/CSP compliance with government's request for information	20	1	3	1	$4 589

Costs associated with implementation and compliance

Administrative costs are particularly relevant under Option 3 in terms of regulatory impact.

The cost would represent a modest additional cost to the sector which has revenue in excess of $43b a year. An estimate from Australia's large carriers was that the intensive engagement over threat information, network design and significant procurements could amount to one additional member of staff to its existing regulatory engagement team. The impact would be the diversion of some staff. This arguably occurs under the status quo, particularly where late engagement over a potentially high risk proposition is involved. For other smaller carriers, staff are likely to be reallocated causing project pressures elsewhere, although this is unlikely to be too significant.

The estimated cost under the Regulatory Burden Measurement approach, following analysis through the business cost calculator, is estimated to be $220 109 of which $184 317 is ongoing.

A start-up cost of $357 926 for 3 hours for 1560 C/CSPs is based on guidelines that set out what government's expectations are under a security framework. A high priority multi-mode carrier *[redacted text]* would have different expectations relating to the level of national security risk, when compared alongside a backhaul provider, or alternatively a small regional (low risk) Internet Service Provider.

Costs of Engagement

There will be costs to industry in complying with provisions (likely to be contained in guidelines), that detail requirements for industry/government engagement. For example, this may require major high priority carriers to engage in monthly meetings with security agencies and more intensive discussions for significant procurement projects with potential security concerns. Some low risk C/CSPs would be required to complete desk top audits to allow security agencies to assess their compliance.

Security advice would add a small overhead to costs associated with C/CSPs' existing regulatory obligations and informal engagement with government.[13] The table above also factors in regulatory oversight of security obligations through compliance assessment questionnaires. The assumption is that a questionnaire would be issued to *[redacted text]* C/CSPs based on risk prioritisation, including customer numbers, type and criticality. Three hours for one member of staff from the C/CSPs has been allocated.

Compliance costs arising from implementing security agencies advice (albeit on a cooperative basis) could include high priority/risk C/CSPs having independent security auditing and monitoring of their planned procurement activities. The cost of auditing would vary based on the size of the system. For example, a substantial program of auditing undertaken by the Australian Government for security vulnerability can range between $40 000 and $550 000 – an average of approximately $225 000 per audit. The larger carriers have teams to manage compliance and regulation including with privacy obligations and telecommunications interception.

Costs to Government

There are costs to government in developing and consulting on the proposed legislation and guidelines. However, these costs would be absorbed by the relevant government departments and agencies and would not be recovered from industry through cost recovery mechanisms.

The total estimated cost to government in administering and enforcing the scheme would be $1.6m which would include:

- Security agencies costs – security agencies would need additional resources for engaging and monitoring compliance with the Framework including intensive engagement with high risk C/CSPs, developing security threat assessments and advice to C/CSPs on risk and risk mitigation, and collaborating with the regulator on enforcement action and compliance with enforcement action.

  This is likely to involve *[redacted text]* additional officers to meet demand from C/CSPs for national security assessments and advice ($1.1m).

- Cost to the Attorney-General's Department in establishing and maintaining regulatory functions, including implementing processes to engage and obtain information from lower risk C/CSPs, supporting security agency engagement processes, advising C/CSPs of obligations and requirements, supporting the regulator in the exercise of enforcement powers. These functions will require four additional staff with AGD ($0.5m)**.**

[13] AGD and the PJCIS sought, with limited success, to explore with the industry the potential compliance costs and impacts of the security framework on broader competition impacts. Industry has been reluctant to share commercial-in-confidence material or pricing structures to enable estimation of potential costs. The cost information included in the RIS is based on discussions with key telecommunications staff and in one case, the provision of confidential information on procurement scenarios. This, combined with the cyclical nature of technology procurement cycle (3-5 years) and the changing nature of the telecommunications market, also makes it difficult to predict the nature of significant infrastructure investment decisions that could occur in the future.

There will also be costs associated with any enforcement action through the Federal Court to seek civil penalties in the event of non-compliance, however these will be met within existing resources.

Regulatory Burden and Cost Offset Estimate – Option 3: Security Framework

Average Annual Regulatory Costs (from Business as usual)				
Change in costs ($M)	**Business**	**Community Organisations**	**Individuals**	**Total change in cost**
Total by Sector	$0.220	$0	$0	$0.220
Cost offset ($M)	**Business**	**Community Organisations**	**Individuals**	**Total by Source**
Agency	$0	$0	$0	$0
Within portfolio	$0	$0	$0	$0
Outside portfolio	$0.578	$0	$0	$0.578
Total by Sector	$0.578	$0	$0	$0.578
Are all new costs offset? **☒ yes, costs are offset**				
Total (Change in costs - Cost offset) ($M) -$0.358				

The regulatory cost of offsets noted in the above table have been identified within the Communications portfolio. The cost offsets are taken from the cost savings arising from the removal of retail price controls in telecommunications (costs have been agreed with OBPR and reported in Q1 2015).

5.3.2 Benefits of Option 3

A security framework would codify and support a more intensive and tailored two-way channel for the timely sharing of sensitive threat and risk information, improving both government and industry's capability to respond to threats in a strategic manner. The regime would effectively be self-governing with industry only being required to engage with

government where there are material changes that affect more sensitive parts of their systems or equipment or where non-compliance resulted in enforcement.

Compliance with the core principles of the security framework (i.e. competent supervision and effective control) could be further used as a marketing opportunity by C/CSPs. For example, if a C/CSP's wholesale product or service is already compliant under the security framework, a re-seller no longer needs to demonstrate competent supervision and effective control over the same product or service. Although the re-seller would have to protect its own individual network including the details of its customers, the wholesale C/CSP's compliant product or service could be used as security assurance thereby significantly lowering the re-seller's compliance costs**.**

Clarity in expectations would enable C/CSPs to make informed business decisions which are appropriate to the level of security risks. A benefit may arise from frequent engagement and the provision of tailored national security threat information to high risk C/CSPs, which could reduce potential delays to future procurements. This is based on an assumption that high priority C/CSPs will have greater national security risk awareness and clarity about government's expectations than under the status quo where material changes to networks or facilities present national security risks. A consistent approach by government to national security risks may help preserve diversity of supply, by placing a greater value on trusted, higher security suppliers lifting overall security standards (through continued competition) in the longer term.

A transparent security framework would more clearly set out government's expectations over industry's management of national security risks and provision of mitigation plans at an early stage rather than late in the process, before contracts are signed, which often currently occurs. Clear authoritative signals through a direction about national security risks and means to mitigate them may make it easier for a C/CSP to persuade its Board to release funding for a secure supply option or to address potential security risks. *[redacted text]* This minimises complications where procurement decisions are made by boards outside Australia. Clear expectations and processes provide greater certainty for decision making. Grounds for directing mitigation or alternative actions would ultimately be determined by security agencies, based on an assessment of risk following their engagement with a C/CSP. The powers of direction would serve as a means to support the existing powers in the Telecommunications Act relating to national interest matters.

The advantages of a security framework are that it could:

- focus on security outcomes rather than absolute technical requirements, making it adaptable to changes in technology and the telecommunications market;
- provide greater clarity, control and certainty for industry by focusing on self-governance and demonstration of compliance;
- be applied equitably across the telecommunications sector; and
- provide a more effective incentive for industry to place greater emphasis on national security considerations in its business decisions.

This Option achieves security outcomes yet still provides flexibility regarding how risks are managed and networks protected. For example, subject to a direction being issued, the framework is based on broad legislative obligations rather than specifying technical requirements for networks and facilities. The administrative guidelines are intended to provide a flexible and easily revisable form to provide more detail about how these obligations should be achieved. There would however, be clear enforcement mechanisms to manage non-compliance so the security risk can be effectively managed.

The level of national security risk will determine the level of engagement required between a C/CSP and government agencies, with costs of compliance based on the level of national security risks that may be presented through any material changes to a C/CSP's networks. Security agencies would establish close relationships with a number of *[redacted text]* high priority carriers and meet on a monthly basis to understand the business model of the C/CSP, its network operations, and provide targeted threat information based on the characteristics of each C/CSP. The ability to require information early in a decision making process will be significant in determining the national security risk and reducing costs on industry.

Past significant procurement examples among larger carriers in recent years indicate that existing national security regulatory compliance costs are being incurred by C/CSPs that are compliant with the existing regulation. A C/CSP with advanced in-house expertise and management would benefit from a lower risk profile than a C/CSP seeking to outsource or off-shore the supply of its equipment and managed services.

Administrative guidelines would put in place clear requirements for engagement. Information flow for C/CSPs would have regard to their risk profile and will assist security agencies to properly assess the risk level and keep this up-to-date. It might be possible to achieve something similar under the Code although it is likely to be less targeted and less flexible.

There is certainty in provisions that enable enforcement. Industry may avoid having to mitigate or replace high risk systems and achieve longer term savings in infrastructure being supported by more lower risk suppliers. C/CSPs would have the flexibility to meet government's security obligations yet still be adaptable to changes in technology and the broader telecommunications market.

The framework is intended to maximise cooperative engagement between C/CSPs and government on matters of national security. Where such a relationship works effectively there may be no need to invoke more formal directive powers. Administrative penalties or directions to C/CSPs would only be imposed where a risk has been assessed as significant and prior engagement has proved ineffective.

5.3.3 Risks of Option 3

The most significant risk is that, although the framework is designed to build upon cooperative relationships and collaboration, the introduction of formal information gathering and direction powers may reduce the likelihood that national security risks will continue to be managed

cooperatively. In other words, the existence of powers compelling action, and associated protections, may mean that C/CSPs would prefer to have the security of a formal notice or direction when providing information of making a decision which prioritises national security interest over commercial interests.

Risks for option 3 include pressure on market and competition costs caused by potential restrictions on significant procurements, particularly those in more sensitive parts of telecommunications infrastructure. *[redacted text]* Some suppliers *[redacted text]* may be restricted from competing for small parts of this more *[redacted text]* sensitive market *[redacted text]*. However it should be noted that this can already be achieved under the status quo.

Option 3 also potentially imposes new costs on lower risk C/CSPs that to date have avoided needing to engage with security agencies. Under this option all C/CSPs would need to engage, however the level of engagement would be proportional to the risk posed by the C/CSP. As such, any new costs are likely to be minimal or capable of being mitigated through clear communications and relying on the notification requirement under the obligation to protect networks.

[redacted text] There is a risk of possible delays to procurement or business decisions pending an assessment of risk. This is less likely to occur where a C/CSP engages early and intensively with security agencies. Just as under the status quo and Code option, C/CSPs would be required to bear the costs of considering alternative suppliers, or the cost of specific mitigations where the supply of equipment or services presents a national security risk.

Greater intervention in the planning of network design and procurement decisions may reduce business autonomy of C/CSPs. Enforceable obligations to share information and protect networks will mean that security agencies will be more influential in significant procurements that present potential risks. *[redacted text]* While these risks are present in all of the proposed reform options – *[redacted text]* the threat of applying section 581(3) can already impose such restrictions – it is more likely to have a broader effect under Option 3.

Where government seeks to reduce the risk posed by specific design features present in a system provided by a supplier, its intervention with a C/CSP may result in suppliers needing to undertake potentially costly modifications. However, early engagement with government would minimise the risk of C/CSPs entering into contractual arrangements with suppliers and/or managed services that subsequently required costly modifications to be undertaken.[14]

[14]By way of example, a recent procurement of a terrestrial telecommunications project for Defence (JP2047) suggests that considerable price tension exists in the market; despite one of the carriers undertaking significant additional redundancy their final cost fell to be competitive with the final successful provider. This is consistent with recent procurements of 4G LTE technology across mobile telephone networks, despite there being considerable differences in tender responses based on the nature of the project.

5.3.4 Summary of Net Benefits for Option 3

Option 3 is an improvement to maintaining the status quo and developing an industry Code. It most effectively addresses the primary policy objective of providing an effective and efficient mechanism for managing national security risks by providing:

- a clear statement of government's expectations with respect to the management of national security obligations – including clarifying that responsibility for managing risks rests with C/CSPS;
- enforceable obligations on C/CSPs to protect their networks – this will facilitate and incentivise proactive management of risks and early engagement with security agencies;
- information gathering powers to facilitate the timely provision of information from industry to government to enable the assessment of national security risks;
- broad and flexible direction powers to facilitate speedy resolution of non-compliance and national security risks and avoid protracted negotiations – for example, the regulator can specifically direct action to address a national security risk on a case-by case basis; and
- a civil penalty regime to enforce directions and notices to produce information issued by the regulator.

Key risks of Option 3 include:

- reduced business autonomy of C/CSPs – the requirement to protect networks and facilities may restrict business decisions on procurements and network design. While these risks are present in all of the proposed reform options – *[redacted text]* the threat of applying section 581(3) can already impose such restrictions – they are likely to have a broader effect under Option 3; and
- reduced cooperation and increased enforcement action – the existence of formal powers may mean some C/CSPs will insist on formal notifications before releasing information and directions before implementing risk mitigation measures.

There will be a small increase in the regulatory burden to industry under this option, however this is estimated to be lower than the total regulatory burden costs associated with an industry Code. These costs will reflect the resources required to ensure networks are protected from interference, engaging with security agencies including providing information, and responding to enforcement action and will be applied equitably to the entire sector.

Greater clarity of government national security expectations will facilitate early engagement and timely provision of information which will enable security agencies to provide threat assessments more quickly. Direction powers will provide greater certainty for business planning and decision making resulting in a security management process that is more efficient and less costly. The social, community and economic benefits of a security framework for the ongoing protection of data are anticipated to outweigh the modest additional administrative and compliance costs to industry and risks.

5.4 Option 4 Investment Plans – Amending Legislation

5.4.1 Costs of Option 4

Annual administrative and compliance costs for this option would be the same as for Option three ($184 317 over 10 years) plus an additional $357 926 for the management of investment plans by approximately 1560 C/CSPs which equates to a total of: $542 243. This is using an assumption of an average three hours for each C/CSP for a professional level member of staff to complete an investment plan. This calculation is based on an assumption that carriers will be able to get some leverage from their existing compliance activities relating to an ICP in the production of an investment plan. Most CSPs will generally be using a carrier's infrastructure or re-selling services so the investment plan should be less onerous and take around three hours. The limited data provided by industry means these costs are estimates only and based on a break-down of possible administrative and compliance related activity.

Costs to Government

The estimated resources required in ASIO and AGD to implement the security framework in Option 3 totalling approximately $1.6m would also be captured under Option 4. In addition to these costs, there would be an additional resource cost for AGD to administer and assess the receipt of an annual investment plans. This is estimated to cost a further $130 000.

Regulatory Burden and Cost Offset Estimate – Option 4: Investment Plans[15]

Average Annual Regulatory Costs (from Business as usual)				
Change in costs ($M)	**Business**	**Community Organisations**	**Individuals**	**Total change in cost**
Total by Sector	$0.578	$0	$0	$0.578
Cost offset ($M)	**Business**	**Community Organisations**	**Individuals**	**Total by Source**
Agency	$0	$0	$0	$0
Within portfolio	$0	$0	$0	$0
Outside portfolio	$0.578	$0	$0	$0.578

[15]The figure used is an annual average over ten years to factor in the start-up costs.

Average Annual Regulatory Costs (from Business as usual)				
Total by Sector	$0.578	$0	$0	$0.578
Are all new costs offset? **☐ yes, costs are offset**				
Total (Change in costs - Cost offset) ($M) $0				

The regulatory cost of offsets noted in the above table have been identified within the Communications portfolio. The cost offsets are taken from the cost savings arising from the removal of retail price controls in telecommunications (costs have been agreed with OBPR and reported in Q1 2015).

5.4.2 Benefits of Option 4

In addition to the benefits outlined under Option 3, investment plans would require industry to focus on all procurements in the forthcoming year and systematically consider potential national security threats, drawing on government advice. Industry would benefit by transferring the management of risk to government, once a plan is submitted. The benefit to government would be access to information providing visibility of potential risks.

Similar to Option 3, this option meets the proposed reforms' outcomes of: timely information from industry on material changes to networks or facilities to enable the assessment of national security risks; timely provision of threat information to industry by security agencies; and efficient and effective mitigation of national security risks.

5.4.3 Risks of Option 4

While Option 4 would appear to be the most complete 'compliance approach', it would not focus in efficiency terms on where the highest risks lie, as it would require all C/CSPs to provide data, despite there being a very low risk of national security threats in the vast majority of the 1560 C/CSPs. It would also encourage a transfer of the management of risk from a C/CSP to government, once an investment plan is submitted. A C/CSP may consider it had discharged its obligation and responsibility for assessment and treatment of risk by submission of such a proposal.

The length and complexity of ICPs under the TIA Act are commeasurable to the size of the industry participant's infrastructure, services and customer base. They generally range from five pages (simple template response) to 100 pages, for larger C/CSPs providing multiple telecommunications services. It is assumed that investment plans would range in a similar way. *[redacted text]*

5.4.4 Summary of Net Benefits under Option Four

While it would achieve closer engagement with industry, the administrative costs would be significant (which may be passed on to consumers). The preparation of investment plans involves collating information across the business, preparing a detailed response and seeking clearance through legal and management. It would require the compilation of data from procurement documents and submitting it in an approved format to government. A C/CSP would be required to make an assessment of what and how much to notify and if their risk threshold is low or undetermined, could potentially result in a C/CSP providing too much detail on business planning.

Option four provides a medium – high degree of effectiveness meeting the objective, which is to establish an efficient mechanism for the management of national security risks through government and industry engagement. While national security outcomes would be able to be managed, there would be a significant compliance burden on industry and government would need to place significant resources to ensure it is able to manage the transfer of risks by way of its receipt of investment plans.

The investment plan approach considered under Option 4 is not considered to drive a net benefit, largely as the risk to government increases through the transmission of business plans from industry for assessment. This results in a larger cost to business of $578 000 and government of $1.6m a year in order to monitor these risks.

6 Who will you consult and how will you consult them?

In progressing the TSSR proposal for the government's consideration, AGD undertook extensive consultations with industry (in addition to ongoing consultations with relevant government agencies). There has also been a broader public consultation process undertaken by the PJCIS in 2012-13. Government agencies continue to support the proposed security framework and its regulation by AGD. Outcomes of industry consultations and our response are summarised below.

Initial targeted consultation with industry (*[redacted text]* the largest C/CSPs and the Communications Alliance) was undertaken in early 2012 to explore views on a telecommunications security framework, including its feasibility, impact on business and cost. The feedback from industry included reservations on potential reporting/notification requirements, and potential for regulatory overlap. Other issues concerned a desire for a level playing field and clarity about government's expectations under a framework.

To address industry's key concern on new reporting/notification requirements, the proposed framework was refined to leverage the existing notification mechanism through section 202B of the TIA Act, rather than establishing another 'notification framework' for all C/CSPs. AGD also undertook further work on the presentation of the proposal to illustrate how the risk management concepts of competent supervision and effective control would apply equitably to

all C/CSPs, providing assurance over national security risks presented through the supply of equipment and services.

During 2012-13 consultations, industry also sought greater clarity about government's expectations, advocating the development of guidelines to provide further details. In consultation with industry, AGD subsequently produced draft guidelines to provide industry with a better understanding of its obligations under the framework. AGD circulated the draft guidelines for comment setting out how national security threats may be minimised using the concepts of competent supervision and effective control over the network and the information held and passing across it. Industry has shown interest in working with government to develop the guidelines further and supports principles that enable choice of the most appropriate means to manage security risks. The guidelines would be a living document, and government and industry would have the opportunity to update the guidelines as needed.

The focus of the proposal presented for the PJCIS inquiry in mid-2012 was to ensure an even-handed and suitably light-touch approach – this was articulated in a discussion paper that was released publicly. In its June 2013 Report, the PJCIS noted 'warm, if cautious support' of most industry submitters for the proposed reforms and recommended the government proceed with developing a security framework. It should be noted that during the PJCIS inquiry Macquarie Telecom disagreed that there is a need for government intervention on the issue of security, submitting that providing security was already in the interest of service providers.

The PJCIS recommended (at recommendation 19) the government amend legislation to create a telecommunications security framework, including a RIS to cover aspects such as competition impact and regulatory overlap. The PJCIS also recommended government consider any existing obligations, including compatibility with existing corporate governance frameworks, and to look at any good faith provisions.

The current proposal is intended to work with existing national security regulation, particularly the good faith provisions under section 313 of the Telecommunications Act. It also supplements the existing extreme section 581(3) power of the Telecommunications Act, which allows for cessation of a service, and leverages the notification obligation under section 202B of the TIA Act rather than creating a new notification requirement. There are no direct responsibilities under corporations law relating to obligations to manage national security risks, nor are there any incompatibilities.

6.1 Early 2014 consultations

As part of the targeted engagement, AGD consulted *[redacted text]* carriers considered to be of the most interest from a national security perspective to provide guidance about government's expectations of the management of national security risks. Those consulted are broadly accepting of the need for a security framework.

Further consultation with industry was undertaken by AGD and Department of Communications in April-June 2014; those consultations focused on the proposed security framework and cost recovery for the regulation of the framework through the Annual Carrier Licence Charge. The consultations entailed targeted roundtable meetings in Sydney and Melbourne (April 2014 – details at **Attachment B**), written submissions by key C/CSPs and industry bodies (May 2014), and individual meetings between AGD senior officials and C/CSP senior executives.

The outcome of the recent consultations highlighted that industry is reasonably comfortable with the security framework provided it is clearly communicated where national security threats apply to C/CSPs and is administered in a way that seeks to create a level playing field for C/CSPs. Issues raised by industry at the meetings and written submissions included:

- clarity from government about the actual threat, where the problem lies and what will change under the security framework;
- how TSSR is compatible with the government's deregulation agenda;
- where responsibility for security assurance would lie in a wholesale vs retail / resale scenario;
- likely compliance costs for industry;
- why AGD is seeking to recover costs of up to $2m from industry for its regulatory function; and
- whether the proposed transition period may be extended from 6 to 12 months.

AGD has responded to industry's key concern on the threat and the changes required under the framework by clarifying that the framework would not apply to all aspects of a C/CSP's business but to more sensitive areas of networks and facilities – this has lessened industry concerns. AGD has also undertaken to develop an administrative explanatory note (guidance document) for industry to provide greater clarity around the purpose and scope of the security framework. This would provide a communications tool (in addition to the existing industry guidelines) that would articulate the national security threat and the anticipated changes under the framework.

The guidance document would further explain that the framework would supplement existing obligations under section 581(3) of the Telecommunications Act, establishing a formal two-way information sharing process, and proportionate and graduated intervention measures for government. AGD has also agreed to work closely with Communications Alliance (as the peak industry body) to refine industry guidelines, and jointly explore options to develop an efficient and cost-effective security assurance process, which would result in the least compliance impost on industry. In addition, to address industry's concerns around the cost recovery of $2m per annum, the government has decided to not cost recover for its regulatory and administrative functions.

Regarding the transition period, AGD has suggested that C/CSPs will have sufficient time to familiarise themselves with the TSSR, so a 12 month transition period should not be necessary. If a C/CSP is not compliant when the scheme commences – security agencies will continue their engagement to resolve existing issues by developing appropriate mitigation measures. As

in all cases, formal compliance measures (including directions) would only be engaged if agreement could not be reached between security agencies and C/CSPs or there was wilful non-compliance.

On 21 May 2014, to elicit greater engagement over administrative and compliance costs, AGD provided selected industry members and the Communications Alliance with a redacted version of the draft RIS (with more detailed analysis of the additional effort associated under a security framework) seeking feedback on estimates of industry compliance costs. To date, industry has been unable to provide quantitative cost estimates. However, their feedback resulted in a significant decrease in the notional number of 7 FTE that AGD had allocated across the sector, as most compliance costs are already part of existing regulation. Initially, AGD had suggested that approximately 7 FTE staff maybe required to administer changes under a security framework which was estimated at $680 000 – using the professional wage category from OBPR guidance ($43.70 an hour including on-costs).

During further consultation with industry over draft guidelines and the impact analysis from the draft RIS, industry sought greater granularity about the estimated monitoring and compliance activities that a C/CSP would need to undertake to ensure compliance with the framework. Based on feedback, ongoing regulatory burden costs for C/CSPs was revised down to $220 000.

Other key feedback received from industry has been taken into account in this RIS, particularly industry's general preference for a self-regulatory model and its costing experience developing a Code. It should be noted that the Communications Alliance and Telstra's (Telstra requested to keep its input confidential) feedback on the draft RIS expressed a preference for self-regulatory (Code) model. Optus (the second largest C/CSP) acknowledged that "…an industry Code, in itself, may not be capable of achieving a comprehensive regulatory solution as it cannot directly address the components of government involvement".

6.2 February-March 2015 Targeted Consultation

A further round of targeted industry consultation was undertaken in February-March 2015 with a small number of C/CSPs and the two peak bodies (details at Attachment B) and provided more detail about the proposed legislative provisions and how they would operate in conjunction with the draft Guidelines. The purpose of the consultation was to clarify industry's understanding of the proposed framework. The consultation took the form of a roundtable meeting and one-on-one meetings with Vodafone Hutchison Alliance, Telstra, Optus and NBN Co. While views expressed at the roundtable and one-on-one meetings were fairly consistent with feedback provided in previous consultations and there appeared to be general support for an outcomes based regulatory approach, a couple of written submissions were found to be critical of the framework.

While more detail about the proposed legislative provided some degree of certainty and comfort about the intended operation of the legislation, there was concern expressed that it was still not clear what parts of networks would need to be protected and how. Further information was provided to Telstra and the Communications Alliance in the form of a factsheet

highlighting sensitive parts of networks and what changes to networks might trigger the notification requirement. More detail will be provided in the Explanatory Memorandum and revised Guidelines.

C/CSPs indicated they still do not support the cost recovery model and consider that the cost should be borne by government. Recognising the sensitivities associated with imposing further costs on the telecommunications industry on the back of data retention and copyright reforms a decision was made to drop the cost recovery proposal and fund the activity from within government.

A key area of concern was the operation of the draft industry guidelines. There was still some confusion about whether the draft guidelines were enforceable and prescribed rules. Also there was some concern that the Guidelines relied heavily on an ITU standard which some carriers (particularly Telstra) said needed addressing. It was clarified that the Guidelines are a work in progress and would be further developed with industry as they are intended to be meaningful for industry.

7 What is the best option from those you have considered?

Of the four options considered, Option 3 is considered to meet the government's policy objective of a more efficient and effective mechanism for the management of national security risks to the telecommunications sector through collaboration between government and industry.

Option 1, maintain the status quo, would not increase any regulatory burden on industry and would continue to rely on building and maintaining cooperative relationships with industry. However, costs to C/CSPs of managing national security risks on an ad hoc and cooperative basis are likely to present an overall larger cost where a national security risk necessitates extensive engagement to achieve security outcomes, including costs associated with any remedial or mitigation action. Such costs are likely to continue to be borne by the top tier carriers, potentially placing them at a commercial disadvantage to their competitors who attract less national security scrutiny. The absence of a requirement on C/CSPs to provide information to security agencies means security agencies would continue to have a low degree of visibility of risks across the telecommunications sector, and their ability to develop threat assessments is compromised. Reliance on cooperation and goodwill to achieve national security outcomes is inherently risky – it may be insufficient to counter market processes and/or cooperation may not always be achievable. Continued lack of certainty about government's national security expectations and when section 581(3) might be appropriately used means that negotiation to achieve national security outcomes will continue to be protracted, costly and time consuming for industry and government. C/CSPs will not have a clear mandate to assist their Boards balance national security risks against competitive and commercial interests. Continuing the existing regulation under Option 1 would not result in additional administrative or compliance costs for industry or government, noting that come C/CSPs already incur engagement and voluntary compliance costs.

Option 2, develop an Industry Code, would improve the status quo. It would provide a mechanism for greater clarity around government's national security management expectations, including expectations about information sharing and early engagement with government on procurement planning. The benefits of facilitating greater awareness of national security risks, greater clarity around security management expectations and codifying engagement are not sufficient when balanced with the effort required by industry to develop and register the Code, and the risks that enforcement mechanisms will be effective.

The current restrictions on the scope and operation of Industry Code rules under Part 6 of the Telecommunications Act could limit the effectiveness of the Code to impose clear and broad obligations on C/CSPs to protect networks and cooperate with security agencies on the design and planning of networks and facilities (an amendment to existing provisions could address these restrictions). It is likely that a Code would be technically, rather than national security outcomes, focussed and not provide flexibility to address national security risks on a case-by-case basis as required. The long timeframes associated with developing and enforcing non-compliance under the Code also present significant risks. If the Code fails to provide clear enforceable requirements that C/CSPs must cooperate with national security advice, associated enforcement mechanisms will be inadequate. The directions power is restricted to enforcing compliance with Code provisions. In the absence of a direction to comply, compliance with a Code provision may be treated as optional by some company boards and an insufficient mandate when considering national security risks over commercial interests. The additional regulatory burden to industry under Option 2 is approximately $360 000. Government administration costs are estimated to total $2.1m.

The legislative security framework under Option 3 is the best option for achieving an effective and efficient framework for managing national security risks to the Telecommunications sector. It provides a mechanism for imposing clear obligations on industry for the management of security risks, including an expectation that C/CSPs will proactively engage with government to manage those risks. It promotes close engagement between industry and government, while providing effective and efficient mechanisms for addressing security concerns where they cannot be achieved on a cooperative basis. It provides the most effective mechanism for ensuring that government can obtain the information it needs from the telecommunications sector to develop comprehensive and targeted threat assessments. Provided that option three is implemented in a risk-based way, focussed on achieving national security outcomes rather than technical requirements, it will substantially address industry's concerns about a direct regulatory model as confirmed through the early 2012 consultation and 2012-13 PJCIS inquiry.

Option 3 strikes a balance between a regulatory approach and allowing business to make decisions in their own interests. C/CSPs would have an overriding obligation to protect their networks and the data stored and transmitted across them, while retaining flexibility in the majority of their business and investment decisions. Implementation will need to be managed carefully to ensure the requirement to protect networks and facilities does not unnecessarily restrict innovation and network design autonomy, government is best placed to identify and

assess emerging national security risks and provide clear guidance to industry on effective protections and controls to mitigate such risks, while the telecommunications industry is best placed to determine the most appropriate operational and technical controls for their respective businesses. The framework under Option 3 aims to build in flexibility by avoiding overly prescriptive regulatory requirements on industry, with Government responsible for providing a clear set of security guidelines to articulate the risks that must be managed by C/CSPs. As such, government would continue to remain sensitive to the commercial interests of industry by communicating well in advance its expectations to help industry meet their broader operational and commercial requirements.

A key risk is that the existence of formal powers may mean some C/CSPs will insist on formal notifications before releasing information and directions before implementing risk mitigation measures, reducing cooperation and inadvertently driving a compliance based approach. Early engagement and consultation with industry will seek to mitigate this risk.

There will be an increase in the regulatory burden to industry under this option in addition to existing administrative and compliance costs, and could mean that some lower risk C/CSPs would have to enhance security and engagement with government capabilities. These costs will be small given the lower level of engagement with low priority C/CSPs and will ensure administrative and compliance costs are applied more equitably across the entire sector then occurs under the status quo. The regulatory burden to industry under Option 3 is $220 000.Government administration costs are estimated to be $1.4m.

Australia's approach would also be consistent with the direction of recent international developments in managing national security risks to telecommunications infrastructure noting that likeminded countries are pursuing stronger regulatory measures (see **Attachment C**).

Option 4 provides the overall net benefits of Option 3 with an added layer of regulation and cost. It potentially duplicates existing legislative obligations under the TIA Act, to produce annual Investment Plans. There are little additional benefits gained from a national security management perspective when balanced with the regulatory burden placed on industry to produce these plans. The regulatory burden to industry under Option 4 is $578 000. Government administration costs are estimated to be $1.53m.

8 How will you implement and evaluate your chosen option?

Subject to the government's agreement, Option three would be implemented through the introduction of an amendment Bill as soon as practicable through Parliament with a six month transition period to enable C/CSPs to prepare for implementation. Regulation would be supported by administrative guidelines and where relevant, timely and specific advice from security agencies on identified areas of risk to networks (including those presented through access by suppliers of concern), and steps required to protect those networks. The guidelines would be a living document. Administrative arrangements would outline the roles and responsibilities of government and industry and would help define and oversee industry's protection of its networks and facilities from a national security perspective. This would

contribute to risk prioritisation, establishing engagement and information sharing processes, clarifying audit and enforcement procedures.

Should the Parliament pass amendments to the Telecommunications Act, government would work closely with industry to ensure that it is made aware of its obligations and implement risk mitigation measures to address security concerns during the transition period. An evaluation of the security framework would be undertaken after three years (or earlier if required) to ensure government's policy objectives and outcomes are being met. This evaluation would be supported by data on the number of identified instances of unauthorised access to telecommunications networks and the level of government intervention to mitigate risks.

8.1 Agency Responsible for Regulatory Functions under a security framework

[redacted text] While a security framework enabled through changes to the Telecommunications Act would appear to fall within the remit of the telecommunications regulator – the ACMA – as these reforms are focussed on achieving national security outcomes it is proposed that the appropriate regulator would be AGD. The ACMA does not currently possess national security expertise to effectively develop and implement the reforms and implement them. Furthermore, if it were to develop this capability it is likely to duplicate some of the existing functions of security agencies.

The Secretary of AGD could undertake end-to-end regulation of a security framework in terms of administration and enforcement because:

- the Attorney-General has Ministerial responsibility for national security of critical infrastructure, including telecommunications networks and facilities and telecommunications interception powers and powers under the ASIO Act;
- AGD has an established and close relationship with intelligence agencies which makes it, and not ACMA, well placed to provide industry with heightened and tailored threat information on Australian telecommunications traffic; and
- the existing regulatory powers are managed by the Attorney-General, AGD and ASIO officers.

AGD would also be responsible for escalated statutory intervention through directions and regulatory enforcement of non-compliance as-and-when required. Government would seek to use advice and guidance to encourage risk-informed management of security concerns in the first instance. In cases where engagement with C/CSPs was unsuccessful, or a blatant disregard of security information jeopardises the government's confidence in the security and integrity of Australia's telecommunications infrastructure, powers of direction would facilitate greater compliance.

AGD would regulate the security framework including developing and disseminating guidelines (in consultation with agencies and industry), establishing and maintaining a risk framework with input from security agencies. AGD would be responsible for risk profiling, managing and auditing compliance of 'lower risk' C/CSPs *[redacted text]* to monitor potential changes in the market and associated risks. AGD would also manage the escalation of non-compliance matters where collaboration fails, including coordinating and engaging with the

Department of Communications and relevant agencies on enforcement measures such as issuing directions, and initiating and managing the civil penalty process where non-compliance warrants enforcement. The estimated regulatory burden of $220 000 per annum will be offset by regulatory savings achieved through *[redacted text]* reforms within the Communications portfolio. OBPR has confirmed this and will report this in Q2 2015. There are limitations in the net benefit analysis due to limited industry data to highlight and compare the costs associated with mitigating national security risks.

ATTACHMENT A

[redacted text]

ATTACHMENT B

<table>
<tr><th colspan="2">Details of C/CSPs Consulted</th></tr>
<tr><td colspan="2">2012 Initial targeted industry consultations</td></tr>
<tr><td colspan="2">Communications Alliance, NBN Co, Telstra, SingTel Optus, Vodafone Hutchinson Australia, Macquarie Telecom, Primus Telecom, iiNet/TransACT/internode, Reach Networks, TPG Telecom Limited, AAPT, PacNet, PIPE and VividWireless.</td></tr>
<tr><td colspan="2">2012-13 Public consultation undertaken through PJCIS Inquiry into Potential Reforms of National Security Legislation</td></tr>
<tr><td>Public Consultation</td><td>On 24 June 2013, the PJCIS tabled its final report entitled Report of the Inquiry into Potential Reforms of Australia's National Security Legislation of which the TSSR was one of three national security reforms considered.The following telecommunication service providers appeared before Committee and discussed TSSR:
- 5 September 2012 – Macquarie Telecom
- 14 September 2012 – Huawei; Australian Mobile Telecommunications Association and Communications Alliance; Optus and Cisco.
- 26 September 2012 – Ericsson
Submissions relevant to TSSR received by the Committee were provided by Telstra; Optus; Vodafone Hutchinson; Macquarie Telecom; iiNet; Huawei; Australian Mobile Telecommunications Association and Communications Alliance; Cisco; Unisys Australia Pty Ltd; Internet Industry Association (IIA); Internet Society of Australia; Pirate Party; Department of Communications and NSW government.</td></tr>
<tr><td colspan="2">April 2014 targeted consultations</td></tr>
<tr><td colspan="2">Communications Alliance, AMTA, NBN Co, Telstra, Optus; Vodafone Hutchinson Australia, Macquarie Telecom, iiNet (owns TransACT, internode, Agile Adam Internet), Soul TPG (owns AAPT and PIPE, NextGen (owns Silk Telecom), M2 (owns Primus, Dodo, Orion, Datafast and iPrimus), Amcom; Exetel, Pacnet, NewSat, Verizon, Digital Distribution Australia, Inmarsat Leasing, New Skies Satellites Australia Victoria Railtrack, Ipstar and Digital River Networks.
Written submissions were received from the Communications Alliance/AMTA, Nextgen, Macquarie Telecom, TPG, Optus, VicTrack and Telstra.</td></tr>
<tr><td colspan="2">February/March 2015 targeted consultations</td></tr>
<tr><td></td><td>Communications Alliance, AMTA, NBN Co, Telstra, Optus, Vodafone Hutchinson Australia, Macquarie Telecom, iiNet, M2, Verizon, Foxtel, aarNet and Next Telecom</td></tr>
</table>

International Comparison

Similar to Australia, other countries are taking steps to manage security risks associated with telecommunication infrastructure and supply chains. These countries recognise that the threat of cyber intrusions into critical telecommunications networks is increasing, and also that the globalisation of the supply chain is increasing the level of security risk in the telecommunication sector. Key concerns shared by these countries include:

- suppliers of concern are currently increasing the services they provide and growing their market share, particularly when these suppliers acquire business in the sensitive parts of networks
- the global trend is for supplier of telecommunications equipment and software to move their management and support functions offshore to a few global centres, creating vulnerabilities for telecommunication networks, and
- there is a global trend for the increasing provision of end-to-end services involving the supply and management of a whole layer of a network.

Furthermore, the benefits to companies of increasing efficiency and reducing overheads can lead them to make decisions that adversely affect the security of their networks and this can have correlating national security implications.

All these factors increase pressure on governments around the world to introduce and continuously build upon strategies to manage the risk posed by those who wish to compromise their national interests and security.

Like-minded countries recognise that managing national security risks to telecommunications infrastructure is a joint responsibility between government and industry and that it can only be achieved through a collaborative approach. These approaches range from weaker to stronger measures *[redacted text]*, with an increasing trend to legislate cyber security requirements and enhance information sharing between government and industry.

[redacted text]

United States of America

Much like the TSSR the US is moving towards legislating regulatory requirements to facilitate risk management of the telecommunication sector and other critical infrastructure sectors. In response to the recent high profile hacking of Sony, President Obama (January 2015) set out for action an updated cybersecurity legislative proposal for Congress, which among other things would enable cybersecurity information sharing between the private sector with the Department of Homeland Security's National Cybersecurity and Communications Integration Centre (NCCIC). This would then be shared with relevant federal agencies and with private sector-developed and operated Information Sharing and Analysis Organizations (ISAOs), by providing targeted liability protection for companies that share information. The proposal also covers national data breach reporting requirements which aim to standardise an existing patchwork of 46 state laws (plus District of Columbia and several territories) to streamline data breach reporting requirements into one federal statute. More recently President Obama signed an Executive Order (13 February 2015) to

support these measures and provide a framework for these to occur while cybersecurity information sharing legislation is being considered by the Congress.

These measures build upon existing arrangements and initiatives. A number of legislative measures have been previously pursued (e.g. *Cyber Intelligence Sharing Protection Act 2013*) to improve cybersecurity arrangements and promote information sharing between the private sector and government. However, privacy issues and sensitivities surrounding the Snowden disclosures have delayed consideration and passage through Congress of any bills promoting information sharing. An Executive Order (EO) 13696 *Improving Critical Infrastructure Cybersecurity,* was signed by President Obama in February 2013 as an interim measure.

A deliverable of the EO is the US National Institute of Standards and Technology (NIST) Cybersecurity Framework which was released in February 2014. The Framework is a risk-based voluntary approach leveraging existing industry standards and complementing existing cybersecurity practices. Its ongoing development is supported by legislation passed recently (18 December 2014) under the Cybersecurity Enhancement Act 2014. Key cybersecurity legislation which supports information sharing on cyber threats is still pending, but expected to be passed soon following approval by relevant Senate and House committees in late March 2015.

In addition, the US is one of the first countries to restrict Chinese telecommunication companies (mainly Huawei and ZTE) from its telecommunication sector due to national security concerns based on the findings of the US House of Representatives Intelligence Committee's report (October 2012). The Report recommended US carriers view Chinese telecommunication companies (particularly Huawei and ZTE) with suspicion, citing data and espionage concerns, and that the US Government and private firms not use Huawei or ZTE equipment. It also recommended that the Committee on Foreign Investment block acquisitions and mergers involving Huawei and ZTE. Huawei's presence in the US market is limited to services outside core and sensitive parts of telecommunication networks such as white labelling under carrier names and selling its branded phones through smaller companies. In April 2013 it was reported that 14.5 per cent of Huawei's international revenue[16] is generated in the Americas.

New Zealand

In November 2013, the New Zealand Parliament passed the Telecommunications (Interception Capability and Security) Bill 2013 which, among other things, establishes a network security compliance regime obliging network operators to engage with the NZ Government on network security, where it might affect NZ's national security interests. It specifically places:

- obligations on network operators to engage in good faith and notify the NZ Government Communications Security Bureau (GCSB) of proposed decisions, actions or changes made in areas of specified security interest (any procurement, or

[16] http://www.telecomasia.net/content/huawei-establish-2nd-home-europe

change to architecture or ownership/control of network operations centres, equipment and information);
- a requirement on network operators to create a proposal to prevent or sufficiently mitigate a security risk identified by GCSB. GCSB will then assess the proposal , and require the network operator to implement it; and
- a pecuniary penalty up to $500 000 for 'serious' non-compliance with a duty. The High Court may impose a further penalty of $50 000 each day or part of a day the contravention continues.

The NZ legislation is comparatively more onerous then obligations under this proposed TSSR framework, noting the additional administrative requirement on C/CSPs to submit annual plans to the NZ Government.

[redacted text]

United Kingdom

In December 2005, Huawei signed a contract with British Telecom's (BT) '21st Century network' (21CN) to deploy its multi-service access network (MSAN) and provide optical transmission products for the revolutionary 21st Century network in which BT were to invest £10b over the next five years. In January 2009, the Chairman of the Joint Intelligence Committee reportedly briefed members of the ministerial committee on national security and the risks presented by Huawei's involvement in the 21CN.

The UK Parliament's Intelligence and Security Committee released a report in June 2013 investigating the relationship between the British telecommunications sector and Huawei. The report recognised a number of concerns affecting national security interests and recommended that there must be:

- an effective process by which the UK Government is alerted to potential foreign investment in the critical national infrastructure;
- an established procedure for assessing the risks;
- a process for developing a strategy to manage these risks throughout the lifetime of the contract and beyond;
- clarity as to what powers the UK Government has or needs to have; and
- clear lines of responsibility and accountability.

Aspects of these recommendations are reflected in the proposed approach under TSSR.

On 18 July 2013, former UK Prime Minister David Cameron tabled in Parliament the UK Government's response to the Committee report. It accepted that national security was not sufficiently considered as part of the BT 21CN contract and committed to a review of the Cell by the National Security Adviser, Kim Darroch. The review was finalised in December 2013. In a written statement to the Parliament, PM Cameron concluded that the UK Government would enhance oversight of the Cell and that the GCHQ should take a leading role in future senior appointments.

The UK Government has also implemented a number of measures to address cyber security as part of its national Cyber Security Strategy. Like the US and the TSSR, the UK has developed with industry a set of voluntary cyber security standards. These now underpin the UK Government's recently released Cyber Essentials scheme – a cybersecurity assurance certification program that caters for both small and large businesses. The scheme is an award to industry that allows them to show customers they have measures in place (based on these cyber security standards) to help protect them from cyber threats. The UK Government requires all suppliers tendering for certain contracts handling personal and sensitive information to be Cyber Essential certified. In addition, the UK has an established Cyber Security Information Sharing Partnership which facilitates the exchange of information on cyber threats between industry and the UK Government in a trusted environment.

India

The Indian Government has taken a stringent approach to address national security concerns presented through the telecommunications supply chain. These measures are stipulated in licensing agreements with telecommunications service providers and focus on the compliance of end-to-end-security standards and the imposition of various trade restrictions. For example, "sensitive" government ICT projects must source from a list of "domestic manufacturer" status companies approved by the Telecom Equipment Manufacturers Association of India.

In addition, India has stringent security review and clearance conditions in place for Chinese investment in sectors such as telecommunications. This includes visa restrictions placed on Chinese business executives. However, recently there has been pressure placed on the Indian Government to relax some of these measures to support foreign investment in the country.

We note that the Indian approach may be as much about supporting local industry development as addressing security concerns.

Taiwan

Taiwanese Government agencies have prohibited telecom operators in Taiwan from procuring telecom equipment from Chinese companies, particularly Huawei. In 2011, Taiwanese national security agencies encouraged telecom operators to quickly replace their existing Chinese-made core network equipment.

Singapore

The Singapore Government amended its Computer Misuse Act in January 2013 with a number of offence provisions relating to the misuse of computer networks or information. The Act includes provisions to strengthen Singapore's ability to protect critical information infrastructure (cyber security measures and requirements), through a ministerial direction which requires any specified person or organisation to take measures or comply with requirements necessary to prevent, detect or counter any threats to ICT.