SENETAS
Security without compromise

11 February 2018

Mr Andrew Hastie MP
Chair
Parliamentary Joint Committee on Intelligence & Security
Parliament House
Canberra ACT 2600

Dear Mr Hastie

Submission to PJCIS - Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018

Senetas Corporation welcomes the decision to undertake a review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 (the **Act**) by the PJCIS, and we appreciate the opportunity to provide a further submission for the committee's consideration in relation to this unprecedented legislation.

In the short period leading up to the parliament's consideration of the Bill in early December 2018, the then proposed legislation was the subject of extensive public debate. Notwithstanding the slew of last-minute amendments made to the Bill prior to its passing on the 6th of December 2018, the majority of the more serious concerns raised, by very many parties during the period of its review by the PJCIS, were largely dismissed, if not ignored. More worrying however, has been the realisation of many of the concerns, expressed by industry and others, of the consequences of the then Bill becoming law.

This submission provides further evidence of the weaknesses in the legislation and implications to the Australian technology and telecommunications industry. Senetas strongly urges the Government to reconsider the Act in its entirety as part of a collaborative consultation process which takes into account the views of all relevant stakeholders and persons that may be affected by the Act and balances all competing interests, including the national interest.

Senetas recognizes the important role of the committee in providing advice to parliament in relation to this legislation and is available to provide any further information or evidence at a future hearing.

Yours Sincerely

[redacted]

Francis W. Galbally
Chairman
Senetas Corporation Ltd

[redacted]

Andrew Wilson
Chief Executive Officer
Senetas Corporation Ltd

SENETAS
Security without compromise

11 February 2019

Submission to PJCIS - Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018

At the outset, Senetas reiterates its comments, made in our previous Submission, in addition to the comments and evidence presented by Senetas' Chairman and CEO to the committee, and in the various related submissions concerning the then Bill in late 2018. Senetas does not consider the concerns and issues raised then to have been adequately addressed or rectified prior to the passage of the Act. In particular, we strongly support and endorse the comments made in submissions to the Committee by the Law Council of Australia, Communications Alliance, Ai Group, AIIA, AMTA, DIGI and IPTA, and Associate Professor Vanessa Teague and Dr Chris Culnane, both as part of the current review and prior to the passage of the Act.

Senetas' earlier submission outlined six substantive areas of concern. The amendments made to the Bill have, in the main, failed to address these issues. In summary the outcomes are:

Issue	**Response/Outcome**
1. The Bill risks damaging Australian developers' and manufacturers' reputations in international markets leading to lost exports, jobs, technical expertise, etc.	This risk has been realised. See also Issue #1 below.
2. The Bill increases the risk of compromising the security and privacy of citizens and businesses as a consequence of weaker cyber security practices and easier access to new tools for cyber criminals.	Little or no action taken.
3. Poor integration testing of capabilities could lead to unforeseen consequences, including the potential for large scale network outages impacting internet service in Australia and throughout the world.	Little or no action taken. The Risk remains unmitigated and the revised secrecy provisions potentially elevate likelihood. See also Issue #2 below.
4. The proposed legislation risks compromising critical encryption systems by introducing "systemic weaknesses" into products and the internet as a whole.	Unintelligible definitions of "Systemic Weakness" added (without industry consultation). The Act fails to address the underlying concern. See Issue #2.
5. Bill may force Providers to breach foreign laws.	Partially addressed.
6. Limited Consultation with industry in the development of the draft Bill.	Recent attempts by DHA to address this in relation to implementation of the Act are noted.

This submission reflects our views on several specific, targeted areas that we have identified as being of particular concern as a consequence of the Act becoming law in December 2018. While some aspects touch on issues raised in our earlier submissions, in the main the matters included here should be seen as being in addition to those raised earlier. **Attachment A** to this submission represents a number of proposed amendments to the Act for the committee's consideration.

SENETAS
Security without compromise

11 February 2019

Notwithstanding these specific comments, and the proposed amendments (at **Attachment A**), we continue to strongly urge the Government to reconsider the Act in its entirety as part of a collaborative consultation process which takes into account the views of all relevant stakeholders and persons that may be affected by the Act and balances all competing interests, including the national interest. To be clear, the proposed Amendments at **Attachment A** do not represent an attempt to exhaustively address our concerns with the Act. It merely reflects our views on a number of specific, targeted areas that we have identified as being of particular concern, including in this and our earlier Submissions, in order to assist the Committee as far as possible in its consideration of the Act.

In the body of this submission, we identify two additional issues in relation to the Act (among other concerns):

1. The risk previously stated by many industry providers that the legislation would damage Australian developers' and manufacturers' reputations in international markets, has now been realised. Australian based providers of information technology products and services are now regularly fielding questions regarding the impact of the Act on their installed products and in the context of prospective sales engagements. This situation is not aided by foreign competitors making use of the media and other material to improve their competitive position.

2. As a consequence of the perverse and inconsistent definitions of 'Systemic Weakness' and 'Systemic Vulnerability', the proposed legislation does, in fact, allow for actual "systemic weaknesses"[1] to be introduced into technology products and services.

In summary, even this limited analysis has identified major defects in the Bill that would see any of the potential benefits achieved by this proposed legislation far outweighed by the damage it would do to the nation's security, economy and internet-based services in addition to International reputation and trade. The Bill is so demonstrably flawed that the only practical option is to see it withdrawn. The Government should then review its primary objectives and commence genuine engagement and consultation with all stakeholders – including consumers, business, industry representatives, Technology & Communications Organisations (including Australian SMEs), Internet Standards bodies and academia in order to achieve a workable way forward.

[1] The use of the term "Systemic Weakness" here is to be interpreted in terms of its general meaning – not the perverse definition contained in the Act. For clarity, see Attachment A, Section 4.

SENETAS
Security without compromise

11 February 2019

1. The Act has damaged Australian developers' and manufacturers' reputations in international markets and the likelihood of the forecast negative impact on local technology R&D, Manufacturing, Start-Ups and Education now seem certain.

Extensive media coverage in local and foreign press has highlighted the nature of the legislation and the threat that it represents to other governments and commercial parties using or considering purchasing Australian technology products and telecommunications services (See **Attachment B**). Foreign Government have publicly stated their intentions to migrate off Australian cloud services. In addition, Australian companies are reporting that they are receiving requests from existing customers either asking for assurances or stating their intention to investigate the procurement of non-Australian products.

Evidence supporting this position

It is difficult to overstate the extent and impact of local and international media coverage on the Australian technology community, as a result of the passing of the legislation in December 2018. What follows is a brief summary of the coverage and consequences arising from the Act.

The New Zealand Government is reconsidering its policy of allowing its agencies to use Australian based cloud service providers. Clearly, there is significant concern by the NZ Government that sensitive and encrypted data, held in Australia and/or managed by Australian based companies, is potentially exposed by this legislation. This is eerily similar to the Australian Government's stance on the use of non-Australian based/hosted cloud services. It is also consistent with concerns expressed publicly by the Australian Government in its early Cloud Strategy/Policy documents regarding the US Patriot Act. As NZ firms are now lobbying to see such services repatriated, this will result in a loss of business for Australian based companies.

The Massachusetts Institute of Technology (MIT) has expressed a number of concerns about the legislation. In particular, that it could see local and international companies leave the Australian market. More worrying though, in its view, is that the back doors created as a result of the legislation will endanger internet users worldwide. It is not alone in holding this view.

The widely read and arguably most authoritative technology industry publication – ***Wired Magazine***, has named Australia's Attorney General, Christian Porter MP, as *"one of the most dangerous people on the internet in 2018"*. In commenting on his support for the legislation, *Wired* describes the passing of the legislation as *"a dangerous development on a global scale"* and places it alongside the actions of the Russian President in supporting state sponsored murder and hacking. Regardless of the fairness or otherwise of this comparison, *Wired*'s international 20 million readers now have a perspective about Australia's apparent disregard for their safety.

Coverage of the legislation has not been limited simply to the technology press. Numerous articles have appeared in major newspapers such as ***The New York Times*** (NYT). In an article published on 22 January 2019, the NYT suggested that Australia had damaged phone security for the entire world. Based on expert opinion from the Open Technology Institute, it went on to state that the legislation represented *"...an encryption back door for the U.S."* In doing so, the articled outlined how Australia had in effect compromised the First Amendment to the US constitution (Freedom of Speech). The article quoted several Australian citizens, including:

- Mike Cannon-Brookes, (founder of one of Australia's largest IT companies, Atlassian) - *"All of Australian technology is tarnished by it."*
- In the context of comparing the Act to the legislative actions by other nations, Michelle Price, CEO of Australia Cyber Security Growth Network (formerly Senior Advisor, Domestic Cyber Policy at PM&C) said that *"...Australia's version has gone much further."*

- Casey Ellis of Bugcrowd - *"People are factoring it in as a risk when you're looking at hiring an Australian now,"* and that *"It's causing a chilling effect around Australian companies."*
- Sarah Moran, CEO of Geek Girl Academy, in commenting on how drastically the legislation has undermined investment and education in technology, asked *"Why would I tell young girls to go build tech here if there's not going to be any tech industry?"*

There has been considerable commentary amongst the more influential business journals. Specifically:

- The Nasdaq report - identifies both the extraterritorial nature of the law and its implications to Australian based companies. *"The long-term effects of these laws will surely be felt by the local economy, as innovative businesses are forced overseas or out of business."*
- The Economist – suggests that larger US firms may choose to exit the Australian Market to avoid damaging their global reputation. Clearly, this perspective will likely now cause foreign corporations to pause before investing here.
- The Nikkei Asian Review – describes the legislation as a *"shock to the global tech community"* and a threat to *"privacy and security"*. It identifies the blatant contradiction between the aims of the legislation and Australia's actions in relation to Huawei & ZTE.

In the context of the business world, international credit and risk agency Fitch Solutions, was concerned that *"The new rules are negative for Australia's tech sector, but they will have the most impact globally, as they target international companies."* Fitch also expressed the view that *"Australia's unilateral decision is not the right way to proceed and will have an overall negative impact on security services."*

Finally, a very large number of international media articles reported on the short statement issued by the Reform Government Surveillance (RGS) coalition. The RGS represents many of the largest international technology companies – including Apple, Microsoft, Google, Facebook, Twitter, Dropbox and Linkedin. This statement described the legislation as undermining the cybersecurity, human rights and right to privacy of users. It also stated that the *"new Australian law is deeply flawed"*.

Implications

The accuracy of any of the above is entirely irrelevant. It is now a fact that citizens, businesses and governments across the world believe that, by passing this legislation, the Australian Government has fundamentally compromised their interests. As a consequence, trust in Australian companies operating in this market has been severely damaged. Amongst many other issues, Foreign Governments and competitors are already using this coverage as evidence that Australian information technology products and services are not to be trusted. This situation is compounded by foreign competitors making use of the media and other material to improve their competitive position in the marketplace. Sales are being lost, exports will decline, and local companies will fail or leave Australia. Jobs in this industry are threatened and related technical skills are likely to deteriorate.

It is difficult to forecast precisely the exact nature of the impact on industry, the economy, citizens and government. As it happens, we have a timely example of how government intervention in the technology area can have major economic and technology impacts. In their submissions to the PJCIS's review of the Bill last year, a number of parties made the point that the proposed legislation could have unintended consequences. Not only might these be unintended, they might also be unpredictable. The following example has a number of issues in common with the development and implementation of the Act.

Consider the announcement by TPG Corp in late January 2019, not to proceed with its proposed construction of Australia's 4th mobile phone/data network as a direct result of the Government's ban on the use of Huawei. Notwithstanding the validity or otherwise of the arguments related to this ban, the reality is that Australian businesses and citizens will now pay significantly more for mobile voice and data services given that decision by TPG which substantially lessens competition in the marketplace. As a price leader in this market, selling through its low-cost brands such as iiNet and WestNet, TPG has significantly contributed to a reduction in prices charged for these services. Further, given that TPG paid the Commonwealth more than $1.2 Billion for spectrum to support this network, it is now highly likely that the prices paid for future spectrum sales will be substantially lower than forecast.

While the potential for this type of outcome was predicted at the time of the Government's decision on Huawei, concerns by industry and others that this would lead to higher prices were largely dismissed by Government. We raise this example, not to question the decision behind the ban, but to expose the degree to which the consequences of such decisions are regularly downplayed or ignored. The commercial reality, and the implications for businesses and citizens in Australia, on the other hand are real and they hurt. While unintended consequences are regrettable, parties consciously choosing to ignore or gloss over known or forecast risks, need to be held accountable.

SENETAS
Security without compromise

11 February 2019

2. Despite claims to the contrary the proposed legislation does, in fact, allow for systemic weaknesses to be introduced into technology products and services.

During the course of the review of the Bill, the Government claimed that the proposed legislation would not compromise critical encryption systems or introduce any "systemic weaknesses" into products. This claim does not stand up to scrutiny. The supposed guarantees offered by Section 317ZG are undermined and made worthless by virtue of the perverse definition of "systemic weakness" and "systemic vulnerability" introduced without consultation with industry immediately prior to the legislation passing the lower house.

Evidence supporting this position

Notwithstanding extensive discussion concerning the absence of any definition of these terms during the course of the Committee's review of the Bill in late 2018, the Government amended the draft bill to introduce definitions for these terms immediately prior to the legislation passing the lower house. As far as we are aware, the wording of these definitions was developed without consultation with industry, and certainly does not reflect their common meaning.

To aid in understanding, the definitions as they appear in the Act at Section 317B are:

> ***systemic vulnerability*** *means a vulnerability that affects a whole class of technology, but does not include a vulnerability that is selectively introduced to one or more target technologies that are connected with a particular person. For this purpose, it is immaterial whether the person can be identified.*
>
> ***systemic weakness*** *means a weakness that affects a whole class of technology, but does not include a weakness that is selectively introduced to one or more target technologies that are connected with a particular person. For this purpose, it is immaterial whether the person can be identified.*

Firstly, these definitions are perverse. They bear no correlation with the common meaning of the terms as used by industry, academics or technology experts for decades.

As noted by the Law Council in its submission (#5), these definitions *"... simply allow for the introduction of any weakness or vulnerability as requested"* and *"their very intention is to introduce a diminution in security standards..."*.

It is as if the Government has chosen a definition of a well understood concept and refashioned it in such a way as increase the likelihood of the very risk that the industry was concerned about. The secrecy provisions of the Act not only further increase the likelihood of a real systemic weakness but complicate a response to correct it.

As noted in a number of submissions, including that of the Law Council, the phrasing of two equivalent sub-sections included in Section 317ZG (in respect of systemic weaknesses and systemic vulnerabilities respectively) would seem, in part, to include words closer to the normal use of the terms — but which arguably renders those sections inconsistent with the definitions of systemic weakness and systemic vulnerability at 317B.

> *"(4A) In a case where a weakness is selectively introduced to one or more target technologies that are connected with a particular person, the reference in paragraph (1)(a) to implement or build a systemic weakness into a form of electronic protection includes a reference to any act or thing that will, or is likely to, jeopardise the security of any information held by any other person."*

The explanations of the effect of these definitions offered by the Department of Home Affairs in its submission (#16) at pages 10 to 11, demonstrate a fundamental failure to understand the implications of these definitions to technology-based systems and services. While claiming to respond to industry's demands to introduce a definition, the Department again failed to consult on the definitions. These were fashioned at the last minute. The explanations offered in the submission also contain a number of contradictions. For example, Paragraphs 34 to 36 claim to limit the scope of any introduced vulnerability and that it *"...reinforces that a weakness or vulnerability may only be introduced to the particular technology that is used, or likely to be used by a particular person"*. Contrast this claimed limitation with Paragraph 40, which outlines precisely the contrary use *"The phrase 'for this purpose, it is immaterial whether the person can be identified' in the definitions in section 317B acknowledge the fact that some law enforcement investigations and national security exercises, while targeted, are not conducted in relation to a particular identified person."*

Importantly, as noted in our submission to the committee in November 2018, changes to communications systems and to any devices or technologies forming part of the supply chain of such systems (without undertaking extensive regression and integration testing) could lead to any number of unforeseen consequences resulting from an inability to follow standard software development and testing procedures, including the potential to compromise the wider security of those systems and potentially make them unstable. This includes, for example, the potential for large scale network outages impacting internet service in Australia and throughout the world.

As noted by Telstra, in their submission to the committee's review of the draft Bill, it *"covers the entire communications services supply chain, making it possible a TA Notice or TC Notice could require 'modification' to a piece of network equipment or its operating software without the knowledge or awareness of other communications providers. For example, if a telecommunications provider (such as a carrier or carriage service provider) uses equipment or software supplied by a third party, that third party may have been separately required to provide technical assistance to an agency (potentially including the installation of software or equipment supplied by the agency) or to introduce new technical capability into their products. Given the secrecy provisions of the Bill, this could occur without the knowledge of the telecommunications provider and could result in an adverse impact to its network and/or customers' use of the network. Such adverse effects could include service degradation, network faults, or other impacts on its business, or on non-target customers."*

There is simply no way that an individual provider, supplying a single element of an integrated system, could possibly have visibility of the implications of making changes to their product on other elements of a complex system. Over time, the risk of a small, and otherwise insignificant, change to a component of the network resulting in catastrophic failure is high. The consequences to all parties (including government) are unpredictable. The existing definition completely fails to recognise this risk. More serious though, is that even were such a risk identified, the existing definitions would not necessarily prevent an agency proceeding to enforce a TCN.

Implications

Failing to recognise the true meaning of a Systemic Vulnerability and Systemic Weakness within the context of the Act, and to treat it accordingly, exposes every technology user to quite unpredictable consequences. The fact that the definitions included in the Act are inconsistent (both with the terminology and understanding of industry and experts, and with the provisions of the Act itself), are complex, and difficult to understand also means that the Act itself suffers from ambiguity and difficulties in interpretation, giving rise to further issues in respect of both enforcement by government and compliance by industry.

In an effort to assist, **Attachment A** includes revised definitions at Section 4 for the consideration of the Committee.

SENETAS
Security without compromise

ATTACHMENT A

Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 – Some Proposed Changes to Aspects of the Legislation

1 Introduction

This attachment reflects our views on several specific, targeted areas that we have identified as being of particular concern, including in this and our earlier Submissions, in order to assist the Committee as far as possible in its consideration of the Act.

However, notwithstanding the specific comments and proposed amendments set out below, we continue to strongly urge the Government to reconsider the Act in its entirety as part of a collaborative consultation process which takes into account the views of all relevant stakeholders and persons that may be affected by the Act and balances all competing interests, including the national interest.

2 Overview of our comments

The comments set out below are drafted as proposed amendments to the Act.

Text that is:

- proposed to be deleted is ~~in strikethrough and in red text~~; and
- proposed to be inserted is underlined and in blue text.

Due to the size of the Act and the specific and targeted nature of this letter, please note that our comments are confined to Schedule 1 (and the associated Part 15 of the *Telecommunications Act 1997* (Cth)).

Our amendments are proposals only, and would of course benefit from broader consideration and consultation as noted in section 1 of this letter above.

3 Scope of coverage

3.1 Designated communications providers

We propose the insertion of the following definitions in section 317B, as well as the following new section 317ZGB of the Act:

317B Definitions

In this Part:

…

critical infrastructure systems means any or all of the domain name system (DNS), the border gateway protocol (BGP), the internet protocol suite (TCP/IP), a public key infrastructure (PKI), or [others to be inserted following consultation].

…

317ZGB Designated communications provider must not be required to do specified acts or things in respect of certain systems etc.

(1) A technical assistance request, technical assistance notice or technical capability notice must not have the purpose or effect of requiring a designated communications provider to do any specified acts or things (other than the acts or things listed in subsections 317E(1)(d) and 317E(1)(g)) in respect of:

SENETAS
Security without compromise

ATTACHMENT A

(a) any critical infrastructure systems; or

(b) any other system for which the designated communications provider holds a permit under Part 2 of the *Defence Trade Controls Act 2012* or regulation 13E under the *Customs Act 1901*.

(2) A technical assistance request, technical assistance notice or technical capability notice has no effect, and will cease to be a technical assistance request, technical assistance notice or technical capability notice (as applicable) for the purposes of this Part, to the extent (if any) to which it would have an effect covered by paragraph (1)(a) or (b).

(3) For the purposes of subsection (5), ***this Part*** includes any other provision of this Act, so far as that other provision relates to this Part.

Explanation of proposed amendments

The above amendments seek to recognise that there are certain systems (please refer to the associated proposed definition of system in section 4 below) that are of such importance, both to Australia and more globally, that the regime in Part 15 should not extend to them.

We also endorse the comments made by a number of participants with respect to the need to revisit and narrow the list of designated communications providers and associated eligible activities in section 317C, and in particular those listed in items 8, 10–11 and 14–15.

3.2 Listed and specified acts or things

We endorse the comments made by a number of participants with respect to the need to revisit and narrow the acts or things listed in section 317E, including references to undefined terms such as 'technical information'.

In addition, we support proposals to make the scope of the 'specified acts or things' the subject of a technical assistance request, a technical assistance notice or a technical capability notice exhaustive and only capable of expansion via legislative amendment. That is, we propose to:

- replace the words 'include (but are not limited to)' with 'must be' in of section 317G(6), to mirror the amendments previously made in sections 317L(3) and 317T(7); and
- delete subsection 317T(5), and associated sub-sections (4)(c)(ii) and (6).

4 Systemic weaknesses and systemic vulnerabilities

We propose the deletion of the definitions of 'target technology', 'systemic vulnerability' and 'systemic weakness' previously inserted in the Act, and the insertion of the following alternative definitions in section 317B, as well as the following amendments to section 317ZG of the Act:

317B Definitions

In this Part:

…

related system means, in respect of a system, any other system that:

(a) forms part of, or is otherwise connected to, that system; or

(b) is dependent, interdependent or otherwise reliant upon that system, or on which that system is dependent, interdependent or otherwise reliant, for the proper functioning of either or both of that system or the other system.

SENETAS
Security without compromise

ATTACHMENT A

software means all computer programs and programming (including source code, object code and microcode), middleware, firmware, sub system software, operating systems, database management systems, system utilities and all software tools, methodology, associated documentation and media on which software is stored.

system means any current or proposed system, network, hardware, software, product or service (including any components or parts of such system, network, hardware, software, product or service).

systemic weakness means a weakness in any system that will or might extend beyond the specific instance or device forming part of that system that is the subject of a technical assistance request, technical assistance notice or technical capability notice in a manner that will or might impact:

(a) any related systems (including the security, functionality, performance or reliability of such other systems);

(b) other users of the system or other systems;

(c) the information or data of any users of the systems or related systems (including the security, accuracy or reliability of such information or data); or

(d) the integrity or reliability of any activities, processes, tools or methodologies that are integral to the security, functionality, performance or reliability of that system and any related systems.

systemic vulnerability means a systemic weakness that can be exploited to perform unauthorised actions that will or might impact a system or one or more users of that system, product or service.

…

317ZG Designated communications provider must not be required to implement or build a systemic weakness or systemic vulnerability etc.

(1) A technical assistance request, technical assistance notice or technical capability notice must not have the purpose or effect of:

(a) requiring a designated communications provider to implement or build a systemic weakness, or a systemic vulnerability~~, into a form of electronic protection~~; or

(b) preventing a designated communications provider from rectifying a systemic weakness, or a systemic vulnerability~~, in a form of electronic protection~~.

(2) The reference in paragraph (1)(a) to implement or build a systemic weakness, or a systemic vulnerability, ~~into a form of electronic protection~~ includes a reference to implement or build a new decryption capability ~~in relation to a form of electronic protection~~.

(3) The reference in paragraph (1)(a) to implement or build a systemic weakness, or a systemic vulnerability, ~~into a form of electronic protection~~ includes a reference to one or more actions that would render ~~systemic~~ methods of authentication or encryption less effective.

(4) Subsections (2) and (3) are enacted for the avoidance of doubt.

~~(4A) In a case where a weakness is selectively introduced to one or more target technologies that are connected with a particular person, the reference in paragraph (1)(a) to implement or build a systemic weakness into a form of electronic protection includes a reference to any act or thing that will, or is likely to, jeopardise the security of any information held by any other person.~~

~~(4B) In a case where a vulnerability is selectively introduced to one or more target technologies that are connected with a particular person, the reference in paragraph (1)(a) to implement or build a systemic vulnerability into a form of electronic protection includes a reference to any act or thing that will, or is likely to, jeopardise the security of any information held by any other person.~~

~~(4C) For the purposes of subsections (4A) and (4B), an act or thing will, or is likely to, jeopardise the security or information if the act or thing creates a material risk that otherwise secure information can be accessed by an unauthorised third party.~~

(5) A technical assistance request, technical assistance notice or technical capability notice has no effect, and will cease to be a technical assistance request, technical assistance notice or technical capability notice (as applicable) for the purposes of this Part, to the extent (if any) to which it would have an effect covered by paragraph (1)(a) or (b).

(6) For the purposes of subsection (5), ***this Part*** includes any other provision of this Act, so far as that other provision relates to this Part.

Explanation of proposed amendments

The above amendments seek to:

- define 'systemic weakness' and 'systemic vulnerability', including in line with similar submissions made both in writing and in public hearings; and
- clarify the application of section 317ZG(5), and the meaning of a notice (or request) having 'no effect' under the Act.

We strongly support and endorse the comments made in other submissions in relation to the definitions included in the Act shortly before its passage, as well as the corresponding sections 317ZG(4A) to (4C), in particular with respect to their ambiguity and inconsistency (and associated difficulties with interpreting and understanding their effect). Our proposals accordingly aim to clarify, consolidate and harmonise the provisions (and definitions) applying to systemic weaknesses and vulnerabilities.

5 Transparency and disclosure

We endorse the comments made by the Law Council of Australia in relation to the authorisation of disclosures of information in relation to a TAR, TAN or TCN, in particular to require that certain requests for disclosure under sections 317ZF(14)–(16) must be authorised unless certain conditions are met.

6 Use of TARs, TANs and TCNs

Our comments in this section 6 should be considered in conjunction with section 7.1 of this letter below, and in particular our concerns with respect to the need for independent judicial review and oversight of Part 15.

6.1 Distinctions between TANs and TCNs

We propose the following amendments to section 317L(2A) of the Act:

317L Technical assistance notices

...

(2A) The specified acts or things must not be directed towards ensuring, and a technical assistance notice will have no effect to the extent that it would require, that a designated communications provider is capable of giving help to ASIO or an interception agency where the designated communications provider is (as at the date the technical assistance notice is given) not already capable of giving such help.

SENETAS
Security without compromise

ATTACHMENT A

Explanation of proposed amendments

We appreciate the introduction of section 317L(2A) in the Act, however propose the above amendments in order to better clarify the application of technical assistance notices as distinct from technical capability notices.

We also support the general comments made in other submissions requesting that the 'graduated' nature of technical assistance requests, technical assistance notices and technical capability notices be made more clear.

6.2 Criteria for issuance

We propose the following amendments to section 317P of the Act, as well as equivalent amendments to sections 317JAA, 317JA(11)–(14), 317Q(10), 317V and 317X(4):

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.

Note: See also section 317RA.

We also propose that Division 2 of Part 15 include an equivalent provision with respect to the criteria for issuance of a technical assistance request.

In relation to the associated provisions 317RA, 317JC and 317ZAA, we propose the following equivalent amendments to all sections:

317RA Whether requirements imposed by a technical assistance notice are reasonable and proportionate

The following matters will be relevant to any determination of ~~In considering~~ whether the requirements imposed by a technical assistance notice or a varied technical assistance notice are reasonable and proportionate~~, the Director-General of Security or the chief officer of an interception agency, as the case requires, must have regard to the following matters~~:

(a) the interests of national security; and

(b) the interests of law enforcement; and

(c) the legitimate interests of the designated communications provider to whom the notice relates (including, but not limited to, commercial and reputational interests); and

(d) the objectives of the notice; and

(e) the availability of other means to achieve the objectives of the notice; and

(ea) whether the requirements~~, when compared to other forms of industry assistance known to the Director-General of Security or the chief officer, as the case requires,~~ are the least intrusive ~~form of industry assistance~~ means to achieve the objectives of the notice so far as the following persons are concerned:

(i) persons whose activities are not of interest to ASIO; and

(ii) persons whose activities are not of interest to interception agencies; and

SENETAS
Security without compromise

ATTACHMENT A

(eb) whether the requirements are necessary; and

(f) the legitimate expectations of the Australian community relating to confidentiality in communications, privacy and cybersecurity; and

(g) whether the notice will require the designated communications provider to do (or fail to do) any acts or things that may contravene section 317ZG.

~~(g) such other matters (if any) as the Director-General of Security or the chief officer, as the case requires, considers relevant.~~

Explanation of proposed amendments

The above amendments seek to ensure that the criteria for issuance of technical assistance requests, technical assistance notices and technical capability notices are clear, objective and directed towards ensuring that the request or notice (as applicable) do not go further than necessary in order to achieve their objectives (that is, that there is no less restrictive means to do so).

As previously noted in other submissions and public hearings, and as subsections (e), (ea) and (eb) already recognise, there may be a number of other means to achieve the objectives of the notice. Given the risks raised by the regime in Part 15, as described in our and other submissions, the above amendments seek to ensure that the regime in Part 15 is specific and targeted.

7 Assessment and review

7.1 Judicial review under Part 15

We reiterate the concerns raised in a number of submissions with respect to the lack of independent judicial oversight and review of technical assistance requests, technical assistance notices and technical capability notices under Part 15. We have not sought to incorporate detailed amendments to the Act in this letter, as such amendments would need to be made comprehensively and consistently throughout the Part.

Our proposals, expressed at a principle level, are that:

(a) the decision to issue technical assistance notices and technical capability notices should be made by an independent judicial authority (as is the case under *UK Investigatory Powers Act 2016*);

(b) the relevant requesting agency should be required to provide evidence to the judicial authority in relation to its request, reflecting the satisfaction of objective criteria consistent with existing sections 317P and 317V, noting our comments in section 6 of this letter above in this respect; and

(c) the Act should include comprehensive and robust review processes available to designated communications providers who receive technical assistance notices and technical capability notices (including, where the recommendation in paragraph (a) above is not adopted and at a minimum, judicial review of decisions made under Part 15 under the *Administrative Decisions (Judicial Review) Act 1977* (Cth)).

We also endorse comments made in other submissions with respect to the adequacy of review mechanisms already specified in the Act for TCNs, including the considerations applicable to ministerial approval in section 317TAAA and 317XA, and the consultation, assessment and reporting processes in sections 317W and 317WA.

8 Other provisions

As noted above, the comments set out in this Attachment are specific and targeted, and do not exhaustively address all of our concerns in relation to the Act. We note that many of these concerns have been covered in other submissions, including our Submissions, in relation to areas such as the conferral of immunity under the Act.

SENETAS
Security without compromise

ATTACHMENT B

Sample media coverage in local and foreign press that has highlighted the nature of the legislation and the threat that it represents to other governments and commercial parties using or considering purchasing Australian technology products and telecommunications services.

https://www.stuff.co.nz/technology/109402792/nz-officials-consider-impact-of-australias-controversial-encryption-law

https://www.technologyreview.com/the-download/612562/this-is-how-australias-ban-on-encryption-could-endanger-us-all/

https://www.wired.com/story/most-dangerous-people-on-internet-2018/

https://www.nasdaq.com/article/australias-controversial-encryption-legislation-may-threaten-more-than-online-privacy-cm1067566

https://www.economist.com/asia/2018/12/15/an-australian-law-to-expose-vice-annoys-the-tech-world

https://asia.nikkei.com/Politics/Australia-shocks-global-tech-community-with-anti-encryption-law

https://www.scmp.com/business/companies/article/2179252/australias-new-telecom-bill-allowing-law-enforcement-access

https://www.smh.com.au/technology/negative-for-tech-sector-fitch-slams-australia-s-new-encryption-laws-20181213-p50m55.html

http://www.reformgovernmentsurveillance.com/rgs-statement-on-the-australian-parliaments-passage-of-assistance-and-access-bill/

https://www.nytimes.com/2019/01/22/technology/australia-cellphone-encryption-security.html

https://www.innovationaus.com/2019/02/AA-laws-killing-us-overseas