Department of Home Affairs
GPO Box 241
Melbourne VIC 3001
Australia

Date 10 Sep 2018
Reference Assistance and Access Bill 2018 (draft)

By Email:
[redacted]

Internet Australia appreciates the opportunity to comment on the Department's draft *Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018* released in August 2018 (The Bill).

In preparing its submission, Internet Australia has had access to the joint submission of Communications Alliance, AMTA and AIIA, and wishes to strongly support the concerns raised in section two of that submission.

Confidential and trusted communications are essential to the ongoing safety, security and efficient use of global Internet communications networks for business, government and personal interactions. Strong encryption technologies are recommended to ensure confidentiality, and to ensure trust by authenticating that communications are really with the desired recipient and are not being hijacked and redirected by an imposter.

We recognise that law enforcement has a legitimate desire to access and view information transmitted across telecommunications networks by serious criminals, and that often these messages are encrypted in some form, as Internet developers enhance the security and confidentiality of the services they provide to the public.. We must however always be vigilant to ensure well-intentioned measures to facilitate such access does not reduce security or privacy for the vast majority of legitimate and law-abiding uses, or retard the ongoing development of future secure and trusted methods of communication. The legislation must put in place a framework that is fit for purpose and protects all of the parties in the system, including protecting end-users from harmful changes to their devices and applications.

After only a few weeks to review and evaluate a complex and lengthy document we remain very concerned at the vague, ill-defined descriptions and requirements, the lack of effective consultation, and the lack of effective checks and balances. In many cases the protections and limitations described in the Explanatory Document are not reflected in the text of the Bill.

This draft legislation clearly needs further work before it can be seriously considered to be ready for passing. The Government and the Australian public needs to recognise the clear potential dangers to the security and privacy of ordinary Australians which this legislation, in its current form, poses.

This draft legislation is unprecedented in Australia, and we believe, globally, in the broad expansion of entities that are drawn into the communications access and interception regime. Beyond licensed carriers and carriage service providers this legislation aims to enforce content-access requirements for the first time on the device manufacturers and resellers of end-user's devices, on content services, and on any organisation or person who operates a website. Australia is only the second OECD country to embark on such legislation (behind the UK), although we note the recent statement of intent by the Five Eyes group of nations to take wider action in this area. Many of the over-the-top communications messaging platforms that this legislation seeks to access have no presence or connection with Australia, while the vast majority of the organisations and individuals that this legislation might apply to are individuals or small organisations with no reasonable capacity to understand these new rights and obligations, or ability to prepare for new laws.

We have valued the opportunities over the past year to meet with members of the group that has worked on this draft, although without the document being available for review at those times those discussions were necessarily extremely high level and limited in detail. Now that we and the various affected industries have had a chance to review the text and requirements, we would welcome further opportunities to have our members and experts meet with the Department to further discuss our comments and observations raised in this paper.

About Internet Australia

Internet Australia is the not-for-profit organisation representing all users of the Internet. Our mission – "Helping Shape Our Internet Future" – is to promote Internet developments for the benefit of the whole community, including business, educational, government and private Internet users. Our leaders and members are experts who hold significant roles in Internet-related organisations and enable us to provide education and high level policy and technical information to Internet user groups, governments and regulatory authorities. We are the Australian chapter of the global Internet Society, where we contribute to the development of international Internet policy, governance, regulation and technical development for the global benefit.

Yours Sincerely

Dr Paul Brooks
Chair – Internet Australia
[redacted]

[redacted]

Submission by Internet Australia

Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (draft)

Introduction

This submission is in two major parts.

The first part contains high-level comments and observations on the overall structure of the legislation, and the environment of modern encrypted communications.

The second part contains detailed comments and observations of specific provisions within the draft legislation.

1 High-Level Comments

1.1 Inadequate opportunity for consultation

We consider the four week period provided for review of these papers to be wholly inadequate for such a complex issue with such wide and global ramifications.

This consultation alone required the review of over 150 pages of explanatory material, and a 174-page draft legislation paper that modifies 9 other items of legislation, requiring the new provisions to be cross-checked against those other documents.

Four weeks is not sufficient to perform such a review comprehensively, so this submission is necessarily incomplete, with other substantive issues likely to be found following deeper review. Similarly there are many directly-affected companies, including many licensed carriers, many carriage service providers and likely internationally-based over-the-top (OTT) service providers who have not have been able to review the papers and provide considered feedback within the limits advertised by the Department. The Department should not consider that the list of concerns raised by the collection of submissions in this consultation round is a complete list of aspects that need to be rectified.

Australia must be exceedingly cautious in looking at these laws and new capabilities, as they have an affect not just in Australia and on Australians, but across the globe. Unintended consequences and hasty implementation of subtly interconnected requirements could harm the future development of Internet commerce and trust world-wide, and hamper Australian industry from competing internationally. The things that Australia does well in their legislation are likely to be copied by others. Similarly, mistakes that Australia makes in designing its framework are also likely to be emulated by other countries.

We urge the Government to consult publicly and transparently over multiple rounds, to enable a much wider range of affected providers and manufacturers to be engaged, beyond the limited subset of industry that we understand the Department consulted with prior to the release of these papers.

In parallel with that process, we recommend the Department institute a series of meetings and workshops with affected industry bodies to consolidate feedback and further review of future drafts, similar to the extensive consultation process that occurred with the introduction of data retention requirements.

Recommendation #1

We recommend that the Government refer the draft legislation to the Parliamentary Joint Committee on Intelligence and Security (PJCIS) for public and, if necessary, private hearings with a wide range of stakeholders.

Recommendation #2

We recommend the Department institute a series of meetings and workshops with industry bodies, affected stakeholders and the public to consolidate feedback and further review of future drafts, similar to the extensive consultation process that occurred with the introduction of data retention requirements.

1.2 The importance of strong encryption

Encryption is a technical foundation for trust on the Internet. It promotes freedom of expression, commerce, privacy, user trust, and helps protect data from bad actors. Encryption and related techniques are also used to build increased security for financial transactions and to protect the private communications of end users. Examples include establishing whether data has been tampered with (data integrity), increasing users' confidence that they are communicating with the intended receivers (authentication), and forming part of the protocols that provide the evidence that messages were sent and received (nonrepudiation).

Encryption is all around us. It hides usernames and passwords from prying eyes, protects the information exchanged every time a person uses an ATM or swipes a credit-card, conducts a purchase from a smartphone, makes a call from a mobile phone, or presses a key fob to unlock a car. It is a versatile technology, increasingly pervasive in our daily lives, and critical to the security of much of what we do. It is critical for all global commerce, banking, and securities markets. Automatic software updates for billions of end-user devices depend on strong encryption and authentication to prevent the update process being maliciously hijacked.

For these reasons, the Internet Society believes that encryption should be the norm for all Internet traffic and data storage.

As far back as 1996, the Internet community has been driving increased use of encryption to enhance security and trust[1]. This drive has increased since 2014, when the Internet Architecture Board and the Internet Engineering TaskForce (IAB and IETF) urged the industry [2] to work to build strong encryption, and enhanced security measures such as authentication by cryptographically strong digital signatures, into every new and old protocol communicating across the Internet:

> The IAB urges protocol designers to design for confidential operation by default. We strongly encourage developers to include encryption in their implementations, and to make them encrypted by default. We similarly encourage network and service operators to deploy encryption where it is not yet deployed, and we urge firewall policy administrators to permit encrypted traffic.
>
> We believe that each of these changes will help restore the trust users must have in the Internet.
> (IAB Statement on Internet Confidentiality, 14 November 2014)

Internet Australia is heartened to note the Department's support for encryption technologies as a vital part of Internet and computer security, and that this legislation is not designed to weaken encryption technologies. Rather, this legislation seeks to gain access to devices and communications applications, including websites, to look at messages and data stored on the device or in the application before or after transmission.

1.3 Impact on Small Business

In its current form, the draft legislation is concerning for export oriented Australian small businesses because of the uncertainty which it will create with their international markets. These companies frequently have to guarantee that they will comply with the laws of the country into which they are making the sale and that their products will not be tampered with. This legislation could jeopardise these markets Further, small businesses will need to pay costs for compliance before the actions are taken for compliance with a Request or Notice and funding assistance, therefore, should be available up front.

In this context, Internet Australia's discussions with officials and Ministerial offices revealed that the Government has engaged in very extensive consultations with large service providers (particularly trans-national corporations) in framing the draft legislation. However, there appears to have been little or no consultation with smaller Australian owned service providers. This appears to us to represent a major failure in legislative design which must be addressed.

[1] RFC 1984 "IAB and IESG Statement on Cryptographic Technology and the Internet", August 1996, online at https://tools.ietf.org/html/rfc1984

[2] IAB Statement on Internet Confidentiality, 14 November 2014, online at https://mailarchive.ietf.org/arch/msg/ietf-announce/ObCNmWcsFPNTIdMX5fmbuJoKFR8

1.4 Need for Scenarios and Case-Studies

In conversations with officials we have asked how the government imagines its legislation will work in practice. The answers have been varied.

This Bill is complex, with interactions with other provisions in existing legislation that is difficult to determine.

We believe it would be very helpful if the Government could develop some illustrative scenarios and flowcharts for decision-making in which the thing requested is technically feasible, and cases where it is not feasible, and cases where Government and industry cannot agree as to its technical feasibility. The case-studies and flowcharts should enable a provider to navigate through the processes and their options and decisions should they receive any of the three proposed forms of notices, without a provider needing to engage legal assistance to refer back to the legislation

It is essential that Government establish clear and consistent processes if it is to expect industry to trust the new framework.

Recommendation #3

We recommend that Government, with industry and affected providers from each of the described provider classifications, jointly create multiple flowcharts, case-studies, processes and procedures and other guidance material to assist providers in navigating through their options and responsibilities should they receive various types of Notices with different categories of applicability, feasibility or non-feasibility, to create systemic and non-systemic weaknesses, to assist providers in understanding the expectations of Government when a notice is received.

2 Specific Comments on the draft legislation

2.1 Relevant Objectives for Assistance or Access

The primary and essential purpose of this draft legislation is to facilitate enforcement authorities to gain access to the content of communications – specifically, communications where intercepting the content as it travels 'over the wire' would be unintelligible because the content of the communication is encrypted.

The existing regulatory framework recognises that the privacy of the content of such communications must be respected unless there are strong grounds for access or interception. Federally there are protections for both voice communications and 'stored communications' (text and emails, for example). Interception or access to the communications content requires a warrant

to be issued, and are, in both cases, only permitted in circumstances including the commission or likely commission of a 'serious offence', a 'serious contravention' or a 'serious foreign contravention'[3].

This new legislation also is designed to access the content of communications:

> *"The proposed changes are designed to help agencies access intelligible communications through a range of measures, including improved computer access warrants and enhanced obligations for industry to assist agencies in prescribed circumstances."*[4]

In other words, the aim of this legislation is to give access to 'intelligible communications' – the content of communications that is otherwise protected by Federal, State and Territory legislation.

The 'relevant objective' for which Voluntary Technical Assistance can be requested under this new legislation however has a much lower and broader hurdle:

> *(a) Enforcing the criminal law and laws imposing pecuniary penalties; or*
> *(b) Assisting the enforcement of the criminal laws in force in a foreign country; or*
> *(c) Protecting the public revenue; or*
> *(d) The interests of Australia's national security, the interests of Australia's foreign relations or the interests of Australia's national economic well-being.*[5]

There is a similar breadth of 'relevant objectives' for the issue of a Technical Assistance Notice[6] and a Technical Capability Notice[7].

There seems to be little point in requesting assistance or issuing a notice if not to subsequently gain access to the content of communications, through a warrant under the TIA Act or through police activity physically inspecting the contents of memory of the device. Indeed the new legislation is stated to be designed to enable access to intelligible (unencrypted or plain-text) communications.

For this reason we submit that the relevant objectives for the new legislation and for the assistance and notices are too low and broad, and should be changed to the objectives applying to the circumstances under which warrants are to be justified for access to the contents of the communication through lawful interception or stored data warrants, had the communication contents not been encrypted.

---

[3] *Telecommunications (Interception and Access) Act 1979* (TIAA) ss 5D, 5E, 5EA and 7 and Part 3. (see also state and territory legislation on the use of listening devices which also restricts) their use.

[4] Assistance and Access Bill 2018: Explanatory Document, p. 5.

[5] Telecommunications and Other Legislation (Assistance and Access) Bill 2018 (the Bill) Clause 317G(5).

[6] The Bill Clause 317L(2)

[7] The Bill Clause 317S(3).

2.2 Reasonable, proportionate, practicable and technically feasible.

The Explanatory Document suggests that requirements imposed under the Bill should be guided by four principles: that the requirements are reasonable, proportionate, practicable and technically feasible.

Within the Bill, we note that a Technical Assistance Request (TAR) (Sect 317G-K) is not required to be reasonable, proportionate, practicable or technically feasible. Sect 317ZA (1), many pages away in the draft document, identifies that a TAR must be complied with to the extent that the provider is capable of doing so. As drafted, a provider would be in breach of the Act if they were to be asked to do an act that required unreasonable or impractical efforts to achieve the requested result, such as putting so many resources into delivering the requested activity that the rest of the business suffered.

Regarding a Technical Assistance Notice (TAN), Sect 317P identifies it is the Director-General of Security or a chief officer of an interception agency that is to make a judgement call about these four matters:

> *317P Decision-making criteria*
>
> *The Director-General of Security or the chief officer of an interception agency must not give a technical assistance notice to a designated communications provider unless the Director-General of Security or the chief officer, as the case requires, is satisfied that:*
>
> *(a) the requirements imposed by the notice are reasonable and proportionate; and*
> *(b) compliance with the notice is:*
> *(i) practicable; and*
> *(ii) technically feasible.*

Similarly Sect 317R identifies that the Director-General of Security, or a chief officer of an interception agency must revoke a TAN if they are satisfied the requirements are not reasonable or proportionate, or compliance is not practicable or is not technically feasible. It is not clear how such a person is likely to form an opinion that a TAN should be revoked for these reasons, if they couldn't have formed the same opinion prior to the TAN being issued., or how the industry should expect to be able to demonstrate that a TAN should be revoked..

With a TAN we note there is no opportunity for consultation with the provider prior to issuing the TAN, as is contemplated in Sect 317W for a Technical Capability Notice (TCN).

With a TCN, these can only be issued by the Attorney-General, and only after at least 28-days' notice is allowed for the provider to make a submission regarding the Notice.

It is clearly unworkable that the agency, rather than the provider who is being issued a Notice to do an act on a network or item of equipment or software for which the provider is the most informed

and expert, is to determine whether the request is practicable or technically feasible, or reasonable given the nature of the investigation. Only the provider receiving the request could be able to make that subjective judgement call.

Only with a TCN does a provider have an opportunity to educate and submit reasons why a TCN would be unreasonable or impracticable. The Attorney-General must give at least 28 days' notice of such Notice and invite the communications provider to make a submission on the Notice, although if it a 'matter of urgency' or compliance with the 28 day consultation period is 'impractical' then even that consultation can be waived[8]. There are no similar provisions for a Voluntary Assistance Request of a Technical Assistance Notice.

Clearly, the myriad of communications providers caught by this legislation will not have legal experts on tap, and they will need assistance in understanding what may be required of them and indeed, have access to independent arbitration to address situations where what may be sought by security and law enforcement agencies is not possible, reasonable or practicable under the circumstances. Sect 317ZF(3)(e) permits a provider to seek legal advice in relation to a Notice, however a legal practitioner is unlikely to have the necessary engineering and technical expertise to determine an appropriate response.

The apparent absence of a technically literate and expert arbitrator of disputes is a deeply troubling aspect of the draft legislation. If a Law Enforcement Agency insists that a technical solution is feasible and this is disputed by the communications provider, there should be a mechanism to ensure such disputes can be sensibly resolved. Internet Australia does not accept that the Attorney-General or a CEO of an interception agency, acting on the advice of officials, is an acceptable arbitrator in these circumstances. We consider that there is a clear role for a technical arbitrator who is trusted by both sides of the conversation, as well as for independent legal advice.

Recommendation #4

We recommend that a consultation period if at least 28 days be allowed for voluntary Technical Assistance Requests and for Technical Assistance Notices, and that the ACMA or other independent arbitration facility knowledgeable about the technical and other aspects of providers be available to the provide to assist in determining whether and/or how compliance with a request or notice could or should be addressed.

2.3 Breadth of Coverage of providers

In its current form, the potential reach of this legislation is enormous. Indeed, the chart indicating possible 'designated communications providers' and their 'eligible activities' extends over three pages of the Bill[9]. It will cover many hundreds (if not thousands) of smaller players - web hosts, software developers, maintenance and installation companies, data processers, contract line

[8] The Bill, Clause 317W

[9] The Bill Clause 317C

technicians – as well as non-telecommunications entities such as consumer electronic suppliers, department stores, etc. Many will have no idea that they will be covered by this legislation, let alone what will be required of them.

The other issue is the very lengthy and vague 'list of acts or things'[10] that a communications provider could be asked or required to do. Indeed, it would be very difficult for many communications providers to know in advance whether they would be able to comply, or at what cost to them.

Internet Australia is fearful that, in designing such a broad scope of coverage, the legislation is not fit for purpose since it is likely to design in over-reach by law enforcement agencies and the creation of vast potential for damaging unintended consequences further down the road.

Recommendation #5

We recommend the Department consider a size threshold for organisations that are to be subject to the Bill, such as the upper threshold of 'small business' per the ATO definition, such that the organisations subject to the onerous requirements are large enough to reasonably already have sufficient legal and regulatory expertise to respond to the majority of requests, while the Department has a reasonable expectation of covering the majority of encrypted communications.

Recommendation #6

We recommend that the Department consider a process for an organisation to be formally exempted from the requirements of the Act, if they demonstrate that they can play no useful part in facilitating access to encrypted communications. An example of such an entity would be a retail department store, where the small-electrical department might sell Internet connected devices such as Smart TVs and consumer modems , but have no part in their connection or use or be able to influence modifications to their software.

2.4 Confusion over participants in the Telecommunications Industry

The *Telecommunications Act 1997* Sect 108-111B defines sections of the telecommunications industry and participants, including a definition of electronic messaging service providers.

The new legislation in Sect. 317C lists a vastly greater range of persons or organisations, including manufacturers of components for use, or likely to be used, in the manufacture of customer equipment and facilities. This legislation also lists a 'person who provides an electronic service that has one or more end-users in Australia', which may duplicate the existing *electronic messaging service provider* definition.

[10] The Bill, Clause 317E

[redacted]

Such varied lists of persons and organisations, multiple descriptions of electronic messaging service providers, is likely to cause confusion in lay-persons attempting to interpret the Telecommunications Act.

Recommendation #7

We recommend the Department harmonise and attempt to re-use existing definitions in the Telecommunications Act 1997, including relating to Sect. 108-111B, rather than have multiple different definitions of relevant and participating persons and organisations scattered throughout this Act, to avoid further confusion.

2.5 Component manufacturers should be removed

The new Sect 317C list of types of persons deemed to be *designated communications providers* includes:

- person manufactures or supplies components for use, or likely to be used, in the manufacture of a facility for use, or likely to be used, in Australia
- person manufactures or supplies components for use, or likely to be used, in the manufacture of customer equipment for use, or likely to be used, in Australia

with their 'eligible activities' being 'a) the manufacture by the person of any such components; or (b) the supply by the person of any such components'

We submit that it is ludicrous to include component manufacturers and component suppliers into this list. Firstly, a component manufacturer or supplier will likely have no idea if their component 'is likely to be' included in a telecommunications facility or equipment, and even if it is, how it might be used. Even if they do know, the facility operator and equipment manufacturer are also in the list, so any request or notice for assistance can be served on the operator or whole-of-device manufacturer. Including suppliers of components is also questionable – storefronts and wholesale warehouses can have little impact or information relevant to this subject, and no expectation of being subject to the legislation or able to determine an appropriate response should they receive a notice.

Including these types of persons into the lists raises suspicions that this legislation could be used to overreach and implant surveillance software into components and thus into devices or facilities without even the device or facility owner knowing about it, thereby compromising and likely forming a systemic weakness in the device or facility, (without the owner or the component manufacturer being able to recognise the systemic weakness) and bypassing authorisation processes for interception or device tampering in ways that should only be expected for ASIS/ASIO for matters of national security.

Recommendation #8

We recommend that 'component manufacturers and suppliers' be removed from the list of 'designated communications providers'

2.6 Complexity of multiple agencies

Service provider members are extremely concerned about the large number of organisations, and potential profusion of authorised individuals issuing notices under delegation. There is great risk that uncoordinated Notices from multiple agencies may overlap and cause unintended problems, without the provider being able to disclose the fact of a Notice or the acts that it required them to do or modify to another agency.

Within the Lawful Interception regime, this concern was addressed with the creation of the Communications Access Coordinator[11], an office that coordinates and mediates the various interception agencies and presents a single point of contact to the service provider community.

With this new legislation the need for a central coordinating mediation office is even more essential, as this legislation contemplates agencies requiring changes to be made to the operation of devices and systems, and the insertion or deletion of security and other functions. With no coordination amongst the various offices and individuals seeking to issue requests and notices, changes required by one agency may invalidate or counteract changes requested by a different agency or individual, leaving the provider in the situation of being unable to comply in any meaningful way, and leaving both agencies frustrated in their attempts to achieve their goals.

Recommendation #9

We recommend that the Department create a new agency similar to the Communications Access Coordinator, or add the coordination of TARs, TANs and TCNs to the duties of the Communications Access Coordinator, to form a single-point of contact for service providers for all Requests and Notices under this Bill. Such a centralised resource would be essential for transparency and accountability, and could help ensure the agencies requests are, in fact, reasonable, proportionate, practicable and technically feasible, and do not invalidate each other.

2.7 Costs of Compliance for Technical Assistance Requests

The Explanatory Document says that:

> *The Bill maintains the default position that providers assisting Government should not absorb the cost of that assistance nor be subject to civil suit for things done in accordance with requests from Government.* [12]

[11] Telecommunications (Interception and Access) Act 1979 (TIAA) ss 6R

The Bill provides that a communications provider must comply with a requirement on the basis that the provider neither profits from complying with the requirement nor bears the reasonable costs of complying. However, that section only applies to Technical Assistance Notices and Technical Capability Notices[13]. There is no similar provision for recipients of Voluntary Technical Assistance Requests, despite the fact that the Government expects this to be the most common form of assistance sought under this framework.

A clear concern for many of the small communications providers is that they may have little or no spare resources to respond to these Voluntary Requests and would be strongly motivated not to comply with the Request or may be unable to address the request through insufficient resources. Therefore, such Requests should allow for prior consultation, and flexibility around the time requirements, and also the Bill should be changed to provide for cost-recovery on the same basis as for TANs and TCNs.

Recommendation #10

We recommend that providers can recover their reasonable costs in complying with a TAR on the same basis as the Bill provides for TANs and TCNs. Costs that should be recoverable should include all reasonably incurred CAPEX and OPEX costs, including costs of hiring staff or having to backfill staffing through employment or contract of resources to do the duties of staff diverted from their normal duties while implementing a TAR, TAN or TCN.

2.8 Systemic Weaknesses and Systemic Vulnerabilities

Under both Technical Assistance Notices and Technical Capability Notices, the legislation has an apparent safeguard that a communications provider cannot be requested to:

- build or implement a systemic weakness or systemic vulnerability into a form of electronic protection, or
- prevent a designated communications provider from rectifying a systemic weakness or a systemic vulnerability in a form of electronic protection.[14]

We not there is no similar provision or safeguard for voluntary Technical Assistance Requests to not result in systemic weaknesses or vulnerabilities.

[12] Explanatory Document p. 9

[13] The Bill Clause 317ZK(1) and (3)

[14] The Bill Clause 317ZG

Recommendation #11

We recommend that Clause 317ZG should be amended to extend its prohibitions against creating systemic weaknesses and systemic vulnerabilities to cover Voluntary Technical Assistance Requests.

Further, the Bill fails to define what sort of weaknesses or vulnerability might be classified as 'systemic', and the concept is inherently subjective. Further, it appears to be the issuer of the instruction, rather than the recipient, who is to determine whether compliance with the request would result in a systemic weakness or systemic vulnerability. The vesting of this subjective judgement with the agencies making the request, trusting that the agencies will be able to self-limit their requests, makes the apparent safeguard an illusion.

Only the recipient of the notice is likely to be in a suitably informed position to judge whether complying with the Notice would likely result in a systemic weakness or vulnerability in a system, and what forms of changes could result in weaknesses and vulnerabilities, systemic or otherwise.

Recommendation #12

We recommend that the Department consider creating guidance documents regarding 'systemic' weaknesses and vulnerabilities, especially as compared to ordinary weaknesses and vulnerabilities, and engage with industry to jointly assist in describing guidance and process flowcharts to assist the agencies and industry to distinguish when a systemic issue is likely to be created.

2.9 Accountability

In this legislation, both the recipient and provider of the request or Notice must not reveal that they have issued/received a Request or Notice except in very limited circumstances[15]. Providers may, but are not required, to disclose the number of TARs, TANs and/or TCNs no more frequently than a period of 6 months.

While there is a requirement that the number of Technical Assistance Notices and Technical Capability Notices be reported annually by the Minister[16], there is no such requirement for reporting the numbers of voluntary Technical Assistance Requests.

We have a broader concern arising from the lack of transparency and accountability in the proposed scheme to be established by the legislation. We accept that there is a legitimate need for secrecy around the details of any individual investigation or its attendant technical information assistance requests. However, an accountability regime which simply counts the number of such requests provides little opportunity for any external scrutiny to determine whether the scheme itself is effective in achieving its objectives, or whether it is having unintended consequences.

[15] The Bill Clause 317ZF

[16] The Bill Clause 317ZS

[redacted]

Recommendation #13

We recommend Clause 317ZS be amended to require that statistics of all voluntary Technical Assistance Requests be reported annually, together with annual reporting of the broad range and coverage of these requests and notices.

Ends

[redacted]