

24 April 2008

Committee Secretary  
Senate Standing Committee on Environment,  
Communications  
and the Arts  
Department of the Senate  
PO Box 6100  
Parliament House  
Canberra ACT 2600  
Australia

Email: [eca.sen@aph.gov.au](mailto:eca.sen@aph.gov.au)

**Public Policy and  
Communications**

Executive Director Regulatory  
Affairs  
Unit 11, Level 2  
11 National Circuit  
BARTON ACT 2600

Telephone 02 6208 0740  
Facsimile 02 9261 8390

Dear Sir/Madam

**Inquiry into the Telecommunications Legislation Amendment  
(National Broadband Network) Bill 2008**

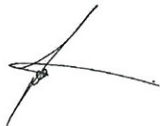
I attach a submission from Telstra in relation to this inquiry.

Telstra's contact officer for the submission is:

Mr Bill Gallagher  
General Counsel, Public Policy and Communications  
Ph: (02) 9298 5597  
Email: [bill.gallagher@team.telstra.com](mailto:bill.gallagher@team.telstra.com)

Telstra apologises for the delay in lodging the submission.

| Yours faithfully,



Tony Warren  
Executive Director Regulatory Affairs  
Public Policy and Communications

**SENATE STANDING COMMITTEE ON ENVIRONMENT, COMMUNICATIONS  
AND THE ARTS**

**INQUIRY INTO THE PROVISIONS OF THE TELECOMMUNICATIONS  
LEGISLATION AMENDMENT (NATIONAL BROADBAND NETWORK) BILL  
2008**

**SUBMISSION BY TELSTRA CORPORATION LIMITED**

**1 INTRODUCTION**

- 1.1 Since the proposal of requiring carriers to disclose their network information was first mooted, Telstra has been concerned about potential risks attending the proposal. What is involved here is information which has a highly sensitive character, from both a national security and a commercial point of view, and its disclosure and use must be tightly controlled.
- 1.2 It is important not to underestimate the national security implications of the disclosure of certain telecommunications network information. Persons - both within Australia and overseas - determined to damage the public health and safety of Australian people, institutions and communities, could potentially use certain telecommunications network information to precisely identify points of access to the network in an attempt to disable communications and security systems for sensitive installations, such as banks, government agencies, and traffic control systems.
- 1.3 In addition, unauthorised access to network information has the potential to harm the commercial interests of Telstra - and by extension its many shareholders, both institutional and individual - Telstra's customers, and the public welfare at large.
- 1.4 Telstra recognises the Government's desire that the National Broadband Network RFP tender process is transparent and accountable, and agrees that it should be conducted expeditiously.
- 1.5 However, a balance must be struck between, on the one hand, the Government's desire for administrative efficiency and participation in the tender process and, on the other, the significant national security and commercial risks outlined above. In Telstra's view, a number of amendments to the Bill will ensure that this appropriate balance is struck with the Bill. In particular, there is a need to provide adequate safeguards for the disclosure of carriers' network information and to provide sufficient incentives for proponents in the Government's National Broadband Network RFP process and their personnel to preserve the confidentiality of the information. There also needs to be sufficient specific controls on the manner in which the information may be dealt with.
- 1.6 Telstra's proposed amendments to the Bill are as follows:
  - (a) Telstra makes submissions to amend existing provisions of the Bill so as to introduce additional, essential safeguards for the protection of carriers' network information:

- (i) by regulating the uses to which information may be put, rather than merely the circumstances in which it may be disclosed (clauses 531G, 531K);
  - (ii) by expanding the compensation mechanism currently found in clause 531L and including a reporting regime to ensure that carriers can pursue compensation and preventative measures effectively;
  - (iii) by ensuring that the making of “restricted recipients rules” and other security and destruction rules is mandatory (and prescribing some part of their content) (clauses 531N, 531P).
- (b) Telstra makes submissions on other matters which create potentially significant risks for carriers, including:
- (i) clarifying that the information able to be requested (subclause 531C(1)) is the general location, type and dimensions of existing telecommunications networks and facilities;
  - (ii) clarifying the additional purposes for disclosure that may be prescribed by the regulations (paragraph 531G(2)(e)); and
  - (iii) clarifying the scope of other “conditions” which must be met in order for information to be disclosed (paragraph 531H(1)(d) and subclause 531H(4)).

Further detail on these amendments is set out below.

- 1.7 These proposals are nothing out of the ordinary for regimes regulating the handling of sensitive and confidential information. They draw upon existing analogous legislative regimes, commonly used commercial confidentiality arrangements, and widely accepted information security standards and protocols.<sup>1</sup>
- 1.8 Telstra has also been working constructively with the Government in relation to the Government’s original voluntary request for the provision of network information. Telstra has indicated its willingness to provide such information on a voluntary basis with necessary safeguards to protect against unauthorised disclosure and misuse of the information. Telstra’s preference is that this happen in a timely fashion with necessary safeguards such that the Government’s National Broadband Network RFP tender process proceeds as expeditiously as possible.

## **2 SCOPE OF INFORMATION TO BE DISCLOSED (CLAUSE 531C)**

- 2.1 Under clause 531C, the Minister is permitted to require “specified information” to be disclosed.

---

<sup>1</sup> For example, some of the specific security and destruction matters discussed in this submission are drawn from aspects of the Australian Government’s own *Information Communications and Technology Security Manual* (“ICTSM”), published by the Defence Signals Directorate.

- 2.2 This provision imposes no obvious limits on the types of information that could be required to be disclosed. Carriers could be required to disclose any information, not just about their existing network infrastructure, but sensitive commercial information that would be demonstrably unfair for competing carriers to know. Such a result would go far beyond what, on any sensible view, was necessary to enable participation in the tender process.
- 2.3 The Explanatory Memorandum indicates that the main concern motivating the need for information is that an “important element in efficiently deploying an FTTN network ... is likely to be the efficient *use of existing infrastructure, especially elements of Telstra’s fixed-line customer access network and elements of certain carriers’ optical fibre core networks*” (emphasis added). In addition to publicly available network information, “[a]dditional information that may be relevant could include the location of facilities between the local telephone exchange and the customer premises and the lengths of cables from the local exchange to the customer premises” as well as information “regarding optical fibre infrastructure in rural and regional Australia”.
- 2.4 The Explanatory Memorandum thus demonstrates a well-defined understanding of the type of information that needs to be made available. This being so, Telstra sees no reason why the power in clause 531C(1) should not be more closely drawn to serve its intended function.
- 2.5 Telstra therefore submits that the information able to be specified by the Minister under clause 531C be limited to information comprising the type, physical dimensions and general locality of existing telecommunications networks and facilities. This change would limit national security risks and result in considerably greater certainty for carriers, while imposing no unfair limitations on proponents or on the tender process.

### **3 RESTRICTION ON USE OF INFORMATION (CLAUSES 531G, 531K)**

- 3.1 Telstra submits that clauses 531G and 531K (headed “protection of information”) do not presently provide adequate “protection” for carriers’ information, because they fail to explicitly control the uses to which the information may be put.
- 3.2 Commercial confidentiality agreements typically regulate both use and disclosure of sensitive information. For example, in the “Proponent Confidentiality Deed Poll” (section 8 of Schedule 2 to the RFP); clause 2.1 provides that recipients must (a) “not use the Confidential Information for any purpose whatsoever except the Permitted Purpose” and (b) “keep confidential all Confidential Information (subject to disclosure permitted under [the deed poll])”.
- 3.3 Part 13 of the *Telecommunications Act 1997* - which, like clauses 531G and 531K of the Bill, deals with “Protection of communications” - makes a similar distinction. This Part imposes obligations of confidentiality on carriers, carriage service providers and their staff and contractors in relation to information about the supply of carriage services, and the content of communications over a carriage service. Part 13 recognises that these types of information can be highly sensitive.

The obligations it imposes relate not only to *disclosure* of that information, but also to its *use*.

- 3.4 The efficacy of the tender process does not require that both government and commercial parties have unrestricted flexibility in the uses to which they might put the protected carrier information. But the Bill presently enables this to happen.
- 3.5 Instead of following the well-established precedent of limiting the purposes for which information may be used *or* disclosed, the Bill is drafted so as to prohibit explicitly *only disclosure* of information other than for specified purposes. A person to whom information *has been disclosed* for a permitted purpose may then, apparently, use that information for any purpose they wish with only further *disclosure* in the course of that use having to be in accordance with the legislation.
- 3.6 There is no reason why there should not be restraints on misuse of carriers' network information. Rather, there are many clear reasons why there *should* be such restraints.
- 3.7 Furthermore, there is no reason why the Bill should not control the uses to which entrusted public officials may put the protected carrier information. Given the range and gravity of the risks identified earlier, there is no justification for providing boundless flexibility here. In any case, not all "entrusted public officials" are government policy officers; many, in the context of the National Broadband Network tender process, may be private sector consultants engaged to advise the Government on a commercial basis, whose roles - and legitimate uses of network information - are necessarily limited.
- 3.8 Telstra therefore submits that the Bill be amended so that the current restrictions on the disclosure by entrusted public officials and entrusted company officers of protected carrier information apply equally to the use of the information.

#### **4 POWER TO PRESCRIBE ADDITIONAL PURPOSES OF DISCLOSURE/USE OF INFORMATION (PARAGRAPH 531G(2)(e))**

- 4.1 Paragraph 531G(2)(e) allows protected carrier information potentially to be disclosed (and used) by the Government, or any of its agencies (including the ACCC) for a "purpose prescribed in the regulations".
- 4.2 This overbroad language would readily extend to a purpose completely unconnected with the request for proposals.
- 4.3 The limited 12 month time frame provided by subclause 531G(3) does not serve to reassure carriers. The undesirability of this position is compounded by there being no restriction on *use* of information - it is not clear if information disclosed for the purpose specified in the regulations could continued to be used for those purposes even *after* the 12 month period expires.
- 4.4 The Explanatory Memorandum notes that this paragraph was included for "flexibility". But the width of the "ancillary or incidental" limbs of the existing purposes connected with the RFP (see eg paragraphs 531G(2)(a)(iv), (2)(b)(iv),

(2)(c)(vii), (2)(d)(vii)) gives ample flexibility for the Government. Telstra does not see what additional benefit comes from the existing para 531G(2)(e) in this regard. Rather, it introduces unnecessary risk and uncertainty for disclosing carriers.

- 4.5 The Explanatory Memorandum also justifies the provision on the basis that it is necessary for the Broadband Fibre to Schools initiative. Given the considerable sensitivities of this Bill, Telstra submits that paragraph 531G(2)(e) should be clarified to limit it explicitly to purposes connected with the Broadband Fibre to Schools initiative - or other existing and specifically identified policy initiatives - or else deleted.

## **5 DISCLOSURES IN BID SUBMISSIONS (PARAGRAPH 531K(2)(b))**

- 5.1 Paragraph 531K(2)(b) currently permits an entrusted company officer to disclose protected carrier information in a bid submission in response to the RFP.
- 5.2 Submissions in response to the RFP may not necessarily be confidential documents. Paragraph 6.3.1 of the RFP simply permits proponents to identify in their bid submission any confidential information that they consider should be protected.
- 5.3 Telstra sees no reason why proponents should be able to designate their own information as confidential in a bid submission, but should not be required to treat protected carrier information as confidential when included in a bid submission. Given its sensitive subject-matter, there is no public interest in the protected carrier information being anything other than confidential in bid submission documents.
- 5.4 Therefore, Telstra submits that paragraph 531K(2)(b) should be narrowed so as to require any disclosure in a bid submission to preserve the confidentiality of the protected carrier information.

## **6 COMPENSATION AND ACCOUNTABILITY (CLAUSE 531L)**

- 6.1 The compensation mechanism provided for in clause 531L provides a measure of protection for disclosing carriers' interests in particular circumstances. However, Telstra submits that the provision as currently drafted is unduly limited in a number of significant ways, and consequently there is a significant lack of accountability for misuse of information under the Bill. Provision for compensation would ordinarily be a key deterrent against persons misusing confidential information. However, due to the limits of clause 531L, the deterrent here is lacking.

### *Recourse limited to a single "company"*

- 6.2 Under the current clause 531L, orders for compensation may only be made against *the company* of an entrusted company officer who has contravened section 531K(1). Companies involved in the tender process could be impecunious. FANOC Pty Ltd, the corporate vehicle used for the lodging of a Special Access Undertaking by the G9 consortium last year, is a case in point - that company appearing to have no significant assets. Hence it is conceivable that a "judgment-proof" company may be a vehicle for conduct which causes significant commercial detriment to

competing carriers, with the carrier having no effective right to compensation.<sup>2</sup> However, related bodies corporate, or bodies corporate or partnerships providing advisory or other services to the carrier, may not be so financially limited.

- 6.3 For that reason, carriers should have rights to pursue compensation against entrusted company officers who contravene the Bill as well as the proponent companies themselves. If the entrusted company officer is an employee, director or partner of a body corporate or partnership providing services to the company (or which is engaged as a consultant to a body politic providing services to the company), then the court should be empowered to make orders against the body corporate or partnership providing the services. This reflects normal vicarious liability principles and would represent a necessary enhancement of the accountability required by the Bill, ensuring that all companies and private persons dealing with protected carrier information have a direct deterrent against non-compliance with the restrictions on disclosure and use.
- 6.4 Furthermore, Telstra sees no reason why proceedings for compensation should not also be available against entrusted public officials who abuse their position to the detriment of carriers and their shareholders. In particular, as mentioned above, the definition of "entrusted public official" extends well beyond the traditional "official" in a government department, embracing private consultants engaged by government on a commercial basis.

*Proper standards of vicarious liability must be set for entrusted company officers*

- 6.5 Paragraph 531L(1)(d) should not be a necessary condition of compensation being available in respect of contraventions by entrusted company officers. The existence of that paragraph dramatically and inappropriately cuts down the deterrent against misuse of information.
- 6.6 This effect of the paragraph can be seen from its legislative precedents. Paragraph 531L(1)(d) is apparently drawn from section 12.3 of the Commonwealth *Criminal Code*. Subsection 12.3(1) states:

*"If intention, knowledge or recklessness is a fault element in relation to a physical element of an offence, that fault element must be attributed to a body corporate that expressly, tacitly or impliedly authorised or permitted the commission of the offence."*

- 6.7 It is inappropriate to take a provision designed to address attribution to a company of a subjective fault element of a criminal offence and import that provision into the context of a civil remedy - particularly a private right of action for compensation. A provision such as section 12.3 of the *Criminal Code* assumes that the criminal law's notions of subjective blameworthiness are applicable. It effectively holds the

---

<sup>2</sup> Paragraph 8.1.2 of the RFP provides that the bond submitted by proponents is to be security for any liability to the Commonwealth arising from breach of provisions of the Proponent Confidentiality Deed Poll (or the deed poll in schedule 1 to the RFP). Consequently, it provides no surety at all for disclosing carriers.

company to a criminal standard of *mens rea*<sup>3</sup> - even though the provision in the Bill does not require the individual entrusted company officer to have any particular mental state for a contravention of the Bill to occur.

- 6.8 This being so, clause 531L fails to set satisfactory standards of diligence for companies that would be in receipt of highly sensitive and potentially damaging information. Companies should have maximum incentive to take all possible measures to safeguard against disclosure by accident or by rogue “entrusted company officers”.
- 6.9 There is no reason why a court could not take account of any express, tacit or implicit authorisation or permission of a contravention when exercising its discretion to set an amount of compensation “that the Court considers appropriate”. But there are several good reasons set out above why that consideration should *not* be a precondition to a carrier having *any* right to compensation.
- 6.10 In view of these issues, the Bill acts against a carrier whose interests have suffered significant detriment, when the detriment arose out of a legal compulsion to disclose valuable information in the first place. Telstra therefore submits that paragraph 531L(1)(d) should be removed and replaced with a provision that attributes liability to a company where the conduct of the entrusted company officer resulting in a contravention of the Bill is undertaken within the actual or apparent scope of his or her employment or within his or her actual or apparent authority.
- 6.11 Telstra notes that the position it advocates above is consistent with the approach taken under the “Proponent Confidentiality Deed Poll” annexed to the RFP. That deed poll imposes an unqualified indemnity upon recipient companies for the conduct of their employees and officers (see clause 2.3(c) of the deed poll).

#### *Need for preventative injunctions*

- 6.12 Thirdly, Telstra submits that the compensation mechanism should be extended to permit the Court to grant orders in the nature of injunctions. In this context, prevention may be a more cogent remedy than compensation. If any evidence comes to light that a company or its entrusted company officer may be about to contravene section 531K (see proposed amendments below for a reporting regime), a carrier should be entitled to seek orders preventing this potentially destructive event from occurring.
- 6.13 Section 564 of the Telecommunications Act would ordinarily apply to a breach or apprehended breach of sections 531K and 531G. However, carriers should not be forced to rely upon the Government’s decision to institute or not institute proceedings. The Government does not share the interests of carriers in relation to the commercial value of network information. But there would be no reason why it would be contrary to the Government’s interests for carriers to seek to protect those interests, when it comes to an unauthorised disclosure. In that respect, carriers

---

<sup>3</sup> So, for instance, subsection 12.3(2) of the Criminal Code refers to this standard being satisfied by evidence such as the state of mind of members of the company’s board of directors, or of a “high managerial agent”, or the existence of a corporate culture conducive to the contravention.



should be free to make the decision for themselves, and to prevent damage to their interests whenever the carrier considers it necessary to do so.

- 6.14 Consequently, it is necessary for carriers to have a direct right to seek an injunction under section 564.

#### *Reporting regime*

- 6.15 To support these accountability mechanisms, Telstra further submits that a reporting regime should be instituted. The authorised information officer should be obliged to inform the disclosing carrier of the identity of all entrusted company officers. The disclosing carrier must keep these details confidential and only use them for the purpose of exercising its rights under the Bill.
- 6.16 Proponent companies should be required to notify an authorised information officer on a regular basis of details as to the identity of all entrusted company officers to whom protected information has been disclosed. These details should then be made available to a carrier, but strictly for the purposes of determining whether to institute proceedings for compensation or an injunction. To allay any concerns about the uses to which carriers might put information about the identity of recipients, the Bill should require the carrier to implement “Chinese wall” internal confidentiality arrangements to prohibiting the disclosure of the information to employees responsible for conducting the tender process.
- 6.17 Furthermore, entrusted company officers should be required to notify an authorised information officer immediately upon becoming aware of any actual or imminent contravention of section 531K. The authorised information officer then should be required to provide to such a carrier sufficient details of any actual or imminent contravention to enable the carrier to institute proceedings for an injunction or for compensation.
- 6.18 To ensure the efficacy of this regime within the company in question, it would be useful for the company to nominate a particular entrusted company officer for the purposes of receiving all such information within the company and passing it to the authorised information officer. In this respect, the reporting system would be underpinned by the amendments proposed below in connection with the storage, handling and destruction rules to be made under clause 531P - specifically, that those rules should include provision for the company to establish systems for tracking possession of and access to the protected carrier information.
- 6.19 This regime should also be imposed in relation to entrusted public officials.

### **7 RESTRICTED RECIPIENTS RULES (CLAUSE 531N)**

#### *Rules should be mandatory and robust*

- 7.1 The making of the restricted recipient rules is currently entirely discretionary under the Bill. There may be no restrictions whatsoever on who may be in possession of commercially and security sensitive network information, beyond the requirement

that they be entrusted company officers. The class of persons who can be entrusted company officers is very wide.

- 7.2 The purpose of the restricted recipients rules is to restrict this wide class to persons having some connection with the request for proposals, as the wider the range of persons able to access the information, the greater the risk of misuse and consequent damage from both a national security and commercial perspective. Given that purpose, Telstra considers that the restricted recipients rules should be both mandatory and robust.
- 7.3 Telstra submits that clause 531N(1) should be amended to require that:
- (a) within a specified time of the commencement of Part 27A and prior to making any instrument under section 531C, the Minister *must* make restricted recipients rules; and
  - (b) the restricted recipients rules *must* provide for specified conditions to be satisfied by persons prior to information being disclosed to them, including at least that:
    - (i) their duties must be directly relevant to the authorised purposes described in paragraphs 531H(1)(g)-(j);
    - (ii) they must have a need to know the particular information for the purposes of performing those duties.
- 7.4 Telstra further submits that, in order to provide some measure of procedural fairness, it would be desirable for the Minister to provide a draft of the restricted recipients rules to affected carriers before the rules are made, and to consider the carriers' views. This would bring the rules into line with the instruments to be made under clause 531C.

*An "expert only" category of information*

- 7.5 Further, Telstra submits that the restricted recipients rules should allow for particular categories of information to be available only to external consultants to a tendering company. This would be an additional security measure to prevent carriers' competitors from using network information for commercial purposes unrelated to the National Broadband Network tender process. This would be broadly consistent with the practice sometimes adopted in relation to confidentiality undertakings for access to Telstra's confidential information in arbitration proceedings before the ACCC. It would also be consistent with the way in which courts deal with confidential information in sensitive proceedings. These types of arrangement are also commonplace and familiar in the commercial world.
- 7.6 What particular information, or types of information, fall into this "expert only" category would ultimately be determined by the Minister, taking into account the views of the carrier (expressed when the Minister provides the carrier with a draft instrument under clause 531C).

### *Application to entrusted public officials*

- 7.7 Finally, Telstra submits that the restricted recipients rules should apply to entrusted public officials as well as to entrusted company officers. Much the same risks attend the holding of protected carrier information by public officials as by companies. Valuable proprietary information could be used for unrelated purposes or disclosed in contravention of the provisions of the Bill. It is at least as valuable to minimise the risk of this harm arising as it is to provide for criminal penalties for unauthorised disclosure. One good way to minimise risk is to limit the classes of person - including APS employees as well as external consultants - who can have access to the protected carrier information. The relevance of a person's duties to the RFP processes, as well as the "need to know" principle, are equally applicable to public officials as to company officers.

## **8 SECURITY AND DESTRUCTION REQUIREMENTS (CLAUSE 531P)**

- 8.1 To date there is little clarity about what these requirements are likely to entail, but their details are of vital importance to carriers. Security requirements are critical to the effectiveness of the confidentiality arrangements contemplated by the Bill. They are critical to minimising the very significant risks posed by the dissemination of telecommunications network information - risks to which each of the Government and proponents, and their respective personnel, must be alert. Considering the potential gravity of the situation, there is a need for specific guidance on the type of safeguards that will be in place.
- 8.2 As with clause 531N(1), clause 531P(1) provides that the Minister *may* make rules relating to storage, handling or destruction of protected carrier information. For the same reasons as already discussed in relation to clause 531N, Telstra submits that clause 531P(1) should be amended to require that the Minister *must*, within a specified time and before issuing any instrument under clause 531C, make rules relating to storage, handling *and* destruction of protected carrier information.
- 8.3 The following features of the rules should apply equally to both entrusted public officials and entrusted company officers and be expressly set out in the Bill.

### *Destruction mandatory*

- 8.4 Most importantly, persons (whether entrusted public officials or entrusted company officers) to whom information has been disclosed must destroy or delete the information as soon as practicable after it is no longer required by them for the purpose for which it was disclosed to them. The longer the information is retained - *including* where it lies idle in recipients' records - the greater the risk of unauthorised disclosure or misuse. Upon destroying information as required by the rules, a person should be required to provide a certificate of destruction to an authorised information officer.

### *Key security matters to be covered*

- 8.5 In addition, more generally, there is a need for further guidance from Parliament as to the subject-matter which must be covered by the rules to be made by the Minister

under clause 531P. Telstra submits that the Bill should require the rules to provide for the establishment and maintenance of appropriate systems and processes in relation to the following key security topics:

- Physical security measures including secured areas and access logs;
- Software and network security measures including email security, anti-virus measures, firewalls and cryptography;
- Access control and active security measures including user identification and authentication, intrusion detection and access logging;
- Hardware and media destruction/sanitisation procedures;
- Security compliance review and incident detection and management;
- Personnel security measures including training programs and security clearances.

8.6 These topics are drawn from the public version of the Government's own *Information Communications and Technology Security Manual*. That manual contains a wide range of further and more specific requirements which represent world's best practice in relation to the handling of highly sensitive information.

8.7 Telstra does not suggest that the all possible security measures should be prescribed *in the Bill*, or that specific processes or practices should be mandated. But an assurance that at least these core security areas will be addressed in the rules, to some extent, would be a considerable advance. The Minister would retain flexibility to further developing the detail of the systems and processes to be implemented through the rules.

8.8 Finally, as with clause 531N, Telstra submits that clause 531P should require the Minister to provide a draft of the rules to affected carriers before the rules are made, and to consider the carriers' views.

## **9 ADDITIONAL PRE-CONDITIONS TO DISCLOSURE**

9.1 Subclause 531H(1)(d) of the Bill empowers the Minister to make an instrument determining conditions that must be met before disclosure to a company is permitted. The intended scope and nature of these conditions is not clear. The Explanatory Memorandum provides no guidance. It is not mandatory for the Minister to make any such conditions.

### *Ongoing conditions as well as pre-conditions*

9.2 On its present drafting, paragraph 531H(1)(d) contemplates only conditions to be satisfied *at the time of the decision* to grant access to information. What happens if one of these conditions relates to a circumstance that would (or should) continue to apply during the time the entrusted company officer holds the protected carrier information, but at some later stage it ceases to be satisfied? The Bill should be

amended to provide for ongoing conditions to be imposed and to require withdrawal of information and penalties for breach of conditions of disclosure.

*Favourable security assessment to be mandatory*

- 9.3 One condition that should be made mandatory under the Bill is that an authorised information officer should be required to receive some form of favourable security assessment from an officer of ASIO or the Attorney-General's Department prior to making a decision to disclose.

*Security systems to be in place*

- 9.4 In addition, before information is disclosed to an entrusted company officer, the officer's company should have to satisfy the authorised information officer that it has established the systems and processes required under each of the proposed new notification and reporting regime, the restricted recipients rules and the storage handling and destruction rules to be made under clause 531P. This ensures that the recipients of information will have taken active measures to provide an environment conducive to compliance with the Bill's restrictions on use and disclosure.

## **10 CONCLUSION**

- 10.1 The Bill requires a number of amendments to ensure that it strikes an appropriate balance between administrative efficiency and participation in the tender, on the one hand, and the public interest in minimising national security risks and the commercial interests of carriers and their shareholders on the other. Telstra submits that the proposals described above strike the balance required. These proposals reflect accepted, familiar and well-understood aspects of confidentiality schemes in existing legislation, administrative practice and commercial arrangements. They are reasonable and practical ways to enhance the Bill and better promote the achievement of its objectives.

Telstra Corporation Limited  
24 April 2008