# 3

# Telecommunications security

3.1 The Terms of Reference to this inquiry state that the Government expressly seeks the views of the Committee on amending the *Telecommunications Act 1997* to address security and resilience risks posed to the telecommunications sector. This would be achieved by:

- instituting obligations on the Australian telecommunications industry to protect their networks from unauthorised interference;
- instituting obligations to provide Government with information on significant business and procurement decisions and network designs;
- creating targeted powers for Government to mitigate and remediate security risks with the costs to be borne by providers; and
- creating appropriate enforcement powers and pecuniary penalties.

3.2 The Attorney-General's Department (AGD) discussion paper notes that, with the pace of technological change, serious challenges to the security of telecommunications data have emerged:

> Risks to the availability, confidentiality and integrity of our national telecommunications infrastructure can come from hardware vulnerabilities, accidental misconfiguration, external hacking and even trusted insiders.[1]

3.3 The implications of this risk are significant, especially given that Australian businesses, individuals and public sector actors rely on telecommunication carriers and carriage service providers' (C/CSPs) ability to store and transmit their data safely and securely, and to protect it from potential national security threats. The discussion paper notes that:

---

1 Attorney-General's Department, *Equipping Australia against emerging and evolving threats*, Discussion Paper, July 2012, p. 29.

> Failure to effectively manage national security risks therefore has implications beyond individual C/CSPs; it is a negative externality affecting government, business and individual Australians.[2]

3.4 The discussion paper further explains the significance of the telecommunications industry to national security:

> While advances in technology and communications have resulted in unquestionable benefits to society and the economy, they have also introduced significant vulnerabilities, including the ability to disrupt, destroy, degrade or alter the functioning of our critical telecommunications infrastructure and the information held on it. A clear understanding of the current telecommunications environment is essential to identifying network vulnerabilities and managing them effectively. This includes the composition and operation of the telecommunications industry, national security risks, and the current regulatory environment.[3]

3.5 The discussion paper cites the Director-General of ASIO's speech at the Security in Government Conference on 7 July 2011 outlining how poor security of telecommunications information poses a threat to national security:

> States, as well as disaffected individuals or groups, are able to use computer networks to view or siphon sensitive, private, or classified information for the purpose of, political, diplomatic or commercial advantage.
>
> Individual records or files stored or transmitted on telecommunications networks may not be classified or particularly sensitive in and of themselves but, in aggregate, they can give foreign states and other malicious actors a range of intelligence insights not otherwise readily available. This threat extends to information vital to the effective day-to-day operation of critical national industries and infrastructure, including intellectual property and commercial intelligence.[4]

3.6 Furthermore, these threats come from a variety of sources:

> …other nation states, acting in their own national interest; criminal syndicates, especially – but not exclusively – well-resourced organised

---

2 Attorney-General's Department, *Equipping Australia against emerging and evolving threats*, Discussion Paper, July 2012, p. 29. An externality refers to a cost or benefit that accrues to actors which are not directly involved in a transaction.

3 Attorney-General's Department, *Equipping Australia against emerging and evolving threats*, Discussion Paper, July 2012, p. 30.

4 Attorney-General's Department, Equipping Australia against emerging and evolving threats, Discussion Paper, July 2012, p. 32.

> crime networks, which in some cases operate transnationally, compounding the difficulty of detecting and disrupting their activities; business corporations seeking commercial advantage over competitors; political or other issue-specific motivated groups; cyber-vandals; and a catch-all of other malicious and non-malicious 'hacktivists'.[5]

3.7 These threats originate in many different countries. According to a recent study by McAfee:

> 36 percent of all attacks originated from the United States, 33 percent from China and 12 percent from Russia. Of the remainder, Germany, the UK and France accounted for no more than six percent.[6]

3.8 The McAfee study also discussed the types of threats, finding that of the telecommunications infrastructure companies surveyed:

> 89 percent … had experienced infection by a virus or malware; 60 percent had experienced 'theft of service' attacks; 54 percent experienced 'stealthy infiltration' that targeted theft of data or the takeover of critical Supervisory Control and Data Acquisition control systems; approximately 20 percent experienced extortion through the targeting and infiltration of control systems; and 29 percent had experienced large scale distributed denial of service attacks, often several times a month, of which two thirds had impacted on operations.[7]

3.9 To counter those threats, the discussion paper proposes the development and implementation of a 'risk based regulatory framework to better manage' these national security challenges to telecommunications security.[8]

3.10 The discussion paper proposes a package of reforms to the *Telecommunications Act 1997* and associated legislation to establish this regulatory framework:

- An industry-wide obligation on all C/CSPs to protect their infrastructure and the information held on it or passing across it from unauthorised interference to support the confidentiality, integrity and availability of Australia's national telecommunications infrastructure;
- A requirement for C/CSPs to provide Government, when requested, with information to assist in the assessment of national security risks to telecommunications infrastructure; and

---

5 Ian Dudgeon, 'Cyber-Security: the importance of partnerships', *Regional Security Outlook 2013*, Council for Security Cooperation in the Asia-Pacfic, p. 9.

6 Ian Dudgeon, 'Cyber-Security: the importance of partnerships', *Regional Security Outlook 2013*, Council for Security Cooperation in the Asia-Pacfic, p. 10.

7 Ian Dudgeon, 'Cyber-Security: the importance of partnerships', *Regional Security Outlook 2013*, Council for Security Cooperation in the Asia-Pacfic, p. 10.

8 Attorney-General's Department, *Equipping Australia against emerging and evolving threats*, Discussion Paper, July 2012, p. 29.

- Powers of direction and a penalty regime to encourage compliance.[9]

3.11 The discussion paper states that the desired outcomes of the proposed framework are that:

- government and industry have a productive partnership for managing national security risks to Australia's telecommunications infrastructure,
- security risks relating to Australia's telecommunications infrastructure are identified early, allowing normal business operations to proceed where there are no security concerns and facilitating expedient resolution of security concerns,
- security outcomes are achieved that give government, business and the public confidence in their use of telecommunications infrastructure for both routine and sensitive activities,
- the protection of information, including customer information and information about customers, contained on or transmitted across telecommunications networks is better assured, and
- compliance costs for industry are minimised.[10]

## Issues raised in evidence

### Is there a need for an industry wide obligation to protect telecommunications?

3.12 Mr Mark Newton disputed the discussion paper's contention that there is a need for Government intervention in the telecommunications industry for the purpose of national security advising that 'it isn't the role of carriers and carriage service providers (C/CSPs) to make business decisions in the intelligence community's best interests', rather:

> It's the intelligence community's job to stay sufficiently informed and organisationally nimble that they can accommodate C/CSPs' business decisions without feeling a need to interfere in them.[11]

3.13 In a similar vein, Mr Daniel Black contended that telecommunications security was the Government's responsibility:

---

9 Attorney-General's Department, *Equipping Australia against emerging and evolving threats*, Discussion Paper, July 2012, p. 34.

10 Attorney-General's Department, *Equipping Australia against emerging and evolving threats*, Discussion Paper, July 2012, pp. 29-30.

11 Mr Mark Newton, *Submission No. 87*, p. 10.

> Private industry values the privacy of its business and procurement decisions as much as the government values its "information about the national security environment". Instituting obligations in legislation is a crude mechanism and shows the government to industry relationship is broken that these meaningful private dialogues are not taking place to the level required.[12]

3.14 Macquarie Telecom disagreed that there is a need for Government intervention on the issue of security because it saw that providing security was already in the interests of service providers:

> You could imagine that we would have a significant interest in ensuring that that information is kept secure and that it is retained and dealt with at a high level of security. In that sense we wanted to bring it to the attention of the committee that the market is responding to the need for cyber security. We are not saying that means that the entire Australian network and national security is in perfect hands, but we want to bring it to the attention of the committee that there are market responses going on that ought to be taken into account when thinking about what the broader regulatory arrangements should be that affect all players.[13]

3.15 Macquarie Telecom contended that industry-led self-regulation would be a more proportionate alternative regulatory intervention. Self-regulation could involve a voluntary obligation to protect telecommunications infrastructure, networks and systems. Macquarie Telecom further argued that an unenforceable industry code, informed by government guidelines, would be preferable for obtaining voluntary compliance.[14]

3.16 In contrast, the Commonwealth Privacy Commissioner (within the Office of the Australian Information Commissioner), Mr Timothy Pilgrim, agreed with the discussion paper's objective of requiring telecommunications industry participants to protect information:

> The Office of the Australian Information Commissioner welcomes the fact that one of the desired outcomes of the framework is that the security of individuals' personal information contained on or transmitted across telecommunication networks is better assured.
>
> The OAIC supports the policy intention behind the proposal to introduce a regulatory framework that will address security and resilience risks posed to Australia's telecommunications infrastructure.

12 Mr Daniel Black, *Submission No. 97*, p. 7.

13 Mr Matthew John Healy, National Executive, Industry and Policy, Macquarie Telecom, *Transcript,* 5 September 2012, pp. 11 -12.

14 Macquarie Telecom, *Submission No. 115*, pp. 2-3.

> …
>
> The OAIC welcomes the fact that one of the desired outcomes of the framework is that the security of individuals' personal information contained on or transmitted across telecommunication networks is better assured.[15]

3.17 In contrast to Macquarie Telecom, another telecommunications industry participant, Optus, favoured obligations being equally placed on all industry participants and expressed 'cautious support' for a legislated framework:

> For a number of years Optus has engaged informally with national security agencies on matters relating to the security and resilience of its networks and business operations, including offshore operations. Having regard to the positive aspects of this experience, Optus has formed the view that it is desirable to move to a more structured scheme, to ensure that the benefits and responsibilities are proportionately shared across the industry (for competitive and equity reasons). Optus provides "cautious support" for the implementation of a scheme.[16]

3.18 Optus' cautious support was contingent on how the Government might design such a framework:

> I want to emphasise that our caution arises more from the challenge of correctly calibrating the practical design of such a scheme (and the down-side risks of incorrectly calibrated arrangements), than fundamental concern about the principle.[17]

## How should a telecommunications security model be structured?

3.19 The AGD discussion paper proposes a compliance framework, based on requiring industry participants to be able to demonstrate 'competent supervision' and 'effective control' over their networks.

3.20 Competent supervision refers to the ability of a service provider to maintain technically proficient oversight of the operations of their network, and the location of data; awareness of, and authority over, parties with access to network infrastructure; and a reasonable ability to detect security breaches or compromises.[18]

---

15 Mr Timothy Pilgrim, Privacy Commissioner, Office of the Australian Information Commissioner, S*ubmission No. 183*, p. 16.

16 Optus, *Submission No. 206*, p. 3.

17 Optus, *Submission No. 206*, p .3.

18 Attorney-General's Department, *Equipping Australia against emerging and evolving threats*, Discussion Paper, July 2012, p. 35.

3.21 Effective control refers to the ability of a C/CSP to maintain direct authority or contractual arrangements which ensure that its infrastructure and the information held on it is protected from unauthorised interference.[19]

3.22 Optus agreed that this proposed framework could be effective:

> We support the idea that a scheme should be targeted to achieve and verify outcomes, rather than be prescriptive about particular business practices, network designs or purchasing decisions. This aligns with the proposed approach of a scheme requiring carriers to demonstrate:
>
> - Competent supervision; and
> - Effective control.[20]

3.23 The Australian Mobile Telecommunications Association and Communications Alliance, representing the industry as a whole, preferred an outcomes-based approach to regulation:

> The Associations agree that the regulatory framework should focus on security outcomes rather than technical requirements and that industry should be able to demonstrate compliance rather than have prescriptive obligations imposed.
>
> Noting the importance of network security and resiliency in the digital age, the Associations on the whole welcomes the Government's pragmatic security outcomes/objectives based approach as opposed to stipulating a requirement for Government approval of network architecture at a technical or engineering level.[21]

3.24 Similarly, the Commonwealth Privacy Commissioner, within the Office of the Australian Information Commissioner, agreed that a framework should be focussed on the end results, rather than a prescriptive government-led process:

> The Office of the Australian Information Commissioner considers that such an outcomes-based regulatory framework would ensure that [service providers] have sufficient flexibility to respond to changes in telecommunications technology, whilst also ensuring that the Government remains responsible for ensuring that the overall protection of personal information is achieved.[22]

---

19 Attorney-General's Department, *Equipping Australia against emerging and evolving threats*, Discussion Paper, July 2012, p. 36.

20 Optus, *Submission No. 206*, p. 3.

21 Australian Mobile Telecommunications Association and Communications Alliance, *Submission No. 114*, p. 17; see also: Huawei Technologies (Australia) Pty Limited, *Submission No. 149*, p. 11.

22 Mr Timothy Pilgrim, Privacy Commissioner, Office of the Australian Information Commissioner, S*ubmission No. 183*, p. 16.

3.25 The Australian Mobile Telecommunications Association and Communications Alliance further argued that direct government control of the business decision-making process would be excessive:

> A regulatory regime that mandates external controls over procurement and network design practices and requires extensive notification practices would certainly amount to an overly prescriptive level of intervention.
>
> The Associations believe that such a regulatory framework would restrict the ability of network and infrastructure providers to cost-effectively implement platforms that are innovative, progressive and provide supplier differentiation. Controls over procurement would also unnecessarily increase timeframes for network rollouts, which would contradict the Government's advocacy for increased broadband deployment.[23]

## Information sharing and compliance auditing

3.26 The AGD discussion paper states that Government would provide guidance to assist industry to understand and meet its obligations, and to inform Carriers/Carriage Service Providers (C/CSPs) how they can maintain competent supervision and effective control over their networks. In order to monitor compliance with the obligations under a framework, C/CSPs would be required to demonstrate compliance to Government. This could be done by compliance assessments and audits, based on a risk assessment to inform the level of engagement required.[24]

3.27 In relation to the inherent risk of private sector entities being obliged to provide information to Government Mr Mark Newton observed that:

> Businesses also need to be mindful of the fact that any information they provide to the Government can potentially be released (e.g., under Freedom of Information, subpoena, or leak), so it's wise to be reluctant about sharing.[25]

3.28 The Committee observes that industry is required to provide similar network and service information to the Attorney-General's Department under the interception capability obligations contained in the *Telecommunications (Interception and Access) Act 1979*. That information is given statutory protection

---

23 Australian Mobile Telecommunications Association and Communications Alliance, *Submission No. 114*, p. 17.

24 Attorney-General's Department, *Equipping Australia against emerging and evolving threats*, Discussion Paper, July 2012, p. 36.

25 Mr Mark Newton, *Submission no. 87*, p. 10.

from disclosure to any other person without the written permission of the C/CSP concerned.[26]

3.29 Macquarie Telecom, in accepting that protecting the security of Australia's telecommunications network infrastructure is in Australia's national interest, noted that it was incumbent on Government to communicate with industry:

> At the same time, C/CSPs and other players in the broader communications sector are highly motivated to ensure the security of their own network infrastructure, systems and data. With a clear alignment between the interests of industry players and the Government on the need for network infrastructure security, Macquarie believes a better outcome could be achieved with increased communication at a trusted level between industry and Government.[27]

3.30 The complementary roles that industry and government can play was highlighted by Vodafone Hutchison Australia:

- The Government's security agencies are best placed to outline what are actual and emerging security risks and provide clear guidance to the industry about effective protections and controls to mitigate these risks.
- The telecommunications industry is best placed to determine what are the most appropriate operational and technical controls for their businesses.[28]

3.31 The Australian Mobile Telecommunications Association and Communications Alliance argued that industry participants need to know in advance of making their decisions what position and advice Government may have:

> The Associations have proposed that requirements regarding networks and infrastructure need to be clearly defined so that industry can invest and deploy infrastructure with confidence and, without concern that government will raise objections once such networks are deployed.[29]

3.32 Telstra highlighted uncertainty in how risk assessments might work in practice:

> What is not clear is whether these "risk assessments" would be subject to legislated timeframes so as to avoid delaying procurement or network design activities. It is also unclear if C/CSPs will have to implement the

---

26 *Telecommunications (Interception and Access) Act 1979*, section 202.

27 Macquarie Telecom, *Submission No. 115*, p. 2.

28 Vodafone Hutchison Australia, *Submission No. 113*, p.2; see also: Optus, *Submission no. 206*, p. 3, Cisco Systems Australia Pty Limited, *Submission No. 112*, p. 2; and Huawei Technologies (Australia) Pty Limited, *Submission No. 149*, p. 12.

29 Australian Mobile Telecommunications Association and Communications Alliance, *Submission No. 114*, p. 18; see also: Telstra, *Submission no. 189*, p. 12.

> suggested outcomes of the "risk assessments" and if there are any penalties for not doing so.[30]

## Remediation powers and a penalty regime

3.33 The AGD discussion paper proposes that the risk management framework for determining that Carriers and Carriage Service Providers (C/CSPs) will practice competent supervision and effective control of their systems will need to be underpinned by penalties and the ability of government to make directions to service providers:

> Where potential issues of concern are identified, the preferred approach would be to engage with the relevant C/CSPs to establish whether national security concerns can be co-operatively addressed. Where this is not possible, one way to proportionately address various levels and forms of non-compliance could be to provide a graduated suite of enforcement measures (including the power of direction). The availability of enforcement measures would provide industry with greater incentive to engage co-operatively with Government.
>
> Under such an approach, in cases where engagement with C/CSPs proves to be ineffective, or a blatant disregard of security information jeopardises the Government's confidence in the security and integrity of Australia's telecommunications infrastructure, powers of direction could provide a proportionate means to achieve compliance. [31]

3.34 The Australian Mobile Telecommunications Association and Communications Alliance in their joint submission were not convinced that it is yet necessary to create an interventionist or punitive compliance regime:

> With regard to the proposal for an amendment to the Act to allow for the creation of appropriate enforcement powers and associated pecuniary penalties, the Associations' position is that development of a financial penalties framework is premature, and not conducive to the development of an appropriate level of trust, and a common vision on security and resiliency, between Government and service providers.[32]

3.35 Telstra argued that government already possesses the means to dissuade service providers from engaging in poor security practices:

---

30 Telstra, *Submission No. 189*, pp. 12-13.

31 Attorney-General's Department, *Equipping Australia against emerging and evolving threats*, Discussion Paper, July 2012, p. 37.

32 Australian Mobile Telecommunications Association and Communications Alliance, *Submission No. 114*, p. 19.

> Telstra believes the most sensible way to provide these incentives would be through the Government's own procurement practices – i.e. Government to specify in requests for proposal/tender their security, resilience and integrity requirements for IT and communications services supplied to Government by C/CSPs.[33]

3.36 The Australian Mobile Telecommunications Association and Communications Alliance also argued that if the framework in the discussion paper was to be established as proposed, the framework should include avenues to appeal government decisions:

> The Associations propose that it should include a facility for an appropriate and truly independent means of review or appeal to prevent arbitrary or unjust use of directions or penalties.[34]

## Other considerations

### Regulatory impacts

3.37 The Committee received some limited evidence about the potential regulatory impacts that the telecommunications security reform might have on industry. However, these points were not elaborated upon in submissions or in oral evidence to the Committee. The Australian Mobile Telecommunications Association and Communications Alliance in their joint submission stated:

> Concerns previously raised by the Associations on the proposal to make legislative and regulatory changes to enhance the security and resilience of telecommunications network infrastructure, are as follows:
>
> - the potential for the proposed regime to bring providers into conflict with existing corporate regulations, particularly those relating to the disclosure of information;
> - the compatibility of the proposed regime with existing corporate governance where a provider's activities might be driven by decisions made outside of Australia. Many operators have global or regional supply arrangements which would in effect become invalid under the proposed regime. This would result in costs to operators in the amount of many millions of dollars as a result of having to break regional/global supply contracts;
> - impacts on competition in the market-place and risk that proposed requirements may create a barrier to entry for new, lower cost providers and could eliminate some of those already in the market,

33 Telstra, *Submission No. 189*, p. 13.

34 Australian Mobile Telecommunications Association and Communications Alliance, *Submission No. 114*, p. 18.

resulting in decreased market competition on pricing and general consumer detriment;

- the absence, to date, of any protection/indemnity to civil action for providers who have acted in good faith under the requirements of the proposed amendments;
- the fact that the rapidly changing technology landscape, where potential vulnerabilities now exist at the physical, network and application layers, has not been sufficiently taken into account, specifically with regards to the concept of "critical infrastructure"; and
- the need to engage further with industry on possible regulatory alternatives: such as a set of guidelines to provide guidance for providers in the areas of procurement and network design; a process for Government-industry engagement where a high risk event is identified and a framework for periodic reporting to Government agencies on the security measures being taken by providers.[35]

## Data breach notifications

3.38 The Privacy Commissioner, within the Office of the Australian Information Commissioner (OAIC), raised the potential introduction of a compulsory data breach notification regime to supplement security arrangements:

> While notification of a data breach is currently not required by the Privacy Act, the OAIC suggests that it be considered as part of the proposed framework as an important mitigation strategy against privacy risks. It may also assist in promoting transparency and trust for C/CSPs.
>
> The OAIC suggests that the implementation of an effective mechanism for ensuring that industry has taken reasonable steps to mitigate security risks is essential and will assist in achieving the necessary levels of transparency and accountability. In the event that there is a complaint to the OAIC, access to any compliance assessments and audits of the Government under the proposed regime would assist the OAIC in its investigation of the matter.[36]

3.39 Similarly, the Australian Mobile Telecommunications Association and Communications Alliance, in their joint submission, contended that a cyber-attack reporting regime would be preferable to the penalty and remediation regime proposed in the discussion paper:

---

35 Australian Mobile Telecommunications Association and Communications Alliance, *Submission No. 114*, pp. 18-19.

36 Office of Australian Information Commissioner, *Submission No. 183*, p. 20.

> An alternative, and preferable, approach would be to require a reporting regime relating to cyber-attacks on Australian networks with noticeable operational impact by service providers as opposed to a system which enforces penalties on those providers. Where service providers can demonstrate implementation of reasonable minimum network security measures then imposition of a penalty based instrument would seem to be punishing those service providers who have taken steps to ensure, within their control, that a certain level of precaution has been exercised at a network level.[37]

3.40 Senetas, a private sector security consultant, was also of the view that the government make data breach notification mandatory for C/CSPs.[38]

## Free trade commitments

3.41 Australia's free trade commitments require any barriers to trade to be no more trade-restrictive than necessary to fulfil the legitimate objective of protecting national security. Huawei Australia cautioned that a legislative framework that targets particular vendors or vendors from particular countries could also raise concerns about free trade commitments:

> Under the General Agreement on Tariffs and Trade (GATT), World Trade Organisation (WTO) members are essentially required not to discriminate against imported products on the basis of their country of origin. If the Network Security Reforms result in discrimination against vendors on the basis of their country of origin, it is likely that this would place Australia in breach of its WTO obligations under the GATT.[39]

37 Australian Mobile Telecommunications Association and Communications Alliance, *Submission No. 114*, p. 19.

38 Senetas, *Submission No. 237*, p. 1.

39 Huawei Technologies (Australia) Pty Limited, *Submission No. 149*, p. 15.

## Committee comment

3.42 The Committee understands the rationale of the Telecommunications Sector Security Reform proposal and notes the warm, if cautious support, of most industry submitters.

3.43 There are threats to Australia's national security that can be effected through the telecommunications systems. The industry itself is best placed to deal with those threats, however, it cannot protect its systems and infrastructure of which it is ignorant or that it does not understand. As well, there is the problem of participants which ignore, or fail to take them sufficiently seriously. The relevant threat information is held by government. Where appropriate, there is therefore a need for Government to share threat information with industry in order for industry participants to make informed decisions about their procurements and outsourcing arrangements.

3.44 Conversely, it would not be possible for government and industry to have effective or guided discussions without industry providing essential background information to government with which it can assess threats. The greatest improvements to telecommunications sector security would come through dialogue – with both industry and Government exchanging useful, and sensitive, information.

3.45 The Committee is of the view that it will be necessary to encourage service providers to engage with Government and to accept the advice given to them. Although there are currently indirect incentives for service providers to protect their customers' information (such as public relations damage), commercial interests will not always align with the national interest.

3.46 To account for those instances were advice is not acted upon and where national security is threatened, the Committee agrees that Government should create a scheme including the capacity for Government to direct service providers to take certain remediation actions.

3.47 The Committee believes there cannot be an effective and equitable security regime without enforcement mechanisms.

### Interaction between data retention and telecommunications security

3.48 The Privacy Commissioner drew the Committee's attention to the need to consider telecommunications sector security reform for telecommunications data that is held under any potential data retention regime:

> The OAIC notes that ensuring that Australian telecommunications networks are protected by an effective security framework is particularly important given the proposals relating to data retention.[40]

3.49 The Committee agrees with the Privacy Commissioner that there is a clear need to secure information or data that is stored, given that there are already large volumes of telecommunications information held by telecommunications providers.

3.50 The Committee is, therefore, of the view that an infrastructure and information security regime should be introduced whether or not Government chooses to introduce a data retention regime.

## Regulatory impacts

3.51 As highlighted by the Australian Mobile Telecommunications Association and Communications Alliance, a Regulation Impact Statement should consider further issues that were not examined in detail in submissions or in evidence given at hearings to this inquiry. Such issues should include:

- the interaction of the proposed regime with other corporate regulations;
- the compatibility of the proposed regime with existing corporate governance where a provider's activities might be driven by decisions made outside of Australia;
- consideration of an indemnity to civil action for service providers who have acted in good faith under the requirements of the proposed framework; and
- impacts on competition in the market-place, including:
  - ⇒ the potential for proposed requirements may create a barrier to entry for lower cost providers;
  - ⇒ the possible elimination of existing lower cost providers from the market, resulting in decreased market competition on pricing; and
  - ⇒ any other relevant effects.

40 Mr Timothy Pilgrim, Privacy Commissioner, Office of the Australian Information Commissioner, S*ubmission No. 183*, p. 16.

### Recommendation 19

**The Committee recommends that the Government amend the *Telecommunications Act 1997* to create a telecommunications security framework that will provide:**

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

**The Committee further recommends that the Government, through a Regulation Impact Statement, address:**

- **the interaction of the proposed regime with existing legal obligations imposed upon corporations;**
- **the compatibility of the proposed regime with existing corporate governance where a provider's activities might be driven by decisions made outside of Australia;**
- **consideration of an indemnity to civil action for service providers who have acted in good faith under the requirements of the proposed framework; and**
- **impacts on competition in the market-place, including:**
  - ⇒ **the potential for proposed requirements to create a barrier to entry for lower cost providers;**
  - ⇒ **the possible elimination of existing lower cost providers from the market, resulting in decreased market competition on pricing; and**
  - ⇒ **any other relevant effects.**