Cisco Systems, Inc.
170 West Tasman Dr.
San Jose, CA 95134
USA
+1.408.526.4000
+1.800.553.6387
www.cisco.com

October 12, 2018

The Secretary
Parliamentary Joint Committee on Intelligence and Security
Parliament House
Canberra ACT 2600
Australia

Submitted electronically

Dear Secretary,

Thank you for the opportunity to provide comments on the *Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018* "The Assistance and Access Bill 2018" ("the Bill"). While we appreciate the important law enforcement goals that spurred the Bill, we have grave concerns about certain aspects of the proposed legislation.

Cisco is the world leader in building the infrastructure of the global internet and has provided a significant portion of the switches, routers, and other equipment used by Australian telecommunications service providers and enterprises. The interconnected nature of the global economy, driven by this infrastructure over the last thirty years, has provided enormous benefits to the Australian people and the enterprises they have created. At the same time, there are costs as well as benefits that come with increased connectivity between Australia and the rest of the world. The work of law enforcement and national security agencies globally has both been boosted and also complicated by the rise of new Internet-based communications.

It is both necessary and reasonable, therefore, for the people of each nation and their governments to periodically review the scope and reach of electronic surveillance laws to ensure that a proper balance exists between various dimensions of security in tension with one another. Given the complex nature of the global communications ecosystem and the potential impact on both civil liberties and the security of those communications, it is essential that such reviews occur in an open and participatory

Cisco Systems, Inc.
170 West Tasman Dr.
San Jose, CA 95134
USA
+1.408.526.4000
+1.800.553.6387
www.cisco.com

manner. It is also essential that we avoid the false dilemma of trade-offs between privacy and security.

With this in mind, we write to express serious reservations, outlined below, regarding various provisions in the Bill pending before Parliament that threaten to undercut sustained efforts by Cisco and others to develop, deploy, and maintain technologies that are secure, trustworthy, transparent, and accountable. Other governments will likely follow the example Australia sets in this Bill. We are concerned that some of those other governments may not have Australia's commitment to restraint in the exercise of executive power. Without further amendment, we believe the net result of these changes would harm the security interests of Australia by setting a precedent that could be adopted by less liberal regimes. We, therefore, ask that the Parliament consider several important changes outlined below before the Bill advances further.

Cisco was founded in 1984 from path-breaking work by its founders to address disparate local area network protocols that made communication extraordinarily clumsy between disparate computer systems, if not impossible. In solving that challenge, the multi-protocol router was born. Our past is rooted in connectivity, and our future is being built around it. Our people, products, and partners help society securely connect and seize tomorrow's digital opportunity today.

Cisco has a long commitment to working with the Australian government, including many elements now within the Department of Home Affairs and the Australian Cyber Security Centre. This includes a more than 20-year commitment to Australian government certifications, such as Common Criteria and the Australian Signals Directorate's Cryptographic Evaluation and Evaluated Products program. Additionally, we formally and informally engage with elements of the ACSC in policy development and revision including the ISM (Information Security Manual) and cloud consumption guidance for government.

Cisco is committed to maintaining and improving the security posture of all Australians and has cyber threat intelligence and information sharing arrangements with ASD and CERT Australia (now ACSC). Additionally, we have provided industry

Cisco Systems, Inc.
170 West Tasman Dr.
San Jose, CA 95134
USA
+1.408.526.4000
+1.800.553.6387
www.cisco.com

placements to ASD and Department of Defence staff into our own Cisco CSIRT and security teams to share best practice and assist with building peer relationships between security practitioners in government and industry.

Cisco works with law enforcement agencies both in Australia and globally and has recently signed an agreement with INTERPOL to share threat intelligence as the first step in jointly fighting cybercrime and supporting secure connectivity around the world. In addition, Cisco played an active role in securing and protecting the 2018 Gold Coast Commonwealth Games as the official networking partner and provided several specialist security staff to help support the Games' Security Operations Centre.

Cisco is also a foundation level partner with the Australian Cyber Cooperative Research Centre. Cisco maintains a board position on the CRC and leads one of the two research streams focused on Critical Infrastructure Protection and maintaining secure connectivity.

This notion of secure connectivity is core not only to Cisco's history, but its mission. Our customers, including the Australian government and the very agencies that are seeking some of the legislative changes reflected in the Bill, depend on it. Foundational to the willingness of the people, businesses, and governments to use Internet-based communications is this notion of trust, which in turn requires commitments to trustworthiness, transparency, and accountability.[1] Trust must be continually earned and can easily be wiped away. It is, therefore, vital that we can say, as Chuck Robbins has unequivocally stated, "We don't provide backdoors. There is no special access to our products."[2]

We agree with the Minister for Home Affairs and the Australian government about the importance of encryption to secure communications. As the Minister noted in his second reading speech for the Bill on 20 September 2018, "Encryption underpins modern information and communication technology. It is a tool that protects

[1] Information demonstrating the trustworthiness of Cisco technology, including Cisco's Trust Principles can be found here: https://trust.cisco.com,

[2] https://www.zdnet.com/article/cisco-ceo-robbins-there-are-no-backdoors-in-our-products

Cisco Systems, Inc.
170 West Tasman Dr.
San Jose, CA 95134
USA
+1.408.526.4000
+1.800.553.6387
www.cisco.com

personal, commercial and government information and supports confidence in a secure cyberspace. These technologies allow us to confidently transact online and to use the Internet for services such as banking and shopping." Strong encryption does all these things and more—including ensuring critical systems that deliver food, water, transportation services, health, telecommunications and energy are effectively secured against interruption and attack. As the Australian government knowns well, the threat of such attacks is one of the greatest issues that nations face today.

Areas of Concern

Cisco considers that continued trust in the reliability of encryption requires consideration of the further changes to the Bill described below.

The Bill seeks to introduce two new authorities that warrant further distinction as the legislation moves forward—Technical Assistance Notices ("TAN") and Technical Capability Notices ("TCN"). As we read the Explanatory Memorandum ("EM"), these authorities are intended to be distinct in that TANs represents a mechanism whereby the government can request assistance in the form of steps that a Designated Communications Provider ("DCP") can already take; whereas, TCNs represent a pathway for the government to demand the development of new surveillance capabilities. The latter is more problematic.

It is clear in the text of the Bill that there are important limitations on the scope of these notices intended to avoid harming the security of encryption unduly. In particular, the Bill explicitly states that neither a TAN nor a TCN may either 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.*

Cisco Systems, Inc.
170 West Tasman Dr.
San Jose, CA 95134
USA
+1.408.526.4000
+1.800.553.6387
www.cisco.com

We applaud the inclusion of prohibitions on the creation of systemic weaknesses and vulnerabilities. However, we recommend the following changes to the TAN and TCN authorities, which we believe are necessary to fulfil the stated intent of these provisions:

Checks and Balances

Both authorities suffer from a lack of checks and balances desirable to ensure that the steps demanded are both "reasonable and proportionate." In the case of a TAN, it is the head of an agency, and in the case of a TCN, it is the Attorney-General, who weighs the factors and makes the decision. In neither case is a court involved in either authorizing the issuance of the notice or in hearing a challenge raised by the DCP. For example, if a DCP believes that the steps required under a TAN are not within its existing capabilities and would require a new capability, it should be able to seek relief from the courts. Similarly, if a DCP believes that less intrusive mechanisms–i.e., one less likely to result in a systemic weakness–could be employed to achieve the government's aims, there should be a clearly-defined appeal mechanism. The process included in Section 317W, whereby an outside party can be engaged to assess and report on whether a TCN would lead to the creation of a systemic weakness or vulnerability, is inadequate, as it does not spell out a power to seek an appeal to the courts. The text of the Bill seems to leave the decision about whether or not a TCN is appropriate in its scope ultimately within the discretion of the Attorney-General.

Transparency

There is a significant issue with regard to transparency around the use of the TAN and TCN authorities. It is understandable that with regard to executing a criminal warrant, the government would demand confidentiality from the DCP during the criminal investigation. The annual reporting requirements in the Bill provide some transparency around the frequency of such requests. However, DCPs should have greater freedom to report on the nature, number, and scope of TANs they receive annually.

Cisco Systems, Inc.
170 West Tasman Dr.
San Jose, CA 95134
USA
+1.408.526.4000
+1.800.553.6387
www.cisco.com

More disconcerting is the notion that DCPs might be prevented under the Bill from publicly reporting the development of anew surveillance capability mandated by a TCN. Specifically, Section 317E provides that:

> *An act or thing done to conceal the fact that any thing has been done covertly in the performance of a function, or the exercise of a power, conferred by a law of the Commonwealth, a State or a Territory, so far as the function or power relates to:*
>
> > *(i) enforcing the criminal law and laws imposing pecuniary penalties; or*
> > *(ii) assisting the enforcement of the criminal laws in force in a foreign country; or*
> > *iii) the interests of Australia's national security, the interests of Australia's foreign relations or the interests of Australia's national economic well-being.*

While this paragraph of the Bill also notes that it cannot be used to force DCPs to make misleading statements or to engage in dishonest behaviour, these could easily be the result of forcing the surreptitious creation of surveillance capabilities. In this regard it is important to recognise that, as a matter of law, silence can render prior statements made by the DCP about the existence or lack of surveillance features to be misleading.

As noted above, Cisco has clearly declared to the public that we do not have backdoors in our technologies. Cisco's Chief Security and Trust Officer, John Stewart has clearly defined what we consider to be the distinctions between a feature, a bug, and backdoor.[3] In brief, "features" must be intentionally created and transparently reported. By contrast, "bugs" are unintentionally created. Once they are discovered, we handle them using international standards pursuant to a publicly described Product Security Incident Response process.[4]

---

[3] https://blogs.cisco.com/security/features-bugs-and-backdoors-the-differences-how-language-can-be-misused-and-a-word-of-caution

[4] https://tools.cisco.com/security/center/resources/security_vulnerability_policy.html

Cisco Systems, Inc.
170 West Tasman Dr.
San Jose, CA 95134
USA
+1.408.526.4000
+1.800.553.6387
www.cisco.com

We have defined a "backdoor" to include any surveillance capability that is intentionally created and yet not transparently disclosed. To the extent that the Bill would require via a TCN the creation of a capability while simultaneously preventing the DCP from documenting the existence of that capability, the law would result in the creation of backdoors. Building an undisclosed surveillance function—even if mandated by law and intended for use only in specific instances pursuant to a lawfully issued judicial warrant—would violate our public pronouncements to the contrary.

To be clear, Cisco does not accept that the concept of a "backdoor" should be narrowly construed to mean a universal mechanism for removing decryption or other forms of electronic protection applied to communications. To maintain the trust of its customers, Cisco believes that any form of surveillance technique which is implemented in its products must be publicly disclosed. Cisco is most certainly not alone in having foresworn the existence of backdoors in technology products and services. As such, this issue is a significant concern that should be promptly addressed via an amendment to the Bill.

Australian communication providers today are subject to the Telecommunications (Interception and Access) Act. Cisco, as a supplier of equipment to these providers, provides the statutorily mandated Lawful Intercept ("LI") capability in relevant platforms. Cisco policy requires that any such LI capability is globally available and built to international standards. This ensures that LI features are not customized on a per market basis. Furthermore, mindful of the distinction drawn above between a "feature" and a "backdoor," we require any LI feature to be publicly and transparently described in the product documentation. We, therefore, strongly believe that amendments to the Bill are necessary to realign its terms with current LI practice globally. This will ensure that the existence of an LI capability is known to the customer even if the *operational* use of that feature during the pendency of a lawfully authorized government investigation may be subject to restrictions regarding notice.

Extraterritorial Application

As this government recognizes and the text of the Bill clearly states, technology is global, and, therefore, technology policies must too be global. In his second reading

Cisco Systems, Inc.
170 West Tasman Dr.
San Jose, CA 95134
USA
+1.408.526.4000
+1.800.553.6387
www.cisco.com

speech on 20 September 2018, the Minister noted that "the supply of communications is a global industry. With major technology providers headquartered overseas, we must work with international partners to adapt to a world characterised by ubiquitous encryption." While the Minister's stated goal is to promote international cooperation in response to concerns about the impacts of encryption on the ability of governments to protect their citizens, this Bill as drafted could have the opposite unintended effect.

The language in the Bill is so broad that it could have the impact of fuelling cross-border application of statutes in ways that create untenable conflicts of laws for multinational companies. Merely providing immunity from civil suit in Australian courts is in no way the solution to this problem. Instead, the Parliament should pursue avenues that limit the application of Australia's laws to technologies in a manner that avoids adversely impacting their design, development, and use globally.

Free-flows of data across borders are important to the continued economic growth of Australia. Therefore, Australia should be wary of adopting country-specific mandates, including those that might inadvertently undermine access to strong encryption. That path would harm the global competitiveness of Australian enterprises and slow their access to new innovations in technology.

The thresholds in the Bill determining when it applies to DCPs that do business in Australia are far too broad. For example, Section 317C states that a DCP includes "an electronic service that has one or more end-users in Australia." The provision should limit its application to companies that either express a clear intent to reach customers in Australia or those exhibiting some degree of constructive knowledge or awareness about serving customers in the country. In addition, demands for TCNs should not be permitted to require the creation of capabilities that impact the security of users beyond Australia's borders. Any other result will undoubtedly point in the direction of adversarial governments each demanding the creation of surveillance capabilities that must be kept secret from the other.

Cisco Systems, Inc.
170 West Tasman Dr.
San Jose, CA 95134
USA
+1.408.526.4000
+1.800.553.6387
www.cisco.com

Mutual Legal Assistance

We view as highly favourable the notion that governments will work cooperatively across borders in order to combat crime and terror. The EM issued by the Parliament notes this point:

> *These powers recognise the fact that computers, communications and encryption are now global and perpetrators of crimes and terrorist acts have a global reach through these mediums. This will be based on the principle of reciprocity - that Australia will work with those who work with Australia - and any other conditions the Attorney-General deems appropriate.*

At the same time, we view it as vital that such arrangements not become a pathway for circumvention of national laws that protect civil liberties. Therefore, we recommend that the Australian government clearly articulate that as a matter of policy: 1) the Australian government will not meet requests that it knows to violate restrictions on surveillance in the requesting country; and 2) Australian authorities will not request assistance from other national governments that would violate laws restricting surveillance authorities in Australia.

Vulnerability Handling and Disclosure

The EM appears to espouse a troubling view regarding unpatched vulnerabilities in Section 317ZG(1), which was ostensibly intended to provide reassurance about the inability of the government to mandate the creation of systemic weaknesses or vulnerabilities. Paragraph 259 helpfully notes that TANs and TCNs "cannot be used to prohibit a provider from fixing flaws across their services or devices." However, the very next paragraph continues that "a requirement to disclose an existing vulnerability is also not prohibited by 317ZG(1)(a)." The Bill and the EM should either strike this reference or clearly restrict its application to vulnerabilities that have previously been disclosed to the public. As written, the Australian government, and others who will emulate the approach, could potentially demand access to undisclosed, *unpatched* vulnerabilities—leading to the development of zero-day exploits.

Cisco Systems, Inc.
170 West Tasman Dr.
San Jose, CA 95134
USA
+1.408.526.4000
+1.800.553.6387
www.cisco.com

The Bill further provides Australian authorities with new powers to engage in remote access searches and seizure of evidence on computers—and expands existing authorities for the Australian Security Intelligence Organisation (ASIO). It is, therefore, increasingly likely, if it is not already true, that law enforcement and intelligence officials will handle vulnerability information in the course of planning and executing remote access warrants. The Minister should ensure that there is a robust and transparent policy for handling and disclosing these vulnerabilities to vendors capable of responsibly patching them.[5] For as certainly as Eternal Blue led to WannaCry ransom attacks, government agencies routinely handling vulnerability information without such policies will lead to additional global security crises.[6]

Conclusion

While strong encryption poses new challenges to those who bear the task of protecting Australia, its people, and institutions against crime and terror, we must not lose sight of the fact that secure communications are vital to both economic competitiveness as well as to defending against threats of cyber-attack. Cisco fully supports developing a better understanding about the nature of the challenges about which the government is concerned. However, in the course of pursuing new creative solutions, we must avoid the trap of assuming that privacy vs. security is a zero-sum game.

We applaud the government for its efforts to protect Australia against threats rooted in both the physical and cyber world. We thank you for the opportunity to comment on the Bill, which we view as part of a commitment by the government to seek practical advice for how best to leverage the innovations accorded by connected, global technologies while effectively managing associated risks. However, we are concerned about the issues described above. We encourage the Committee and the Parliament to take a considered approach to the assessment of this Bill. That should

[5] https://www.lawfareblog.com/its-time-international-community-get-serious-about-vulnerability-equities
[6] https://www.theaustralian.com.au/business/wall-street-journal/dark-knight-saves-the-internet-from-malware-attack/news-story/97aae33950aff521867f6630caf429b1

Cisco Systems, Inc.
170 West Tasman Dr.
San Jose, CA 95134
USA
+1.408.526.4000
+1.800.553.6387
www.cisco.com

include taking the time necessary to fully assess and consider the implications of the Bill. We look forward to the opportunity to continue participating in a dialogue on this Bill as it progresses.

Yours sincerely

Eric Wenger
Director, Cybersecurity and Privacy Policy
Global Government Affairs
Cisco Systems, Inc.

Tim Fawcett
Head of Government Affairs
Cisco Systems Australia Pty Ltd