Submission No 189

Inquiry into potential reforms of National Security Legislation

Organisation: Telstra
George Street Sydney
NSW 2000 Australia

PJCIS INQUIRY ON REFORMS TO NATIONAL SECURITY LEGISLATION

SUBMISSION BY TELSTRA

IT'S HOW WE CONNECT

Contents

A. Introduction 3

B. Executive Summary 3

C. Telecommunications (Interception and Access) Act 1979 5

1. Strengthening the safeguards and privacy protections under the lawful access to communications regime in the TIA Act 5

2. Reforming the lawful access to communications regime 6

3. Streamlining and reducing complexity in the lawful access to communications regime 6

4. Modernising the TIA Act's cost sharing framework 7

8. Streamlining and reducing complexity in the lawful access to communications regime 8

9. Modernizing the industry assistance framework 8

14. Reforming the Lawful Access Regime 9

15. Modernising the industry assistance framework 10

D. Telecommunications Act 1997 12

16. Amending the Telecommunications Act to address security and resilience risks posed to the telecommunications sector 12

E. Australian Security Intelligence Organisation Act 1979 13

5. Amending the ASIO Act to modernise and streamline ASIO's warrant provisions 13

11. Amending the ASIO Act to modernise and streamline ASIO's warrant provisions to 14

12. Clarifying ASIO's ability to cooperate with the private sector 14

17. Amending the ASIO Act to modernise and streamline ASIO's warrant provisions by 15

ATTACHMENT 1 **16**

Note: Submission Sub-section numbers correspond to Terms of Reference numbering.

A. Introduction

Telstra welcomes the opportunity to respond to the PJCIS inquiry into potential reforms of national security legislation. We are a major builder and supplier of telecommunications networks and services with a large customer base and a long history of providing lawful assistance to security and law enforcement agencies. We are keen to share our insights on the issues and proposals contained within the PJCIS inquiry's Terms of Reference and Discussion Paper.

The proposed changes will require that a framework be established that balances our important obligations to protect the privacy of our customers against the equally important need to provide cost effective support to national security and law enforcement requirements in a timely, effective and sustainable way. Detailed consultation and thorough consideration is required before any changes are made.

B. Executive Summary

Telstra recognises the need to ensure that regulation remains relevant and appropriate to support critical national security and law enforcement requirements in a rapidly changing social and technological environment. However, consistent with the Government's Principles of Best Practice Regulation, in addition to identifying specific national security and law enforcement needs the proposed reforms should also be thoroughly evaluated against alternative reform options to ensure the proposals with greatest net benefits are adopted.

All reform proposals in this area will need to balance the public interest objectives, implementation costs to industry and ultimately customers, the need to maintain high levels of network integrity and legitimate community concerns about the security and privacy of customer information. In this context, public interest must be broadly defined and ensure that protection measures do not have the effect of impeding the delivery of high quality and innovative services to customers on Telstra's networks.

Consistent with best practice policy-making, Telstra understands that the Government's approach to the issues raised in the Discussion Paper will be principles-based and seek to strike an appropriate balance between several legitimate, but at times opposing, principles. In Telstra's view, the key principles are:

- Reforms must support critical, identified and specific national security and law enforcement requirements in a rapidly changing social and technological environment;
- The public interest benefits of the reforms must outweigh their cost to government, industry and consumers;
- Reforms must be framed in ways that promote transparency and raise public awareness levels regarding why specific, identified requirements are sought/necessary;
- The highest possible levels of protection for the privacy and security of customer communications, personal information and data should be provided, with transparency as to the circumstances in which such information may be accessed and used for public interest purposes;
- The allocation of financial costs, and operational, legal and reputational risks associated with implementing such reforms as between Government, its LENSAs (Law Enforcement and National Security Agencies), C/CSPs (carriers/carriage service providers), customers and the community more broadly should be allocated to the entities that benefit from them;
- The way changes are implemented should be competitively neutral and applied equally to all service providers to avoid distorting market outcomes and to reduce the opportunity for users to evade the intended outcomes of the changes;
- There must be recognition of the high levels of C/CSP and consumer reliance on communication networks and applications and minimise any impacts on or risks to network access, capacity and innovation;
- Seek to adopt relevant examples of best international practice in law enforcement and national security including from C/CSPs, from LENSAs and on policy/legislative reform;

- Reforms that place new and amended obligations on C/CSPs must be clear and unambiguous so that C/CSPs and their staff do not face any legal risks from complying with these obligations;
- The role of industry under lawful interception legislation should remain strictly limited to providing access to the intercepted material, and not extend to investing capital in capability to process or interpret data or requiring C/CSP personnel to undertake these tasks. Processing interception data is the role of the LENSAs. Telstra does not have the capability to process or interpret interception data. To place C/CSPs in the role of interpreting intelligence data potentially jeopardises the integrity of the intercepted data and creates a real risk that it opens up agencies to further legal challenges from a defendant in a criminal prosecution;
- It is important for the Committee to understand that, were they to be implemented, many of the proposals in the Discussion Paper would entail the imposition of new or additional costs on C/CSPs. Ultimately, the committee should recognise that the greater the implementation and administration costs that are imposed on C/CSPs under these proposals, the greater the likelihood that these costs will be passed onto consumers in the form of higher bills for telecommunications services; and
- To effectively implement these principles Telstra suggests that the Government partner with industry and relevant consumer interest groups in determining the most appropriate and effective ways of addressing these critical public interests. This collaborative approach will provide the appropriate levels of expertise to develop options and test alternate approaches before final decisions are taken, and will assist in building a broader recognition of drivers for change and support for solutions.

Committee members are encouraged to read Telstra's submission through the prism of these principles.

There are many issues canvassed in the Discussion Paper, but our submission is focused on the following issues:

- **Telecommunications interception reform** – Telstra welcomes proposals to streamline processes, but is concerned to ensure that allocation of new responsibilities and associated costs and risks accords with the above principles.
- **Data retention** – Telstra appreciates the objectives but would like to discuss more cost effective options to address the issues raised, consistent with the principles we have articulated above.

- **Telecommunication sector security reform** – Telstra supports measures to ensure that C/CSPs have appropriate incentives to focus resources on network security and believes this can be achieved through the modification of some of the proposed measures to avoid adverse impacts on our ability to undertake efficient procurement and network design and operations.

Attachment 1 of our submission is a summary table where we have brought together responses, where appropriate, on all issues canvassed in the terms of reference.

Below are our detailed responses. Our submission addresses each of the proposals grouped under a particular Act, in the following order:

- *Telecommunications (Interception and Access) Act 1979*
- *Telecommunications Act 1997*
- *Australian Security Intelligence Organisation Act 1979*

Telstra has not provided comment on any of the proposals canvassed for the *Intelligence Services Act 2001.*

C. Telecommunications (Interception and Access) Act 1979

1. Strengthening the safeguards and privacy protections under the lawful access to communications regime in the TIA Act

a. The legislation's privacy protection objective

Telstra supports the proposal to strengthen the safeguards and privacy protections under the lawful access to communications regime in the TIA Act (*Telecommunications (Interception and Access) Act 1979*) to ensure the protection and privacy of a customer's communications. Telstra also supports the need for consistency and alignment between the TIA Act and the Telco Act (*Telecommunications Act 1997*) for lawful interception, stored communications and any other customer data or information requested by Government.

Aligning the powers of both the Telco Act and TIA Act will assist in avoiding situations where C/CSPs are caught between legal obligations to protect customer information under the Telco Act (Part 13) and the legal obligations to provide assistance to LENSAs under the TIA Act. We recommend a simplification of those parts of the two Acts that compel C/CSPs to provide assistance to LENSAs in the public interest, while ensuring that approval thresholds for access are high enough to protect every consumer's right to privacy.

Any reforms should promote transparency and raise public awareness levels of how and why such information may be accessed and used for public interest purposes.

b. The proportionality tests for issuing of warrants

The proportionality testing of warrants will need to be consistent, practical and understandable by those required to implement them. Telstra remains concerned that ambiguity between the roles of agencies and requirements for C/CSPs to complete added steps will add unnecessary and avoidable complexity. There is a real need for these types of proposals to be further evaluated.

The scope of some of the proposed changes to lawful warrants will blur the boundaries between the part of the interception process traditionally conducted by the C/CSPs and that carried out by the LENSAs. This will require a review of the proportionality tests for the existing warrant authorisation and evidentiary certificate regime (and a review of costs arrangements) as well as for any new types of warrants, particularly where C/CSPs may no longer simply be enabling a lawfully issued interception warrant. The new types of warrants that have been proposed in the Discussion Paper may require C/CSPs to undertake processing which could be construed to be a form of interception if the C/CSP is required to record or store the material at some stage of the interception process (for example, in case of decryption).

c. Mandatory record-keeping standards

Telstra understands the desire for a reporting and record-keeping regime, but believes that the potential benefits of such proposals must explicitly and rigorously be evaluated against the costs associated with the implementation. The reporting regime needs to be simple and demonstrate to the public that the intended safeguards and privacy protections are working. At the same time the regime must not be administratively burdensome for both C/CSPs and LENSAs. Although the current record-keeping requirements are not overly onerous on C/CSPs, the regime does need an overhaul to achieve the intended outcomes. The existing obligation could be made more relevant to both LENSAs and C/CSPs, e.g. it is very difficult for a C/CSP to predict what products and services it will launch in 2-5 years' time and whether or not those services will have an impact on the C/CSP's legal interception capability.

d. Oversight arrangements by the Commonwealth and State Ombudsmen

Telstra agrees that there must be consistent and practical arrangements put in place to enable oversight by both Commonwealth and State Ombudsmen aimed at strengthening the safeguards and privacy protections under the TIA Act and the Telco Act to ensure the security and privacy of customer communications.

2. Reforming the lawful access to communications regime

a. Reducing the number of agencies eligible to access communications information

In principle Telstra supports this proposal, acknowledging the levels of rich communications data now available and likely to be the subject of a broader number of LENSA requests in the future.

Telstra believes there is some merit in adopting a two-tiered communications data access regime to address potential risks of allowing access to customer data for the investigation of lesser offences. Under this type of regime, data readily available through C/CSP customer information systems could be provided under the current threshold test and would potentially remain accessible to a larger number of enforcement agencies and LENSAs.

Under this construct, access to more intrusive communications data, e.g. URLs, IP addresses or 'created' tailored data sets proposed under the data retention regime, would only be provided to a limited number of LENSAs and would require higher approval thresholds to be satisfied.

b. The standardization of warrant tests and thresholds

Telstra supports the proposed changes to further limit the number of LENSAs able to request access to communications data given the increased richness of telecommunications information, and the potential for a wide range of non-criminal LENSAs to access to such information. Telstra does not believe the public interest requires the disclosure of personal information to non-criminal LENSAs such as bodies that can impose a pecuniary penalty.

Currently, non criminal LENSAs can access historical data (that is, existing information or documents in the enforcement of a law imposing a pecuniary penalty or protection of public revenue) under section 179 of the TIA Act. In contrast the approval threshold to access *prospective* call data imposes an effective limitation – it may only be authorised by a criminal law-enforcement agency when it is considered reasonably necessary for the investigation of an offence that is punishable by imprisonment for at least three years.

3. Streamlining and reducing complexity in the lawful access to communications regime

a. Simplifying the information sharing provisions that allow agencies to cooperate

Telstra would need to understand how this might work in practice and what, if any, legal and reputational implications might arise under such arrangements before we could express a view on this proposal. For example, if Telstra releases communications data or interception content to one agency under a lawful warrant and then that information is provided by the approved LENSA to one or more other LENSAs (who in turn rely upon the data in evidentiary proceedings), what appropriate processes would need to be established to address the continuity of evidence issues?

b. Removing legislative duplication

Telstra supports the removal of duplication and ambiguity between what C/CSPs are obliged to provide under the TIA Act and what LENSAs expect C/CSPs to provide under Section 313 of the Telco Act (i.e. "*reasonably necessary assistance*"). Section 313 enables LENSAs to request C/CSPs to provide a wide variety of assistance on the production of a lawful request but at present there is no clear delineation between what information must be provided under the TIA Act and what can be provided under Section 313.

4. Modernising the TIA Act's cost sharing framework

a. Aligning industry interception assistance with industry regulatory policy

At present a C/CSP's role in the 'lawful request' process is solely to deliver telecommunications data in compliance with a coercive instrument.

The capital "*cost of developing, installing and maintaining interception capability"* is borne by C/CSPs. C/CSPs are currently entitled to recover costs from LENSAs on a 'no cost - no profit' basis. In practice this means that C/CSPs are investing their shareholders' capital for sub-economic returns, and may not necessarily even recover their full operational costs in complying with existing legislation from the beneficiaries of these arrangements (i.e. national security and law enforcement agencies).

In attempting to assess the financial impact and requirements of future compliance, Telstra submits there is currently much ambiguity around the structure and likely costs associated with these proposals (e.g. initial system build and ongoing maintenance costs and how they will be addressed).

Under current arrangements, almost all of the retained data C/CSPs currently provides to LENSAs has to be 'mined' via manual interrogation of operational and business support systems as opposed to simply electronically accessing telecommunications data from our networks. Any new security related measures which impose additional costs on C/CSPs beyond those absolutely necessary to achieve the legitimate requirements for maintaining security must be subject to a cost benefit.

Telstra submits that C/CSPs should be able to recover their economic costs of developing, installing and maintaining an interception and delivery capability. The imposition of an economic cost recovery model will also mean that LENSAs will need to demonstrate a level of rigor in their application for lawful assistance from C/CSPs.

b. Clarifying the ACMA's regulatory and enforcement role

The ACMA's current role would appear to have diminished over time and particularly so after the Blunn Review when parts of the Telco Act were transferred to the TIA Act. Telstra believes there needs to be clarification as to what role ACMA will have in future in monitoring compliance by C/CSPs with the Telco Act and TIA Act in respect to national security and law enforcement.

The Discussion Paper does not suggest what types of additional powers may be contemplated. Telstra would recommend that whatever agency is given this enforcement role its primary focus should be on undertaking an active role in education and dispute resolution, with any penalty enforcement role being secondary.

8 Streamlining and reducing complexity in the lawful access to communications regime

a. Creating a single warrant with multiple TI powers

Telstra supports simplifying the warrant regime. This could be achieved by introducing a single and more precisely targeted warrant that provides unambiguous direction to C/CSP staff required to assist.

The proposed reforms that define attributes or 'non-traditional' service identifiers for warrants in a manner that focuses on characteristics of communication would represent a substantial shift of interception technology complexity and cost of interception from Government to C/CSPs. Implementation of such a change will require careful consideration to avoid unintended consequences particularly where services may be carried by a C/CSP, but are not managed or operated by the C/CSP, e.g. OTT (Over the Top) applications and services (Whatsapp and Skype), where a C/CSP may not be able to guarantee reliable interception or provide a carrier evidentiary certificate given the uncertainty regarding how the communications may be identified or carried within the C/CSP's network.

The ability to identify communications by attributes rather than services or technologies would require sophisticated equipment that, due to the size and diversified nature of C/CSP networks, may need to be installed at various locations through a C/CSP's networks. The economic cost for this capability cannot be determined without more detail. However based on experience it is reasonable to assume that the total cost will be substantial.

If the creation of a single warrant puts C/CSPs in a position of having to interpret warrants based on vague or incomplete details or attributes of the person of interest, the type of data or the services subscribed to by the person of interest to a LENSA, Telstra would not be able to support this proposal. The proposal for a single (all encompassing) type of warrant will also impact on a C/CSP's warrant management systems and introduce complexity in processes for delivering the required sets of data.

For these reasons single warrants will need to continue to include details of the specific attributes and services required to be intercepted or the type data being requested and not be open to misinterpretation by C/CSP employees. C/CSPs should continue to have the right (and the legal protection) to reject a request from a LENSA that has not met the specific pre-requisites.

The introduction of a single and more precisely targeted warrant may also require the introduction of a secure electronic warrant system to ensure the efficiencies of a single warrant system are delivered. Electronic warrants would benefit both LENSAs and C/CSPs in providing a streamlined system for serving, receiving, filing and managing warrants. A secure electronic warrant system that is used by all LENSAS and C/CSPs may also assist in reducing costs and response times for lawful requests as well as standardising the information in single warrants which would potentially reduce the incidence of vague, incomplete, or ambiguous directions on a warrant.

9. Modernizing the industry assistance framework

a. Implement detailed requirements for industry interception obligations

Telstra believes the proposed model of tiered participation based on participant status creates the potential for criminals and terrorists to bypass interception arrangements through the selection of their C/CSP. In relation to the new security compliance framework that the Discussion Paper suggests in relation to C/CSPs considered to be a higher security risk, it is not clear how LENSAs would make a determination on how compliance assessments and audits could apply. The proposal also raises questions about whether a C/CSP with larger market share might be considered to be higher risk simply because it carries more traffic.

In this regard Telstra is concerned that the Discussion Paper suggests the "level of engagement" would be informed by factors such as market share and customer base, meaning larger operators are likely to receive more scrutiny. Telstra maintains that market share and size of customer base is not an appropriate base on which to assess a company as being of 'higher risk'. A regulatory regime that clearly signals that small providers will have no interception capabilities invites criminals and terrorists to use such small C/CSPs. A more effective regime would be to focus the supply of interception capabilities on mass market and access services where interception is most likely to be utilised and be more effective.

b. Extend the regulatory regime to ancillary service providers not currently covered by the legislation

Telstra believes further work would need to be undertaken in this regard and final proposals would need to be able to demonstrate a practical, fair and reasonable approach on C/CSP compliance.

This proposal indicates that interception-type obligations could be extended beyond Australian based C/CSPs to cover website/application and overseas based providers, such as social media operators, webmail services and cloud computing providers. An ancillary effect of this extension to Australian C/CSPs would be that any products that the C/CSP was offering that covered these types of services such as webmail or OTT applications (Whatsapp, Viber and TU ME) and which have not previously been subject to lawful interception obligations other than for the carriage element would also be caught. In some cases local C/CSPs may not be aware of what services are being used by customers, i.e. VoIP services such as Skype.

c. Implement a three-tiered industry participation model

Telstra believes these proposals run the risk of creating an uneven playing field, where the compliance burden would rest disproportionately with larger C/CSPs and the effectiveness of the overall regime is undermined by allowing criminals or terrorists to avoid interception arrangements by acquiring services from smaller C/CSPs.

In relation to the interception cost sharing framework, the Discussion Paper indicates that a new tiered model may be introduced where larger C/CSPs are expected to have a comprehensive interception capability (presumably at a greater cost) while smaller C/CSPs may only be required to have a minimum level capability (presumably at a lower cost). While the Discussion Paper states that one of its aims is to maintain "competitive neutrality" in the industry, it is hard to see how tiered compliance obligations are consistent with this aim. As such, Telstra does not support this proposal.

This tiered approach would also create the perverse outcome in which criminals or terrorists actively avoided using a Tier 1 C/CSP's services in favour of Tier 3 C/CSP that are not required to comply with the new legislation/regulation.

14. Reforming the Lawful Access Regime

a. Expanding the basis of interception activities

If the intent of this proposal is intended to be consistent with that outlined under 9b, namely "*to extend the regulatory regime to ancillary service providers not currently covered by the legislation*", Telstra would require further information before it could understand how this might work in practice. Telstra would support an expansion, assuming that the proposed changes are implemented in a competitively neutral manner and applied equally to all service providers to avoid distorting market outcomes and to reduce the opportunity for criminals to evade the intended outcomes of the changes.

15. Modernising the industry assistance framework

a. Establish an offence for failure to assist in the decryption of communications

It is Telstra's position that the level of assistance that can reasonably be expected to be provided by C/CSPs should be carefully defined and limited in any event, but all the more so if an offence of failure to assist is to be created. For example, Telstra believes it would be unreasonable for a C/CSP to be required to:

- Decrypt services where the CSP is merely on-selling relevant services for a particular vendor (ie Blackberry). In this context, it would be reasonable for Government to obtain encryption keys from the relevant vendor of that product;
- Weaken or dilute or interfere with the encryption on a communications service in a way that would affect customers other than the authorised interception target;
- Weaken or dilute or interfere with the encryption on a communications service in a way that would affect the reputation or perception of the value of a third-party product (for example, leading to a belief that a CSP or vendor product is less secure than a competitor's product);
- Increase the risk that privacy of other customers will be compromised; or
- Conduct extensive storage and processing of communications to facilitate post-processing or decryption of communications prior to delivery to an agency. As previously stated in this submission, C/CSPs should not be expected to interpret or reconstruct the contents of a communication.

Some of the proposed changes reflect a shift of the interception burden from LENSAs to C/CSPs. As well as developing the capability to enable interception, C/CSPs would also be required to partially process intercepts before delivery to LENSAs to create communications data and also to assist in decryption. The changed process will mean that the enhanced and more intrusive interception role and actions of a C/CSP would be subject to greater scrutiny and may be more likely to be challenged in evidentiary proceedings. Telstra does not support any proposed change to legislation where the interception burden on C/CSPs becomes one of 'processing' or 'creating' communications data.

b. Institute industry response timelines

Telstra submits that for Government to mandate 'response timelines' would also require Government to spend significant funds to support the introduction of a fully automated request management system (as discussed in 8a) for use by LENSAs and C/CSPs otherwise the LENSAs would not obtain the benefits intended from this proposal.

C/CSPs invest in communications networks and systems which are optimised for the efficient carriage of communications products and services between geographic locations. The OSS (Operations Support Systems) and BSS (Business Support Systems) systems that are used by C/CSPs to operate and manage these networks and systems generate information (i.e. customer information and billing records) which is valuable to Government in serving the public interest and maintaining customer privacy.

The proposal to introduce response times into the delivery of customer data and intercepted material introduces a level of complexity perhaps not fully considered, in that almost all of the retained data C/CSPs currently provide to LENSAs has to be 'mined' via manual interrogation of BSS and OSS systems as opposed to simply accessing telecommunications data from C/CSP networks and systems using standard on–line access tools.

Before response timelines could be introduced, LENSAs would need to be provided with enhanced capability (i.e. an automated streamlined electronic system) for serving, receiving, filing and managing warrants and the receipt of intercepted material and communications data. The current electronic delivery system (SedNode) requires manual intervention to enable processing of communications data by C/CSPs.

c. Tailored data retention periods for up to 2 years for parts of a data set, with specific timeframes taking into account agency priorities, and privacy and cost impacts

The proposed arrangements are likely to be very costly and raise substantial security and privacy questions that will need to be answered.

Scope of data to be retained

Capturing meta data created by C/CSPs' communications systems and having to catalogue, store, retrieve and make available such information for possible use by LENSAs for up to two years (including data that passes through a C/CSP's network) raises a wide range of issues that we believe require detailed consultation and thorough consideration before any changes are made.

Telstra believes the proposed changes to retain a larger amount of telecommunications data will blur the boundaries between the interception process traditionally conducted by the C/CSPs and that carried out by the LENSAs.

In Telstra's view, to comply with any data retention regime we may need to routinely intercept and process large volumes of non-target customer communications to inspect, identify, and extract the required communications data from within the communications stream. C/CSPs, and nominated C/CSP personnel, would then need to be approved, similar to the agency interception authorities, to carry out this 'bulk' interception and communications processing. Presumably this would also require the introduction of a new compliance regime where C/CSPs may need to be subject to similar oversight and reporting obligations to the intercepting LENSAs.

The changed process will mean that the enhanced and more intrusive interception role and actions of a C/CSP would be subject to greater scrutiny and may be more likely to be challenged in evidentiary proceedings. It is Telstra's view that the expansion of interception related activities to C/CSP staff would not be appropriate.

Challenges of retaining large data sets

Telstra believes that an effective and fair data retention regime must recognise there is an increased risk to privacy that C/CSPs will need to manage, and the regime should provide indemnity or relief to C/CSPs if such data is compromised despite the best efforts by C/CSPs to avoid that happening.

With very few exceptions, the current communications data that C/CSPs provide to the LENSAs can be validated, by defence counsel, by comparison with a defendant's telecommunications service account ('bill'). This will no longer be the case with 'created' communications data and Telstra believes that prosecutors are highly likely to be challenged in court to substantiate the accuracy of the data in evidentiary proceedings.

Cost of creation and retention of telecommunications data

Telstra believes that the costs involved in any new data creation and retention regime will be significant and we will need to undertake large scale and detailed technical feasibility studies in order to understand what network, IT, vendor changes would be necessary and the costs of implementation and compliance with any new data creation and retention regime.

Telstra recognises the need to ensure that legislation and regulations remain relevant and appropriate to support critical national security and law enforcement requirements in a rapidly changing environment. The potential reforms must be effective in helping to achieve the Government's objectives and the benefits of the reforms must outweigh the costs.

By way of comparison, in July 2011, in Telstra's response to the parliamentary committee inquiry into the *Cybercrime Legislation Amendment Bill 2011* (therefore, a much smaller scale of data extraction

and preservation), we submitted that that C/CSPs would need to budget for a range of significant modifications and that preservation of stored communications for up to 180 days '*will have a major impact on these networks and systems*'.[1]

Therefore it is impossible for Telstra to speculate on the significant costs or timeframes for compliance until Government has settled on the final form of any data retention regime.

D. Telecommunications Act 1997

16. Amending the Telecommunications Act to address security and resilience risks posed to the telecommunications sector

Telstra agrees that there is a need for C/CSPs to be more aware of the security threats to their customer's data and networks and that there are strong arguments for a partnership[2] with Government to share information on potential threats to C/CSP's customer data and networks. However we believe C/CSPs should retain the discretion to assess the risks and make informed decisions based on their knowledge taking into account any advice available from Government in relation to enhancing the security, integrity and resilience of their telecommunications infrastructure.

The proposals as currently crafted would create ambiguity and uncertainty as to what is expected of C/CSPs. Any proposed regime should minimise regulatory hurdles and provide incentives for C/CSPs to act in partnership with Government. Otherwise there is a risk that C/CSPs would not be able to finalise investment decisions or complete due diligence activities whilst waiting on Government decisions about network design and technology choices, acquisitions including overseas acquisitions and equipment purchases. These proposals will require extensive consultation in order to establish a fair, well-defined and balanced regime if the Government is to proceed.

In summary, Telstra's views on the key issues include:

There are already regulated processes under which C/CSPs are required to provide notifications of additions/amendments to our network (either onshore or offshore), procurement or other business arrangements to AGD including the IC Plan (Interception Capability Plan) process and S202B under the *Telecommunications (Interception and Access) Act 1979*. We are concerned that if additional obligations are imposed on local C/CSPs that add to their costs and reduce efficiency with no demonstrated benefit to their customers or their business, we may see the migration of services offshore which would be contrary to Government objectives.

The proposed amendments impose a significant impost on C/CSPs normal operations and procurement activities as well as reducing vendor competition raising overall procurement costs for Australian-based C/CSPs. At face value it would appear that C/CSPs would need to accept government advice on what equipment they could or could not procure, how C/CSPs could or could not configure their networks and systems and possibly how they conduct their day-to-day business activities. It would also appear that this proposed obligation will only apply to a few "nominated" C/CSPs, such that the impost would not be competitively neutral. Telstra does not support this approach.

The proposed amendments appear to offer "risk assessments" to be undertaken by the Government for sensitive procurement or network modifications. What is not clear is whether these "risk assessments" would be subject to legislated timeframes so as to avoid delaying procurement or

[1] Telstra's submission to the Parliament's Joint Select Committee on Cyber-Safety, 26 July 2011, page 2

[2] This partnership could be modelled on the US Government's Joint Cybersecurity Services Pilot which is intended to share classified National Security Agency cyberthreat intelligence with the private sector and is expected to be extended to network providers.
http://www.smh.com.au/it-pro/security-it/symantecs-move-to-end-chinese-joint-venture-linked-to-cyberthreats-20120327-1vwb7.html

network design activities. It is also unclear if C/CSPs will have to implement the suggested outcomes of the "risk assessments" and if there are any penalties for not doing so.

Understanding there are risks that "nominated" C/CSPs may be seen as undertaking anti-competitive behavior if "risk assessments" recommendations limit carriage of competitor traffic, Government protections will be required from civil actions for those "nominated" C/CSPs who do implement the recommendations of the "risk assessments".

Telstra suggests that C/CSPs should be able to obtain reliable and trustworthy advice from Government to assist them in making informed decisions as an alternative. This could apply through a number of mechanisms including:

a) TISN (Trusted Information Sharing Network). Telstra already interacts with Government on national security issues through the TISN and believes that the TISN should be used more constructively in the sharing with C/CSPs of up-to-date and sensitive information on threats and vulnerabilities. TISN would also provide a 24/7 service to C/CSPs seeking security and threat advice;

b) A program that supports financial and commercial incentives for C/CSPs that would benefit both Government and customers if C/CSPs were to:

   I. implement the recommendations of the "risk assessments" from Government;
   II. immediately report (no fault, no blame or penalty in reporting) security breaches/security attacks to CERT rather than rely on voluntary reporting; and
   III. embed in their network and business management processes a set of guidelines developed by Government covering information on what, how and where C/CSPs would need to configure (or make additions/amendments) to networks, procurement or other business arrangements to enhance the security, integrity and resilience of their telecommunications infrastructure. This would limit the number of notifications required and potential risk assessments needed.

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.

E. Australian Security Intelligence Organisation Act 1979

5. Amending the ASIO Act to modernise and streamline ASIO's warrant provisions

Telstra agrees with the proposal to update the definition of 'computer'. The definition must also be consistent with the Criminal Code, Telecommunications and TIA Acts to avoid inconsistency and risks of error in interpretation.

The proposal to vary, simplify and extend the duration of warrants would have a direct impact on the warrant management systems used by C/CSPs. Consideration would need to be given to the impacts on existing interception warrants, the types of variations requested by the Attorney-General and C/CSP's resources required to manage the variations.

11. Amending the ASIO Act to modernise and streamline ASIO's warrant provisions to:

a. Establish a named person warrant enabling ASIO to request a single warrant specifying multiple (existing) powers against a single target instead of requesting multiple warrants against a single target.

While Telstra supports simplifying the warrant regime and the use of a named person warrant, it should not be put in the position of having to interpret warrants based on vague or incomplete details of either the person of interest or their services. Telstra believes warrants must continue to include details of the specific services required to be intercepted. The proposal will also impact on C/CSP's warrant management system and processes required to deliver all information requested from multiple services and systems on the single target warrant.

c. Enable the disruption of a target computer for the purposes of a computer access warrant

ASIO or any other LENSA must be able to demonstrate that such action is consistent with any lawful request. If such a change to legislation is contemplated, Telstra would expect that ASIO provide C/CSPs with full indemnity in relation to proceedings brought by a third party in relation to this form of interception.

e. Establish classes of persons able to execute warrants

Telstra agrees that the classes of persons who are eligible to execute a warrant will need to be clearly defined as to what types of warrants they can authorise and under what law. Careful consideration will also need to be given to the appropriate levels of oversight and record keeping. A list of persons will then need to be conveyed to C/CSPs to reduce any risk of harm, unauthorised interception or breaches of customer privacy by persons who are not eligible to execute a warrant.

12. Clarifying ASIO's ability to cooperate with the private sector

Telstra supports closer cooperation between ASIO (and other LENSAs) and the private sector where there is a sound mutual interest. Whether this is through continued participation in industry forums such as CSER (Communications Security Enforcement Roundtable) and BGAG (Business Government Advisory Forum) or forums such as the TISN, Telstra believes that closer cooperation will assist both LENSAs and C/CSPs in their respective goals while balancing legitimate privacy concerns.

Telstra supports the proposition that LENSAs *"capabilities must keep ahead of terrorists, agents of espionage an organised criminals who threaten national security and the safety"* of Australians. The Discussion Paper suggests there is a technology gap in LENSA capability and Telstra supports Government taking action to increase the technical capabilities within LENSAs.

LENSAs will need advanced technical skills to stay abreast of the interception challenge, understanding what knowledge or intelligence could be derived, how to target the necessary information, what information is possible to extract, the complexities and capabilities of new social communications services, the increasing volumes of internet data, and how to deal with encryption and private networks. Intercepting new types of services, and access to richer communications data provides greater operational opportunities, but with the obvious comment that more information will take longer to 'mine' to find the valuable information from a LENSA perspective.

The National Interception Technical Assistance Centre (NiTAC) was created in 2010 to help ASIO deal with the technological and legal problems of intercepting online communications. Operating as a two year trial, the intention was for NiTAC to identify future requirements for all telecommunications interceptions.

A properly structured, managed and resourced NiTAC, with active contribution and support from key Federal and State LENSAs, would help overcome many practical problems that cannot be solved by C/CSPs and regulation. But for this to work, Government and LENSAs need to understand what role Federal agencies, such as DSD, ASIO and AFP and the major state law enforcement agencies can and should play and how to make the NiTAC effective in lifting the technical capabilities of LENSAs.

This may require a shift in thinking for Government and LENSAs and may also require amendment to the oversight mechanisms by different Departments; State Ombudsman; Commonwealth Ombudsman; and the Inspector General of Intelligence and Security (IGIS). Telstra notes the complex public policy and legislative challenges that may currently constrain cooperation between different LENSAs, however, the magnitude of the technology challenges and the importance of maintaining such an important investigate capability requires a commitment by Government to review all alternative solutions, including how to best make use of existing Government resources.

Industry could also play a role in partnering with NiTAC by:

I. Seconding suitably qualified LENSA staff into C/CSPs' positions to gain knowledge on how C/CSPs develop and deploy advanced communications products, services and networks;
II. Explore opportunities for C/CSPs to rotate staff into NiTAC for short periods to provide technology training and in understanding how C/CSPs operate; and
III. Establish partnerships with equipment vendors and carriers to explore the capabilities of new technologies and understand how C/CSPs deploy the technologies in their networks (similar to US Electronic Warfare Associates or the UK Cyber Security Evaluation Centre (BT)).

17. Amending the ASIO Act to modernise and streamline ASIO's warrant provisions by:

a. Using third party computers and communications in transit to access a target computer under a computer access warrant.

Telstra believes C/CSPs will need to be indemnified from consequences that may arise from the execution of the warrant in a range of circumstances. This will include situations where ASIO is seeking assistance from C/CSPs, including requesting that C/CSPs use computers operated by C/CSPs or used by C/CSP customers who are not the target of the warrant, or that requires C/CSPs to permit ASIO to use computers operated by C/CSPs or C/CSP customers. This includes potential breaches of customer privacy or service levels and resulting commercial damages and C/CSPs would need to be able to exercise a right of refusal.

ATTACHMENT 1

ToR	Proposal	Response
1a	the legislation's privacy protection objective	Telstra supports the proposal to strengthen the safeguards and privacy protections under the lawful access to communications regime in the TIA Act (*Telecommunications (Interception and Access) Act 1979*) to ensure the protection and privacy of a customer's communications. Telstra also supports the need for consistency and alignment between the TIA Act and the Telco Act (*Telecommunications Act 1997*) for lawful interception, stored communications and any other customer data or information requested by Government. We recommend a simplification of those parts of the two Acts that compel C/CSPs to provide assistance to LENSAs in the public interest, while ensuring that approval thresholds for access are high enough to protect every consumer's right to privacy. Any reforms should promote transparency and raise public awareness levels of how and why such information may be accessed and used for public interest purposes.
1b	the proportionality tests for issuing of warrants	The proportionality testing of warrants will need to be consistent, practical and understandable by those required to implement them. Telstra remains concerned that ambiguity between the roles of agencies and requirements for C/CSPs to complete added steps will add unnecessary and avoidable complexity. There is a real need for these types of proposals to be further evaluated. The scope of some of the proposed changes to lawful warrants will blur the boundaries between the part of the interception process traditionally conducted by the C/CSPs and that carried out by the LENSAs. This will require a review of the proportionality tests for the existing warrant authorisation and evidentiary certificate regime (and a review of costs arrangements) as well as for any new types of warrants, particularly where C/CSPs may no longer simply be enabling a lawfully issued interception warrant.
1c	mandatory record- keeping standards	Telstra understands the desire for a reporting and record-keeping regime, but believes that the potential benefits of such proposals must explicitly and rigorously be evaluated against the costs associated with the implementation. The reporting regime needs to be simple and demonstrate to the public that the intended safeguards and privacy protections are working. At the same time the regime must not be administratively burdensome for both C/CSPs and LENSAs. Although the current record-keeping requirements are not overly onerous on C/CSPs, the regime does need an overhaul to achieve the intended outcomes. The existing obligation could be made more relevant to both LENSAs and C/CSPs, e.g. it is very difficult for a C/CSP to predict what products and services it will launch in 2-5 years' time and whether or not those services will have an impact on the C/CSP's legal interception capability.
1d	oversight arrangements by the Commonwealth and State	Telstra agrees that there must be consistent and practical arrangements put in place to enable oversight by both

ToR	Proposal	Response
	Ombudsmen	Commonwealth and State Ombudsmen aimed at strengthening the safeguards and privacy protections under the TIA Act and the Telco Act to ensure the security and privacy of customer communications.
2a	reducing the number of agencies eligible to access communications information	In principle Telstra supports this proposal, acknowledging the levels of rich communications data now available and likely to be the subject of a broader number of LENSA requests in the future. Telstra believes there is some merit in adopting a two-tiered communications data access regime to address potential risks of allowing access to customer data for the investigation of lesser offences. Under this type of regime, data readily available through C/CSP customer information systems could be provided under the current threshold test and would potentially remain accessible to a larger number of enforcement agencies and LENSAs.
2b	the standardisation of warrant tests and thresholds	Telstra supports the proposed changes to further limit the number of LENSAs able to request access to communications data given the increased richness of telecommunications information, and the potential for a wide range of non-criminal LENSAs to access to such information. Telstra does not believe the public interest requires the disclosure of personal information to non-criminal LENSAs such as bodies that can impose a pecuniary penalty. Currently, non criminal LENSAs can access historical data (that is, existing information or documents in the enforcement of a law imposing a pecuniary penalty or protection of public revenue) under section 179 of the TIA Act. In contrast the approval threshold to access *prospective* call data imposes an effective limitation – it may only be authorised by a criminal law-enforcement agency when it is considered reasonably necessary for the investigation of an offence that is punishable by imprisonment for at least three years.
3a	simplifying the information sharing provisions that allow agencies to cooperate	Telstra would need to understand how this might work in practice and what, if any, legal and reputational implications might arise under such arrangements before we could express a view on this proposal. For example, if Telstra releases communications data or interception content to one agency under a lawful warrant and then that information is provided by the approved LENSA to one or more other LENSAs (who in turn rely upon the data in evidentiary proceedings), what appropriate processes would need to be established to address the continuity of evidence issues?
3b	removing legislative duplication	Telstra supports the removal of duplication and ambiguity between what C/CSPs are obliged to provide under the TIA Act and what LENSAs expect C/CSPs to provide under Section 313 of the Telco Act (ie "*reasonably necessary assistance*"). Section 313 enables LENSAs to request C/CSPs to provide a wide variety of assistance on the production of a lawful request but at present there is no clear delineation between what information must be provided under the TIA Act and what can be provided under Section 313.
4a	align industry interception	At present a C/CSP's role in the 'lawful request' process is solely to deliver telecommunications data in compliance with a coercive

ToR	Proposal	Response
	assistance with industry regulatory policy	instrument. The capital "*cost of developing, installing and maintaining interception capability"* is borne by C/CSPs. C/CSPs are currently entitled to recover costs from LENSAs on a 'no cost - no profit' basis. In practice this means that C/CSPs are investing their shareholders' capital for sub economic returns, and may necessarily even recover their full operational costs in complying with existing legislation from the beneficiaries of these arrangements (i.e. national security and law enforcement agencies). In attempting to assess the financial impact and requirements of future compliance, Telstra submits there is currently much ambiguity around the structure and likely costs associated with these proposals (e.g. initial system build and ongoing maintenance costs and how they will be addressed). Telstra submits that C/CSPs should be able to recover their economic cost of developing, installing and maintaining an interception and delivery capability. The imposition of a full economic cost recovery model will also mean that LENSAs will need to demonstrate a level of rigor in their application for lawful assistance from C/CSPs.
4b	clarify ACMA's regulatory and enforcement role	The ACMA's current role would appear to have diminished over time and particularly so after the Blunn Review when parts of the Telco Act were transferred to the TIA Act. Telstra believes there needs to be clarification as to what role ACMA will have in future in monitoring compliance by C/CSPs with the Telco Act and TIA Act in respect to national security and law enforcement. The Discussion Paper does not suggest what types of additional powers may be contemplated. Telstra would recommend that whatever agency is given this enforcement role its primary focus should be on undertaking an active role in education and dispute resolution with any penalty enforcement role becoming secondary.
5a	to update the definition of 'computer' in section 25A	Telstra agrees with the proposal to update the definition of 'computer'. The definition must also be consistent with the Criminal Code, Telecommunications and TIA Acts to avoid inconsistency and risks of error in interpretation.
5b	Enabling warrants to be varied by the AG, simplifying the renewal of the warrants process and extending duration of search warrants from 90 days to 6 months.	The proposal to vary, simplify and extend the duration of warrants would have a direct impact on the warrant management systems used by C/CSPs. Consideration would need to be given to the impacts on existing interception warrants, the types of variations requested by the Attorney-General and C/CSP's resources required to manage the variations.
6a	Providing for officers to be employed under a concept of a 'level,' rather than holding an 'office.'	No comment provided

ToR	Proposal	Response
6b	Making the differing descriptions ('officer,' 'employee' and 'staff') denoting persons as an 'employee' consistent	No comment provided
6c	Modernising the Director- General's powers in relation to employment terms and conditions	No comment provided
6d	Removing an outdated employment provision (section 87 of the ASIO Act)	No comment provided
6e	Providing additional scope for further secondment arrangements	No comment provided
7	Amending the Intelligence Services Act 2001 to clarify the Defence Imagery and Geospatial Organisation's authority to provide assistance to approved bodies.	No comment provided
8a	Creating a single warrant with multiple TI powers	Telstra supports simplifying the warrant regime. This could be achieved by introducing a single and more precisely targeted warrant that provides unambiguous direction to C/CSP staff required to assist. Implementation of such a change will require careful consideration to avoid unintended consequences particularly where services may be carried by a C/CSP, but are not managed or operated by the C/CSP, e.g. OTT (Over the Top) applications and services (Whatsapp and Skype), where a C/CSP may not be able to guarantee reliable interception or provide a carrier evidentiary certificate given the uncertainty regarding how the communications may be identified or carried within the C/CSP's network. If the creation of a single warrant puts C/CSPs in a position of having to interpret warrants based on vague or incomplete details or attributes of the person of interest, the type of data or the services subscribed to by the person of interest to a LENSA, Telstra would not be able to support this proposal. The introduction of a single and more precisely targeted warrant may also require the introduction of a secure electronic warrant system to ensure the efficiencies of a single warrant system are delivered. Electronic warrants would benefit both LENSAs and C/CSPs in providing a streamlined system for serving, receiving, filing and managing warrants.

ToR	Proposal	Response
9a	Implement detailed requirements for industry interception obligations	Telstra believes the proposed model of tiered participation based on participant status creates the potential for criminals and terrorists to bypass interception arrangements through the selection of their C/CSP. The proposal also raises questions about whether a C/CSP with larger market share might be considered to be higher risk simply because it carries more traffic. In this regard Telstra is concerned that the Discussion Paper suggests the "level of engagement" would be informed by factors such as market share and customer base, meaning larger operators are likely to receive more scrutiny. A more effective regime would be to focus the supply of interception capabilities on mass market and access services where interception is most likely to be utilised and be more effective.
9b	extend the regulatory regime to ancillary service providers not currently covered by the legislation	Telstra believes further work would need to be undertaken in this regard and final proposals would need to be able to demonstrate a practical, fair and reasonable approach on C/CSP compliance. This proposal indicates that interception-type obligations could be extended beyond Australian based C/CSPs to cover website/application and overseas based providers, such as social media operators, webmail services and cloud computing providers. An ancillary effect of this extension to Australian C/CSPs would be that any products that the C/CSP was offering that covered these types of services such as webmail or OTT applications (Whatsapp, Viber and TU ME) and which have not previously been subject to lawful interception obligations other than for the carriage element would also be caught. In some cases local C/CSPs may not be aware of what services are being used by customers, i.e. VoIP services such as Skype.
9c	implement a three- tiered industry participation model	Telstra believes these proposals run the risk of creating an uneven playing field, where the compliance burden would rest disproportionately with larger C/CSPs and the effectiveness of the overall regime is undermined by allowing criminals or terrorists to avoid interception arrangements by acquiring services from smaller C/CSPs. In relation to the interception cost sharing framework, the Discussion Paper indicates that a new tiered model may be introduced where larger C/CSPs are expected to have a comprehensive interception capability (presumably at a greater cost) while smaller C/CSPs may only be required to have a minimum level capability (presumably at a lower cost). As such, Telstra does not support this proposal.
10	Amending the ASIO Act to create an authorised intelligence operations scheme. This will provide ASIO officers and human sources with protection from criminal and civil liability for certain conduct	No comment provided

ToR	Proposal	Response
	in the course of authorised intelligence operations.	
11a	Establish a named person warrant enabling ASIO to request a single warrant specifying multiple (existing) powers against a single target instead of requesting multiple warrants against a single target	While Telstra supports simplifying the warrant regime and the use of a named person warrant, it should not be put in the position of having to interpret warrants based on vague or incomplete details of either the person of interest or their services. Telstra believes warrants must continue to include details of the specific services required to be intercepted. The proposal will also impact on C/CSP's warrant management system and processes required to deliver all information requested from multiple services and systems on the single target warrant.
11b	Align surveillance device provisions with the Surveillance Devices Act 2007	No comment provided
11c	Enable the disruption of a target computer for the purposes of a computer access warrant	ASIO or any other LENSA must be able to demonstrate that such action is consistent with any lawful request. If such a change to legislation is contemplated, Telstra would expect that ASIO provide C/CSPs with full indemnity in relation to proceedings brought by a third party in relation to this form of interception.
11d	Enable person searches to be undertaken independently of a premises search	No comment provided
11e	Establish classes of persons able to execute warrants	Telstra agrees that the classes of persons who are eligible to execute a warrant will need to be clearly defined as to what types of warrants they can authorise and under what law. Careful consideration will also need to be given to the appropriate levels of oversight and record keeping. A list of persons will then need to be conveyed to C/CSPs to reduce any risk of harm, unauthorised interception or breaches of customer privacy by persons who are not eligible to execute a warrant.
12	Clarifying ASIO's ability to cooperate with the private sector	Telstra supports closer cooperation between ASIO (and other LENSAs) and the private sector where there is a sound mutual interest. Whether this is through continued participation in industry forums such as CSER (Communications Security Enforcement Roundtable) and BGAG (Business Government Advisory Forum) or forums such as the TISN, Telstra believes that closer cooperation will assist both LENSAs and C/CSPs in their respective goals while balancing legitimate privacy concerns. Telstra supports the proposition that LENSAs *"capabilities must keep ahead of terrorists, agents of espionage an organised criminals who threaten national security and the safety"* of Australians. LENSAs will need advanced technical skills to stay abreast of the interception challenge, understanding what knowledge or intelligence could be derived, how to target the necessary information, what information is possible to extract, the complexities and capabilities of new social communications services, the increasing volumes of internet data, and how to deal

ToR	Proposal	Response
		with encryption and private networks. The National Interception Technical Assistance Centre (NiTAC) was created in 2010 to help ASIO deal with the technological and legal problems of intercepting online communications. A properly structured, managed and resourced NiTAC, with active contribution and support from key Federal and State LENSAs, would help overcome many practical problems that cannot be solved by C/CSPs and regulation. But for this to work, Government and LENSAs need to understand what role Federal agencies, such as DSD, ASIO and AFP and the major state law enforcement agencies can and should play and how to make the NiTAC effective in lifting the technical capabilities of LENSAs. This may require a shift in thinking for Government and LENSAs and may also require amendment to the oversight mechanisms by different Departments; State Ombudsman; Commonwealth Ombudsman; and the Inspector General of Intelligence and Security (IGIS).
13	Amending the ASIO Act to enable ASIO to refer breaches of section 92 of the ASIO Act (publishing the identity of an ASIO officer) to authorities for investigation	No comment provided
14a	expanding the basis of interception activities	If the intent of this proposal is intended to be consistent with that outlined under 9b, namely "*to extend the regulatory regime to ancillary service providers not currently covered by the legislation*", Telstra would require further information before it could understand how this might work in practice. Telstra would support an expansion, assuming that the proposed changes are implemented in a competitively neutral manner and applied equally to all service providers to avoid distorting market outcomes and to reduce the opportunity for criminals to evade the intended outcomes of the changes.
15a	establish an offence for failure to assist in the decryption of communications	It is Telstra's position that the level of assistance that can reasonably be expected to be provided by C/CSPs should be carefully defined and limited in any event, but all the more so if an offence of failure to assist is to be created. For example, Telstra believes it would be unreasonable for a C/CSP to be required to decrypt services where the CSP is merely on-selling relevant services for a particular vendor (ie Blackberry). In this context, it would be reasonable for Government to obtain encryption keys from the relevant vendor of that product. Some of the proposed changes reflect a shift of the interception burden from LENSAs to C/CSPs. As well as developing the capability to enable interception, C/CSPs would also be required to partially process intercepts before delivery to LENSAs to create communications data and also to assist in decryption.

ToR	Proposal	Response
		Telstra does not support any proposed change to legislation where the interception burden on C/CSPs becomes one of 'processing' or 'creating' communications data.
15b	institute industry response timelines	Telstra submits that for Government to mandate 'response timelines' would also require Government to spend significant funds to support the introduction of a fully automated request management system (as discussed in 8a) for use by LENSAs and C/CSPs otherwise the LENSAs would not obtain the benefits intended from this proposal. Before response timelines could be introduced, LENSAs would need to be provided with enhanced capability (i.e. an automated streamlined electronic system) for serving, receiving, filing and managing warrants and the receipt of intercepted material and communications data. The current electronic delivery system (SedNode) requires manual intervention to enable processing of communications data by C/CSPs.
15c	tailored data retention periods for up to 2 years for parts of a data set, with specific timeframes taking into account agency priorities, and privacy and cost impacts	The proposed arrangements are likely to be very costly and raise substantial security and privacy questions that will need to be answered. Telstra believes the proposed changes to retain a larger amount of telecommunications data will blur the boundaries between the interception process traditionally conducted by the C/CSPs and that carried out by the LENSAs. Telstra believes that an effective and fair data retention regime must recognise there is an increased risk to privacy that C/CSPs will need to manage, and the regime should provide indemnity or relief to C/CSPs if such data is compromised despite the best efforts by C/CSPs to avoid that happening. Telstra believes that the costs involved in any new data creation and retention regime will be significant and we will need to undertake large scale and detailed technical feasibility studies in order to understand what network, IT, vendor changes would be necessary and the costs of implementation and compliance with any new data creation and retention regime. Telstra recognises the need to ensure that legislation and regulations remain relevant and appropriate to support critical national security and law enforcement requirements in a rapidly changing environment. The potential reforms must be effective in helping to achieve the Government's objectives and the benefits of the reforms must outweigh the costs. Therefore it is impossible for Telstra to speculate on the significant costs or timeframes for compliance until Government has settled on the final form of any data retention regime.
16a	by instituting obligations on the Australian telecommunications industry to protect their networks from unauthorised	Telstra agrees that there is a need for C/CSPs to be more aware of the security threats to their customer's data and networks and that there are strong arguments for a partnership with Government in advising us of the threats to our customer data and networks. However we believe C/CSPs should retain the discretion to assess

ToR	Proposal	Response
	interference	the risks and make informed decisions based on their knowledge taking into account any advice available from Government in relation to enhancing the security, integrity and resilience of their telecommunications infrastructure. The proposals as currently crafted would create ambiguity and uncertainty as to what is expected of C/CSPs. Any proposed regime should minimise regulatory hurdles and provide incentives for C/CSPs to act in partnership with Government. Otherwise there is a risk that C/CSPs would not be able to finalise investment decisions or complete due diligence activities whilst waiting on Government decisions about network design and technology choices, acquisitions including overseas acquisitions and equipment purchases. These proposals will require extensive consultation in order to establish a fair, well-defined and balanced regime if the Government is to proceed. Telstra understands that the Government has concerns in relation to securing Australian telecommunications data and networks from cyber crime and related criminal threats, and we believe we are well placed to assist the Government to develop a practical framework that can focus on the real problems, while achieving the right incentive structure and value proposition for C/CSPs.
16b	by instituting obligations to provide Government with information on significant business and procurement decisions and network designs	There are already regulated processes under which C/CSPs are required to provide notifications of additions/amendments to our network (either onshore or offshore), procurement or other business arrangements to AGD including the IC Plan (Interception Capability Plan) process and S202B under the TIA Act. The proposed amendments impose a significant impost on C/CSPs normal operations and procurement activities as well as reducing vendor competition raising overall procurement costs for Australian-based C/CSPs. Telstra does not support this approach. The proposed reforms would need to include clear Government protections from civil actions for C/CSPs who do implement the recommendations of the reforms.
16c	Creating targeted powers for Government to mitigate and remediate security risks with the costs to be borne by providers	While the Discussion Paper indicates that directions would only be given after an appropriate period of discussion and engagement with the C/CSP, C/CSPs would be concerned about the prospect of very prescriptive directions, which would limit flexibility and commercial viability around their security solutions and the cost of any remedial action and what the consequences would be to C/CSPs who fail to remediate Government specified security risks. Telstra would not support this proposal. There would also need to be a framework that would include clear mechanisms to enable an independent judicial review or appeal process to deliver timely, balanced, and equitable decisions on Government imposed binding directions or specific mitigation action to reduce the likelihood of drawn out litigation in relation to contentious rulings or decisions.

ToR	Proposal	Response
		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.
16d	Creating appropriate enforcement powers and pecuniary penalties	The proposal to introduce new security compliance obligations on C/CSPs to maintain "competent supervision" and "effective control" over their networks could require C/CSPs to change the way they manage relationships with existing vendors and suppliers. The Discussion Paper indicates that Government will provide general guidelines, advice and briefings, but despite this the standard of security compliance required may still be changeable and difficult for C/CSPs to manage. The proposal may also bring C/CSPs into conflict with existing corporate obligations, particularly those relating to impacts in the marketplace and the continuous disclosure of information to the financial markets. It would also be challenging to retrofit these requirements to existing long-term commercial arrangements that C/CSPs may already have in place with key vendors and suppliers (e.g. in order to comply it may be necessary to renegotiate the security aspects of outsourcing agreements that are currently in place). Telstra would not support this proposal.
17a	Using third party computers and communications in transit to access a target computer under a computer access warrant	Telstra believes C/CSPs will need to be indemnified from consequences that may arise from the execution of the warrant in a range of circumstances. This will include situations where ASIO is seeking assistance from C/CSPs, including requesting that C/CSPs use computers operated by C/CSPs or used by C/CSP customers who are not the target of the warrant, or that requires C/CSPs to permit ASIO to use computers operated by C/CSPs or C/CSP customers. This includes potential breaches of customer privacy or service levels and resulting commercial damages and C/CSPs would need to be able to exercise a right of refusal.
17b	Clarifying that the incidental power in the search warrant provision authorises access to third party premises to execute a warrant	No comment provided
17c	Clarifying that reasonable force may be used at any time during the execution of a warrant, not just on entry	No comment provided
17d	Introducing an evidentiary certificate regime	No comment provided

ToR	Proposal	Response
18a	Add a new ministerial authorisation ground where the Minister is satisfied that a person is, or is likely to be, involved in intelligence or counter- intelligence activities	No comment provided
18b	Enable the Minister of an Agency under the IS Act to authorise specified activities which may involve producing intelligence on an Australian person or persons where the Agency is cooperating with ASIO in the performance of an ASIO function pursuant to a section 13A arrangement. A Ministerial Authorisation will not replace the need to obtain a warrant where one is currently required	No comment provided
18c	Enable ASIS to provide training in self- defence and the use of weapons to a person cooperating with ASIS	No comment provided