

2013-2014-2015

THE PARLIAMENT OF THE COMMONWEALTH OF AUSTRALIA

HOUSE OF REPRESENTATIVES/THE SENATE

TELECOMMUNICATIONS AND OTHER LEGISLATION AMENDMENT BILL 2015

EXPLANATORY MEMORANDUM

(Circulated by authority of the
Attorney-General, Senator the Honourable George Brandis QC)

TELECOMMUNICATIONS AND OTHER LEGISLATION AMENDMENT BILL 2015

GENERAL OUTLINE

1. The Telecommunications and Other Legislation Amendment Bill 2015 (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 services and networks.

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. Telecommunications networks and facilities also by their nature hold information of a sensitive nature, which includes information about the network itself, for example, lawful interception systems, customer billing and management systems which, if unlawfully accessed, can reveal sensitive law enforcement operations or the location of people such as politicians or protected persons. This information presents a rich intelligence target for those who wish to harm Australian interests. Telecommunications networks and systems 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 infrastructure of carriers, carriage service providers and carriage service intermediaries (C/CSPs) are attractive targets and for espionage, sabotage and foreign interference activity for 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 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 and thereby extract information and control, and to disrupt and 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), 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 proposed 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 prioritise national security or the public interest over the company's commercial interests and duty to shareholders. 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 section 581(3) of the Telecommunications Act which authorises the Attorney-General to direct 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 companies 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 security framework means security agencies do not have adequate levers to engage those companies who choose not to engage with those agencies to better manage vulnerabilities on their networks and facilities, except for in the most extreme circumstances. 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. AGD and 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 proposed 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 their networks and facilities from being used to commit offences;
- notification requirements in section 202B of the *Telecommunication (Interception and Access) Act 1979* concerning proposed changes to networks and services; and
- the existing directions power in section 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, network infrastructure and facilities from unauthorised access and interference.

Overview of legislative amendments

14. 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 in their networks 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 networks and facilities that may 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 Attorney-General's Department 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)
- 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.

15. The Bill also repeals and reinserts section 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.

16. 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.

17. 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 Attorney-General’s Department (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.

18. 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.

19. 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.

20. 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.

21. The security framework is not about preventing 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.

22. 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 in their networks, regard will be had to existing arrangements that C/CSPs already have in place when the provisions come into effect. While consideration will be given to existing arrangements when compliance with the security obligation is considered, this does not prevent the exercise of the direction 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.

23. 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. There may be circumstances however 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.

24. Implementation of the legislative frameworks will be facilitated through 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. Detailed fact sheets will set out how the framework will be implemented and how government agencies will work with industry to better manage risks of espionage, sabotage, foreign interference and unlawful access to networks and facilities.

FINANCIAL IMPACT

25. The ongoing costs of resourcing and administering the scheme by ASIO and AGD are estimated to be \$1.6 million 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. The costs do not include resources to support any potential review of decisions in the courts as this is a contingent liability. Any such costs would be absorbed by the relevant agencies.

REGULATION IMPACT STATEMENT

26. The Office of Best Practice Regulation (OBPR) has approved the Regulation Impact Statement (RIS) as compliant and meeting best practice requirements. An unclassified version of the RIS is available on the OBPR website.

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 2015

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 2015 (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 Parliamentary Joint Committee on Intelligence and Security's *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 *Telecommunications Act 1997* (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 Committee 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 their networks and facilities from unauthorised access and interference for the purposes of security. This will complement the existing scheme in subsection 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. Proposed 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 from unauthorised access to, or interference with, telecommunications networks or facilities. This is in addition to the current power of the Attorney-General to provide a direction to carriers or carriage service providers 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. Proposed section 315C of the Bill will grant the Secretary of the Attorney-General's Department (the Secretary) 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 *Telecommunications (Interception and Access) Act 1979* (TIA Act), carriers and nominated carriage service providers have a requirement to notify the Communications Access Coordinator (CAC) in the Attorney-General's Department 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/NCSP'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 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 *Australian Security Intelligence Organisation Act 1979* (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 of the ASIO Act. 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 circumstances¹. 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 their networks and facilities from unauthorised access and interference under new sections 313(1A) and (2A) of the Telecommunications Act; and
- information gathering powers granted to the Secretary of the Attorney-General’s Department under new section 315C.

Obligations of C/CSPs to protect their networks and facilities

40. The new obligations for C/CSPs to protect networks and facilities from unauthorised access and interference under new subsection 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 carriers and carriage services providers to do their best to protect telecommunications networks and facilities from unauthorised interference or unauthorised access to ensure the confidentiality, availability and integrity of communications. New section 313(2A) will apply this obligation to 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

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

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 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

44. The right to privacy under Article 17 of the ICCPR will also be engaged by the proposed information gathering powers granted to the Secretary of the Attorney-General's Department under new section 315C of the Telecommunications Act.

45. New section 315C of the Telecommunications Act will provide that the Secretary may obtain from C/CSPs information and documents relevant to assessing compliance with the obligation on a C/CSP to protect its network and facilities from unauthorised interference and unauthorised access under new subsection 313(1A) and (2A). New section 315E enables the Secretary to inspect a document produced under section 315C and may make and retain copies as necessary. New section 315F empowers the Secretary to take possession of the original documents and keep them for as long as he or she deems necessary.

46. The information sought under new section 315C 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 subsection 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 section 315C, and in any event, section 315C is not intended to target end-users.

47. To the extent that new section 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, not be arbitrary and be reasonable, necessary and proportionate to achieving a legitimate objective.

48. The power in new section 315C is necessary to ensure that the Secretary will have the information needed to make an assessment regarding the C/CSP's compliance with their 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.

49. 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 sections 313(1A) and (2A) to do their best to prevent their 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 must permit the person (or a person authorised by the person) to inspect and make copies of the document.

50. Further, safeguards for the protection of personal information specified in the Australian Privacy Principles under the *Privacy Act 1988* (the Privacy Act) will apply to information gathered under section 315C for any incidental personal information collected by the Secretary of the Attorney-General's Department. 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.

51. Under section 315G the Secretary 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.

52. 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 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 to specify how the delegate is to exercise the power. The delegate must comply with any directions issued by the Secretary otherwise the exercise of the power will be invalid.

53. New section 315H of the Telecommunications Act will provide that a person who obtains information or a document under section 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.

54. It is necessary that the Secretary be able to consult with officials in the Department and 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 obtained under section 315C to the Attorney-General or other relevant Ministers for the purpose of exercising the Attorney-General's directions power in new section 315A (previously section 581(3)), new section 315B, or more broadly for the purposes of security).

55. Information obtained under section 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 security issues that have been

identified. 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.

56. New section 315H also contains important protections governing how the information and documents obtained under either section 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.

57. 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

58. 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.

59. 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 section 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.

60. Under existing section 581(3) the Attorney-General may direct a carrier or carriage service provider 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 *Administrative Decisions (Judicial Review) Act 1977*. 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 proposed new direction power in section 315B.

61. 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 section 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.

62. 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 section 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 be 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, or Australian interests, or to foreign countries to which Australia has responsibilities.

63. 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 section 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 section 581(3) to clarify that the power cannot be exercised unless it is on the basis of an adverse security assessment. 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.

64. Further, introduction of the new power of the Attorney-General to give directions to C/CSPs in proposed new section 315B is intended to reduce the need to rely on the existing powers under section 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.

65. 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.

66. First, the threshold for exercising the power is high. 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.

67. Second, the power cannot be exercised without an adverse security assessment or without 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 be prejudicial to the interests of that person.

68. 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 eliminated 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.

69. 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.

70. 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 company 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

71. 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.

72. Proposed 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.

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

74. 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 subsection 313(1A) and (2A). The information-gathering powers of the Secretary 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.

75. However, subsection 315(D)(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 subsection 313(1A) and (2A).

76. 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 arose 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.

77. 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 may institute a proceeding for the recovery of a pecuniary penalty relating to a contravention of 315C(3) regarding compliance with a written notice given to a C/CSP to give the Secretary 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 \$10 million for a body corporate and \$50,000 for a natural person.

78. 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.

79. The Secretary 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 implications for national security.

80. 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 \$10 million 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

81. 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 hearing². 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.

82. 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 *Administrative Decisions (Judicial Review) Act 1977*.

83. 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 14 days (unless circumstances are urgent) to provide a written response which must be taken into account in issuing a direction.

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

84. 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 65 to 70. As noted in paragraph 62, 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.

85. 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 Tribunal for merits review of the security assessment.

Conclusion

86. 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

87. Clause 1 is a formal provision specifying the short title of the Bill. It provides that when the Bill is enacted, it be cited as the *Telecommunications and Other Legislation Amendment Act 2015*.

Clause 2 – Commencement

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

89. 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.

90. 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

91. 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

92. 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 C/CSPs to protect networks and facilities 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 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) (in other words, to protect their network and systems from unauthorised access and interference). Provision is also made for a C/NCSP to be exempted, in full or in part, from the notification requirement based on ASIO's assessment of the risk profile of the company or aspects of the company's business. C/NCSPs will also be provided with the

option of submitting a Security Capability Plan 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 Attorney-General's Department 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 section 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.

93. 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 subsection 313(1A) and 313(2A) of the Telecommunications Act.

94. 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 section 581(3) to relocate it in new section 315A.

Item 1 – Section 5

95. 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

96. Item 2 inserts the following eight new defined 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 – Before section 311

97. Item 3 inserts the heading ‘Division 1–Simplified Outline’ into ‘Part 14 – National interest matters’ of the Telecommunications Act to apply consistent drafting conventions.

Items 4 and 5 – Section 311 and at the end of section 311

98. Section 311 outlines the key provisions in Part 14 of the Act. Items 4 and 5 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 the Attorney-General’s Department.

Item 6 – Before section 312

99. Item 6 inserts the heading ‘Division 2–Obligations of ACMA and carriers and carriage service providers’ to apply consistent drafting conventions.

Item 7 – After subsection 313(1)

100. Item 7 inserts a new subsection (subsection 313(1A)) into section 313 to establish a new obligation for carriers and carriage service providers (C/CSPs) to protect telecommunications networks and facilities 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 their 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.

101. 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 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. In this way, the terms ‘unauthorised access’ and ‘unauthorised interference’ are defined within the context of security threats of espionage, sabotage and interference.

102. 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.

103. It encourages a risk based approach to managing risks of espionage, sabotage and foreign interference. 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.

104. Importantly, while the obligation applies universally to all C/CSPs, the requirement to do your 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 their networks and facilities 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.

105. 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.

106. 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 and factsheets 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.

107. 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, 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.

108. The Bill does not prescribe what technical solutions a C/CSP should use to secure its network 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* of its network and systems, 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.

109. 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.

110. 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 its network and facilities, infrastructure and information stored or transmitted within, 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).

111. 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.

112. 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 AGD and/or ASIO.

113. 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 Australian Privacy Principles (APPs) contained in the *Privacy Act 1988* (Privacy Act), including 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 APP 11 and the obligation under paragraph 313 (1A) (c), there are a number of differences, including:

- section 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 APP 11 is concerned with protecting individual's privacy.

114. Importantly, while there may be overlap between the steps that a C/CSP might take under section 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 section 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, APP 11 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.

115. Guidance produced by agencies such as the Australian Communications and Media Authority 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 8 – After subsection and 313(2)

116. Item 8 mirrors the obligation under Item 7 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.

Items 9 and 10 – Paragraph 313(5)(a) and at the end of subsection 313(5)

117. Items 9 and 10 extend the operation of the existing good faith protection 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 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.

118. In other words, the provision provides a C/CSP with a broad protection from any liability to a third party for any damage caused 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.

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

Item 11 – After section 314

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

120. Item 11 will insert the heading Division 3 after an existing provision in Part 14, section 314 to apply consistent drafting conventions.

Subdivision A – Individual notifications

121. 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 Communications Access Co-ordinator (CAC) within the Attorney-General’s Department of planned changes to telecommunications services or systems which are likely to have a material adverse effect on the capacity of the C/NCSP to meet their security obligation under the new subsection 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.

122. 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 their obligations under the TIA Act or section 313 of the Telecommunications Act. This Bill will exclude the new security obligations under subsection 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.

123. 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 and factsheets 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.

124. 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

125. 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.

126. 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 subsection 313(1A) or 313(2A) to protect networks from risks of unauthorised access and unauthorised interference.

127. 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).

128. 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

129. Section 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.

130. 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.

131. 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.

132. The CAC may revoke or amend an exemption made under section 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.

133. The statement in subsection 314A(7) that an exemption granted under subsection 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

134. 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.

135. In all circumstances following notification the C/NCSP will receive a notice from the CAC within 30 days. This may be either a:

- 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.

136. 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 the Attorney-General's Department may consider use of his or her new information gathering powers under section 315C of the Telecommunications Act.

137. 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 subsection 313(1A) and (2A).

138. 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.

139. 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 subsection 313(1A) and (2A).

140. 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.

141. The notice provided to the C/NCSP under section 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 section 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

142. Item 11 will also add new sections 314C to 314E to Part 14 of the Telecommunications Act, which will allow C/NCSPs to submit a Security Capability Plan to the CAC. The Plan 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.

143. 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 Security Capability Plan. This plan would be in lieu of individual notifications under section 314A. Section 314E will clarify that if a change is included in a Security Capability Plan 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 plan would need to be separately notified under section 314A. For clarity submission of a Security Capability Plan would not operate to exempt the C/NCSP from the notification requirements in section 314A, where the Security Capability Plan failed to adequately notify of a planned change or changes.

144. The submission of a Security Capability Plan 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 Security Capability Plans 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 Security Capability Plan process. As noted above, section 314E clarifies that if a proposed adverse change included in a Plan 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.

145. The benefits of submitting a Security Capability Plan 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 Security Capability Plan 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.

146. 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.

147. Inclusion of information about a C/NCSP's security policies, 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 subsection 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 Security Capability Plan 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

148. The Security Capability Plan provisions are intended to complement and supplement the new notification provisions in section 314A. For example, a Security Capability Plan, 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 subsection 313(1A) or 313(2A).

149. Section 314C sets out the matters that may be included in a security capability plan if a C/NCSP chooses to submit a plan. There is no particular date on which a plan 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.

150. This includes specifying that the kinds of changes that should be included in the plan includes (but is 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 Security Capability Plan will also be provided in administrative guidelines and factsheets.

Assessment process following notification

151. Section 314D outlines the administrative process following submission of a security capability plan to the CAC. Under section 314D the CAC has 60 days to assess all of the proposed changes in the plan. 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).

152. 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 Security Capability Plan (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.

153. The effect of section 314D is that each change included in a Security Capability Plan 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.

154. 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.

155. 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/CSPs ability to meet its obligation to secure its network to support the Attorney-General in exercising the new directions power 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 section 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 subsection 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).

156. 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 subsection 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 security capability plans 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.

157. There is no exemption process associated with Security Capability Plans 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 Security Capability Plan.

158. Item 11 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 12 – After section 315

Division 5 – Directions by Attorney-General

159. Item 12 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

160. Item 12 relocates repealed section 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. Section 581(3) of the Telecommunications Act is repealed under Item 27 of the Bill.

161. 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 Administrative Appeals Tribunal. The Bill will also remove a current limitation on judicial review of a direction under the *Administrative Decisions (Judicial Review) Act 1977*.

162. The provision 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

163. 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 as 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 direction 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.

164. 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 section 581(3) was already included in the list of prescribed administrative actions which could be the subject of an ASIO security assessment, Item 12 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).

165. 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 was 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.

166. 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 Administrative Appeals Tribunal. 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 Tribunal for merits review of the security assessment.

167. The Bill (Item 31) 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 section 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

168. 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 that 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.

169. 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.

170. 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 (315B(1)) that would be prejudicial to security having reference to the meaning of 'security' in the ASIO Act (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.

171. 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 power 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

172. 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 313B(3). Subsection 315B(3) limits the purpose for which the Attorney-General can issue a direction, to reducing or eliminating the risks identified in subsection 315B(1). In other words, the direction must specifically direct action that seeks to reduce or eliminate the risk of unauthorised access or interference which would otherwise result in a risk prejudicial to security.

173. Noting that the security framework is directed at better managing national security risks associated with the supply of equipment, services and support arrangements, the direction 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.

174. 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.

175. Subsection 315A(3) of the Telecommunications Act provides that the Attorney-General cannot exercise the direction 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/CSPs' 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.

176. 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 Administrative Appeals Tribunal. 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 Tribunal for merits review of the security assessment.

177. In addition to making an adverse security assessment a pre-condition to the exercise of the direction 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 the Attorney-General's Department) 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.

178. 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.

179. Subsection 315B(6) provides a criteria to assist the Attorney-General arrive at a reasonable decision on whether a direction should be issued and what should be included in the direction. The Attorney-General must consider all the factors listed which include considerations about potential costs associated with implementing the proposed direction, potential impact for competition in the sector and potential impacts for end-users. This is to ensure 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. Importantly, subsection 315B(6) clarifies that the potential harm to Australia's security must be given the greatest weight when the Attorney-General is considering whether to issue a direction. Subsection 315B(7) clarifies that the matters listed in subsection (6) are not intended to limit or prescribe the matters to which the Attorney can have regards when exercising the power.

180. 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 this 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'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 directions power and take into account factors such as the potential impact for the affected C/CSP, end-users and the economy more broadly.

181. 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).

182. 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 14 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 14 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 Administrative Appeals Tribunal 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.

183. Subsection 315B(8) does not specify the form in which representations should be made other than 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.

184. 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 the Attorney-General's Department.

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

186. 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 17-25. 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.

187. 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'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

188. Item 12 inserts Division 6, which sets out the Secretary of the Attorney-General's Department's new information-gathering powers under sections 315C-315H.

189. The Secretary 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 their networks and facilities under subsection 313(1A) and (2A). In exercising the power the Secretary must have the belief that the C/CSP has information or documents that would assist the Secretary to assess compliance with the duties in subsection 313(1A) and (2A). It is not necessary that the Secretary 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.

190. 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 ACMA's existing information-gathering powers in Part 27 of the Telecommunications Act and include existing protections against self-incrimination.

191. 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.

192. 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 clarifies that a notice under section 315C must be complied with even if it exposes the person to criminal or civil liability. However, subsection 315D also 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.

193. 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.

194. 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.

195. Subsection 315C(4) sets out the requirements for a notice issued by the Secretary under subsection 315C(2). Subsections 315C(2) and 315C(4) have the effect of requiring the Secretary 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 is to ensure that 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.

196. Given the potential sensitivities of information required to be provided to the Secretary (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.

197. Section 315E clarifies that the Secretary may inspect a document produced under section 315C and may make and retain copies as necessary. Section 315F empowers the Secretary to take possession of the 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 compelled is however limited by relevance to the security obligation imposed in subsection 313(1A) and (2A). Section 315F imposes requirements on the Secretary (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.

198. Section 315G allows the Secretary 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 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 to specify how the delegate is to exercise the power. The delegate must comply with any directions issued by the Secretary otherwise the exercise of the power will be invalid.

199. Section 315H authorises the further use or disclosure of information or documents obtained under section 315C to persons other than the Secretary or their delegate. Disclosure must be either for the purpose assessing compliance with a C/CSP's obligation to protect their 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 section 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.

200. While section 315H does allow an expanded number of people to access the information or document, 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 subsection 313(1A) or 313(2A).

201. Safeguards are built into section 315H to protect commercially sensitive information provided by C/CSPs. Subsection 315H(2) requires the Secretary, the Director-General 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. 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.

202. 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. 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.

203. Australian Government agencies subject to the *Privacy Act 1998* (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).

204. 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.

205. 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.

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

207. 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.

208. Although there are no express consequences for a breach of the confidentiality requirements in subsection 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.

Item 13 – Before section 316

209. Item 13 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 14 – Subsections 564(1) and (2)

210. The directions powers granted to the Attorney-General and the information-gathering powers granted to the Secretary of the Attorney-General’s Department 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.

211. It is expected that the Attorney-General (supported by the Attorney-General’s Department) would manage all compliance and enforcement action with respect to provisions in this Bill. However, this Bill does not expressly preclude the Australian Communications and Media Authority (ACMA) from taking separate and independent action with regard to these new provisions.

212. Item 14 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 15 – After subsection 564(3)

213. 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 15 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.

Item 16 – Before subsection 564(4)

214. Item 16 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 17 – Subsection 571(1)

215. 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 17 grants the Attorney-General that same ability.

Item 18 – Before subsection 571(3)

216. Item 18 inserts the heading ‘Limit on standing of the ACMA’ before existing subsection 571(3) of the Telecommunications Act, which identifies provisions under which ACMA is not entitled to institute a proceeding for the recovery of a penalty.

Item 19 – At the end of section 571

217. Like the limitation imposed on the standing of the Attorney-General to seek injunctive relief, Item 19 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 Act to address non-compliance with the security obligation (new subsection 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 20 – Section 572A

218. Item 20 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 21 – Subsections 572B(1), (3) and (4)

219. 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 subsection 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 22 – At the end of subsection 572B(5)

220. Item 22 authorises (but does not oblige) the Attorney-General to publish the undertaking on the Attorney-General’s Department’s website.

Item 23 – After subsection 572B(5)

221. Item 23 limits the Attorney-General’s authority to accept an undertaking to an undertaking which addresses compliance with the security obligation (new subsection 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) 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 24 – Subsection 572C(1)

222. Item 24 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 25 – At the end of section 572C

223. Item 25 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 subsection 315A(5) or 315B(12) or notice to provide information or a document under new subsection 315C(3).

Item 26 – Subsections 581(3) and (3A)

224. Item 26 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 27 – Subsection 581(4)

225. Item 27 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 28 – Subsection 581(5)

226. Item 28 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 29 and 30 – Subparagraph 202A(a)(ii) and at the end of paragraph 202B(1)(b)

227. Item 29 will amend the TIA Act to exclude the new obligations to protect networks and facilities from unauthorised access and interference in section 313(1A) and (2A) of the Telecommunications Act from the purpose of Part 5-4A of the TIA Act.

228. Item 30 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 section 313(1A) and 313(2A).

229. 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 31 – Paragraph (daa) of Schedule 1

230. Item 31 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 32 – Subsection 35(1) (subparagraph (d)(ii) of the definition of *prescribed administrative action*)

231. Item 32 repeals the reference to existing section 581(3) in the definition of prescribed administrative action and substitutes a reference to the Attorney-General's direction powers under new section 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 33 – Paragraph 38A(1)(b)

232. Item 33 repeals paragraph 38A(1)(b) which references the Attorney-General's direction making powers and substitutes reference to the new section 315A and 315B.

PART 3 – TRANSITIONAL PROVISIONS

Item 34 – Transitional and saving provisions

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

234. Item 34 provides that any directions made by the Attorney-General under the existing section 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.

235. Item 34 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 proposed subsection 315A.

236. Item 34 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.