31 October 2018

**Parliamentary Joint Committee on Intelligence and Security**
By email to: Committee, PJCIS (REPS) <pjcis@aph.gov.au>

**TELECOMMUNICATIONS AND OTHER LEGISLATION AMENDMENT (ASSISTANCE AND ACCESS) BILL 2018 – BSA RESPONSE ON "SYSTEMIC WEAKNESS"**

BSA | The Software Alliance (**BSA**) thanks the Parliamentary Joint Committee on Intelligence and Security (**Committee**) for the opportunity to appear before it during the public hearing on 19 October 2018, and to share the views of BSA and our members on the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (**Bill**).

During the hearing, the Committee requested that BSA take on notice the issue of the definition of "systemic weakness", as used in the new section 317ZG that the Bill proposes to insert into the Telecommunications Act 1997 (**Section 317ZG**). We set out our response below.

## General Comments

BSA's members[1] rely on essential security technologies, such as encryption, to protect customers from cyber threats, while delivering cutting-edge data-driven advancements in emerging areas such as artificial intelligence, machine learning, cloud-based analytics, and the Internet of Things. Therefore, while BSA and our members continue to acknowledge and support the Australian Government's desire to have more powerful tools to aid in the fight against criminal and terrorist activities, we also urge the Australian Government to ensure that improvements to law enforcement access are not made at the expense of privacy, security, and, most importantly, trust in the technologies and tools that underpin the digital economy.

It remains the considered view of BSA and our members that any weakness or vulnerability in a system, regardless of how it is limited or controlled, could be exploited by bad actors with the requisite technological knowledge and means. As such, if the powers under the Bill were exercised to require a weakness or vulnerability to be created or implemented into any system for the purposes of accessing data, then whether or not the weakness or vulnerability relates directly or otherwise to a form of electronic protection, that vulnerability or weakness could be exploited in a manner that puts the data of everyone who uses that technology at risk. Many of the large-scale cyber breaches today originate from the compromise of a small vulnerability that allows the attacker to gain an initial foothold to launch more malicious attacks.

[1] BSA's members include: Adobe, Akamai, Amazon Web Services, ANSYS, Apple, Autodesk, AVEVA, Baseplan Software, Bentley Systems, Box, CA Technologies, Cad Pacific/Power Space, Cadence, Cisco, CNC/Mastercam, DataStax, DocuSign, IBM, Informatica, Intel, MathWorks, Microsoft, Okta, Oracle, PTC, Salesforce, SAS Institute, Siemens PLM Software, Slack, Splunk, Symantec, Synopsys, Trend Micro, Trimble Solutions Corporation, and Workday.

300 Beach Road
#25-08 The Concourse
Singapore 199555

P: +65 6292 2072
F: +65 6292 6369
W: bsa.org

Regional Representative Office
UEN: S97RF0005K

**Proposed Amendments to Section 317ZG**

It is nonetheless BSA's and our members' desire to remain as responsive and helpful as we can to the Committee's deliberations on the matter. Accordingly, we offer the following proposed amendments to Section 317ZG for the Committee's consideration:

*(Red double-underlined text = text to be added; red struck-through text = text to be deleted)*

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

(1) A technical assistance notice or technical capability notice must not have the 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 a ~~systemic~~ method~~s~~ of authentication or encryption less effective.

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

(5) A technical assistance notice or technical capability notice has no effect to the extent (if any) to which it would have an effect covered by paragraph (1)(a) or (b).

(6) In this [section][Part]:

***system*** includes product, service, and component.

***systemic weakness*** means a weakness in a system that extends, or carries the risk of being extended, beyond a targeted system in a manner that affects:
(a) other systems;
(b) the integrity of activities or processes, including patch management or configuration, that are integral to the functionality or security of other systems; or
(c) other users of the targeted system or other systems.

***systemic vulnerability*** means a systemic weakness that can be exploited to negatively impact a system or a user of the system.

These proposed amendments represent our attempt at providing a definition for "systemic weakness", and the related "systemic vulnerability", while giving effect to our recommendation (in our 12 October 2018 submission to the Committee) that the "systemic weakness" carve-out should be broadened to include *any weakness or vulnerability* in *any system, product, service, or component*.

We would welcome the opportunity to continue refining the language above in discussion and collaboration with the Committee and the relevant Government stakeholders.

## Conclusion

As previously noted in our 12 October 2018 submission to the Committee, the Bill and the issues relating thereto are complex and sensitive. In addition to the comments and proposals above, BSA would again like to commend, for the Committee's consideration, the other recommendations in our 12 October 2018 submission, including that:

1. the assistance and access regime should be underpinned by judicial authorization and a review process, wherein decisions to issue mandatory notices are made only by an independent judicial authority, and a robust and transparent review mechanism is available to the subjects of such notices; and

2. the scope of the Bill should be narrowed with respect to:
    a. the "acts or things" that can be required from a service provider;
    b. the scope of the circumstances in which the powers under the Bill can be exercised; and
    c. the application of the Bill to "designated communications providers", both in terms of extraterritorial effect and the types of organizations that are subject to the Bill.

In relation to recommendation 1 above, even with the proposed definition of "systemic weakness" above, there still needs to be a determination of when a weakness extends, or carries the risk of being extended, beyond a targeted system. Given the complexity involved in making such a determination, this would be yet another reason for why technical assistance notices and technical capability notices under the Bill require independent judicial authorization and a review process; and why the determination should not be made by a member of the executive involved in issuing such notices due to the inherent conflict of interest.

We again respectfully encourage the Australian Government to engage in further dialogue with industry to consider the broader issues at play and the implications (and possible unintended consequences) of the Bill.

BSA and our members remain at the disposal of the Committee and the Australian Government to participate in any industry and stakeholder groups, not only to continue refining the proposed Section 317ZG language above, but also to help develop and deliver other enduring solutions to address the challenges of accessing evidence in the digital age.

If you require any clarification or further information in respect of this submission, please contact the undersigned at darrynl@bsa.org or +65 6292 0680.

Yours faithfully,

Darryn Lim
Director, Policy – APAC