Cisco Systems Australia Pty Ltd

Level 14, 101 Collins Street
Melbourne Victoria Australia 3000

CISCO AUSTRALIA RESPONSE TO THE SECURITY LEGISLATION AMENDMENT (CRITICAL INFRASTRUCTURE) BILL 2020 – EXPOSURE DRAFT.

Cisco welcomes the opportunity to respond to the Security Legislation Amendment (Critical Infrastructure) Bill 2020 Exposure Draft.

Our submission to *Protecting Critical Infrastructure and Systems of National Significance Consultation Paper* 2020 covered our feedback on the intended approach to critical infrastructure more holistically. This response focusses on specific points in the exposure draft of the Bill. We appreciate the opportunity to constructively contribute to this consultation process.

Cisco acts both as an operator of technology equipment and services used in industries deemed critical including, for example, Telehealth, as well as a supplier of equipment and integration services to these industries. Our feedback is aligned to both roles, however reflects a subset of what was contained without our initial response.

Positive Security Obligations

Cisco commends the principles based approach of the Positive Security Obligations (PSOs) especially the promotion of a risk management approach to cyber security with a focus on all hazards. As a vehicle for security uplift, a rules-based approach (19) focusing on individual assets would be inadequate without a holistic approach to the overall system risk, which we understand will be provided by the Trusted Information Sharing Network (TISN) (38), industry and government . The consultative approach and industry partnership in this are key. Expertise in securing critical infrastructure assets often sits outside an individual vertical, so inclusion of experts outside of a regulated sector should be an explicit goal of the enhanced TISN program.

Mandatory cyber security reporting

The mandatory reporting of serious cyber security incidents directly to the ACSC raises some concerns about operational costs and efficacy. These concerns arise both from the multi-tenancy nature of the Data Storage and Processing sector, as well as the potential for excessive operational overhead.

This operational overhead arises from two areas, the focus on manual processes, such as the need to write formal reports, and the granularity of an incident deemed as serious. Manual processes are difficult to achieve in a timely fashion and can inhibit dealing with the security problem immediately. The definition of a serious incident is also unclear. If the bar is set too low, it could result in significant burden for not only the sector entity but also the ASD as the recipient. Availability of components can be challenged regularly by DoS attacks, however availability of systems is not compromised.

Cisco operates in 170 countries globally and requests for data of any kind are likely to be replicated in each country. Accordingly, we expect processes particularly for the Data Storage and Processing sector to be adequately streamlined to support the global nature of this industry.

We look forward to reviewing the Department's Regulatory Impact Statement (RIS) especially the cyber incident reporting and the thresholds for incidents as raised in (319).

Given the objectives, it is unclear how these reporting requirements uplift security in a significant way. Incident information is a reactive process for understanding a threat picture and should not be seen to meet industry's desire for improved bi-directional threat sharing arrangements within sectors, between sectors, and with the government. Sector specific definitions of incidents are required. Additionally, on a sector by sector basis, telemetry could better suit the goal of more real time threat understanding.

It is standard practice in this sector that security incidents impacting a tenant are notified to the tenant directly. This is done within the confidentiality and privacy arrangements of the legal contract between provider and consumer. To report cyber security incidents outside of this arrangement may be in conflict.

Additionally, given the shared security responsibility model for DCaaS, IaaS, PaaS, and SaaS, a cyber security incident may have "root cause" with a customer rather than a provider . Indeed, depending on the nature of the XaaS, the provider may have no visibility of an incident by design.

As the Act allows for a selective "on switch" for each aspect, we suggest cyber security incident reporting directly to the ACSC is not "turned on" and Cloud and Data Processing entities continue to report incidents directly to their customers (tenants) who in turn then report to the ACSC as part of their own PSOs. Such an arrangement allows providers to maintain the confidentiality of their customers whilst ensuring that the ACSC gains the desired data and visibility. Additionally, the ACSC will have visibility of cyber incidents related to the customer security responsibilities.

Identification of critical data storage or processing assets.

Cisco recognises that the identification of assets is a primary step in risk management, as you cannot secure what you do not know about. In general, it would seem appropriate for CISONS entities , including government, to map their supply chain in conjunction with the ACSC and/or industry regulator. This would then enable the entity/ACSC/regulator to notify the appropriate XaaS entities and MSPs that they are providing services to a CI.

Given one of the key criteria for identifying critical data storage or processing assets is providing services to various tiers of government and government owned enterprises, an explicit notification from the consumer (government and/or operator) would be preferred. Due to the multilayered XaaS nature of cloud, an IaaS provider may unknowingly operate critical assets because only the SaaS provider using that IaaS provider has visibility of the actual end customers. Similarly, some

SaaS offerings are administered by third parties (eg. white labelled) where only that seller has visibility of the end customers.

It should be noted that the register of assets, and the incident information sharing system, would become critical infrastructure in and of itself.

Partnerships and co-design

We welcome the approach by the Department to co-design the sector specific requirements to avoid duplication of existing approaches, to be principles-based and proportionate to sector risks, and impose the least regulatory burden to achieve the security outcomes.

We would additionally suggest that, in principle, a commonality of approach is followed by the different sectors and their respective regulators. As identified in our previous submission and raised in the Home Affairs Department townhall briefings, Cloud and Data Processing is a horizontal sector across all other 10 sectors. Whilst we recognise and agree sectors need an approach appropriate to the risks for each sector, we also desire to see a common approach (varying in depth or a subset of scope where appropriate) from industry regulators. The risk management approach followed by Cloud and Data Processing sector should be consistent with the needs of each sector. Hence, common standards and recognition of risk assessments performed in or for other sectors should be transportable.

Directions and Step In powers

These aspects of the bill, whilst contentious for all sectors, are of specific concern to cloud and data processors. Whilst a cloud provider may provide business critical services to government or a CISONS entity, it also provides services to many organisations who are not CISONS entities using the same infrastructure – that being the multitenant nature of cloud. Indeed, some of the customers or tenants, or cloud infrastructure, or assets located in Australia that are captured by the Bill, may be providing services to customers not located in Australia.

The potential for damages, both financial and reputational, arising from directives and use of step in powers could be significant and wide ranging. The legislation proposes to provide the Australian government with full immunity from liability, where it uses the step-in powers, despite the risk. There are circumstances that are foreseeable whereby smaller entities may seek government assistance with a breach where they do not have the capacity to deal with the incident. In this case limited liability is reasonable. However, for larger and sophisticated operators of ICT systems, it is difficult to imagine an situation where mandatory use of step in powers would be needed. Even where a situation did arise, other capabilities are more reasonable or even extant.

Additionally, whilst the use case for these directive and step in powers differs from TOLA, that does not change the requirements of the cloud sector to operate and be perceived to operate independently of government interference globally. Hence, we recommend a mechanism to appeal determination of technical feasibility and the application of these powers through the courts or an independent authority.

Conclusion

Cisco appreciated the consultative approach the Department of Home Affairs has taken in drafting this important legislation and is supportive of the steps the Australian government is seeking to take. Cisco will continue to provide input as the legislation proceeds through the Parliament and the committee review stage. Given the significant and world leading powers contained within the draft bill, an ongoing dialogue and debate with industry will result in efficacious and world class CISONs laws.