30 November 2020

Mr. Marc Ablong,
Deputy Secretary Policy
Department of Home Affairs
[redacted]

Subject: Comments on Exposure Draft of the Security Legislation Amendment (Critical Infrastructure) Bill 2020

Dear Mr Deputy Secretary,

The Asia Internet Coalition ("AIC or We") and its members wishes to express our sincere gratitude to the Department of Home Affairs for the opportunity to submit comments on the Exposure Draft of the Security Legislation Amendment (Critical Infrastructure) Bill 2020.

The AIC is an industry association comprised of leading Internet and technology companies. AIC seeks to promote the understanding and resolution of Internet and ICT policy issues in the Asia Pacific region. Our members are Airbnb, Amazon, Apple, Cloudflare, SAP, Expedia Group, Facebook, Google, Grab, LinkedIn, LINE, Rakuten, Twitter and Yahoo (Verizon Media), and Booking.com.

First and foremost, we commend the Department of Home Affairs for their efforts on drafting new measures to strengthen cybersecurity protections for critical infrastructure. While we support these efforts, we believe that the bill's current definition of cloud service providers as well as overly broad authorities regarding data collection and access can potentially undermine the Government's security objectives and conflict with data privacy standards like the European Union's (EU) General Data Protection Regulation (GDPR).

The AIC is generally supportive of bolstering cybersecurity across the economy, but is concerned about regulatory burdens. As such please find appended to this letter details comments and recommendations for your consideration.

We are also grateful to the Department of Home Affairs for upholding a transparent, multi-stakeholder approach in developing this code. We further welcome the opportunity to offer our inputs and insights, directly through meetings and participating in official consultations.

Should you have any questions or need clarification on any of the recommendations, please do not hesitate to contact me directly at [redacted] or [redacted]. Thank you for your time and consideration.

Sincerely,

[redacted]

Jeff Paine
Managing Director
Asia Internet Coalition (AIC)

Detailed Comments and Recommendations

Introduction

We are writing to express our concern regarding the Security Legislation Amendment (Critical Infrastructure or CI) Bill 2020. While we support the Government's effort to strengthen cybersecurity protections for critical infrastructure, we believe that the bill's current definition of cloud service providers as well as its overly broad authorities regarding data collection and compelled access to provider systems, would not only undermine the Government's security objectives but also potentially conflict with data privacy standards like the European Union's (EU) General Data Protection Regulation (GDPR).

The proposed legislation would expand coverage of the Security of Critical Infrastructure (SOCI) Act to cover ten new sectors of the Australian economy including financial services, food and grocery, health care and medical, as well as "data storage or processing," which is defined as "enterprise data centers, managed services data centers, colocation data centres, and cloud data centers," and "infrastructure as a service (IaaS), software as a service (SaaS), and platform as a service (PaaS)."

The bill also expands the government's authority over covered entities, including the power to compel production of systems data and direct access to provider systems. For example, the legislation suggests that providers may be required to allow the Australian Signals Directorate (ASD) to remove or alter files and install “host-based sensors” to collect telemetry, to install programs, “access, add, restore, copy, alter or delete data”, alter the “functioning” of hardware or remove hardware entirely from premises.

Without additional clarification, global providers that potentially fall under the data storage or processing definition will face significant uncertainty regarding their status under the legislation, and how such proposed access will be perceived by non-Australian customers and authorities. Moreover, the prospect of compelled access and compelled production of personal data to the ASD may raise questions about compliance with non-Australian privacy laws like the EU’s General Data Protection Regulation (GDPR). Providing direct government access to network systems that may contain the data of non-Australian individuals appears inconsistent with the requirements of those laws.

Given the substantial uncertainty regarding the scope of numerous provisions of the Security Legislation Amendment (Critical Infrastructure) Bill, we respectfully request consideration of the legislation be postponed until the myriad of concerns are addressed. As part of any additional deliberations, we request that the Government specifically address potential conflicts with major data privacy statutes like GDPR.

Supporting comments

---

1. Timeframes for Cyber Security Reporting

The timelines of 12-hours and 24-hours for reporting a "Critical Cyber Security Incident" and "Other Cyber Security Incidents", respectively, are unnecessarily short. This requirement injects additional complexity at a time when critical infrastructure entities are faced with the difficult task of responding to a cyber incident. It also greatly increases the likelihood that the CI entity will report inaccurate or inadequately contextualised information that could be shared with the government and other members of industry. We strongly recommend that the Government replace these timelines with a requirement for companies to report "as soon as reasonably practicable" or that each sector is subject to tailored timeframes decided in the co-design process. We also note that the full extent and impact of a cyber security incident may not be known or well understood within 12 hours of it being realised. Therefore, it may also be difficult for an organisation to determine whether it is a "critical" or "other" cyber security incident within the timeframes.

2. Critical Cyber Security Incident

The AIC submits that this and other reporting obligations should explicitly be made to apply to incidents taking place within Australia and its territories only. The definition and criteria for a "critical cyber security incident" is not defined in the legislation. Of note, the term "significant impact " in section 30BC (1) (b) (ii) is not defined. The Explanatory Document provides some commentary on this at paragraph 319, noting that determining whether an incident is having a significant impact on the availability of the asset will be a "matter of judgment for the responsible entity" and that the threshold has been left "intentionally undefined as the significance of an impact on the availability of an asset will vary radically between assets". It also notes that it is "not intended that day-to-day incidents ... should be reported." While this guidance is helpful, it does leave many organisations guessing what constitutes a "significant impact" on the availability of an asset. We would recommend that the Government take this as a focus for the co-design process.

3. Obligations to consider digital supply chain and international obligations

In section (8) it is specified that *"... in determining whether the specified direction is ... proportionate ... the Minister must have regard to ... the impact of the specific direction on ... the activities carried on by the specific entity ... and ... functioning of the asset concerned."*

The AIC is concerned that the proposed Ministerial Authorisations for cyber security incidents focuses the engagement solely upon a 'relevant entity". Cyber threats to CI may arise at different parts of the digital supply chain but have implications across the whole supply chain and for global cloud providers be they platforms (IaaS) or software (SaaS) they are often globally interconnected so naturally these providers are very sensitive about any direct action occurring in Australia that affects its global business.

The AIC questions the geographical boundary of the Systems of Critical Infrastructure (2018) regime when it comes to IT and data; data may be stored in Australia but be replicated in other regions. Data can move between borders. Therefore, a government entry onto Australian premises may have a downstream effect overseas, raising questions about international legal liability.

Furthermore, if the government were to direct or intervene with a cloud infrastructure provider, this could have material downstream implications across the whole supply chain without the knowledge of the SaaS, PaaS or CI customer.

Given the potential complexity of a cyber incident and the inter-relationship across the supply chain and the global connected environments of many cloud businesses, we recommend a holistic approach is taken. Where the government seeks to exercise the power there is engagement across the digital supply chain in the event of a direction to act, or direct intervention.

WethereforerecommendthattheMinisterialauthorisationpowerincludesanobligationon the government to consider the supply-chain impacts before exercising its power to intervene. This could be inserted as an amendment to S35AB in the form of a replacement of ss(8)(c) (with the existing ss(8)(c) becoming ss(8)(d)):

[In determining whether the specified direction is a proportionate 25 response to the incident, the Minister must have regard to...]
(c) the consequences of compliance on relevant supply chains

In relation to access to system information, the AIC suggests a comprehensive assessment of relevant international laws, for example the European Union's General Data Protection Regulation, be undertaken in order to understand whether the proposed legislation would have the potential to put entities in conflict with international obligations.

4. Ministerial authorisations, intervention requests and actions

A significant portion of AIC represented entities believe that the data processing and storage sector should be exempt from the direct action provisions in the legislation and wish to find an alternative path to achieving the desired assistance outcomes with government for this sector. Others crave greater regulatory oversight and responsibility from government for cyber security incident management and reporting, but with the maximum clarity, consistency and opportunities for recourse and review.

Under s35AB, which relates to Ministerial authorisations, intervention requests and actions in the case of a cyber security incident, it is stipulated that:
(7) The Minister must not give a Ministerial authorisation under paragraph (2)(c) or (d) unless the Minister is satisfied that:
(a) the specific entity is unwilling or unable to take all reasonable steps to resolve the incident; and
(b) the specified direction is reasonably necessary for the purposes of responding to the incident; and
(d) compliance with the specified direction is technically feasible.

The AIC posits that genuine disagreements as to strategy and best course of action ("*reasonable steps*") may arise between government and industry heads, that this may be interpreted for the sake of justifying intervention as an 'unwillingness' to take 'all reasonable steps to resolve the incident'.

These concerns apply equally to s35AB(10), pertaining to ministerial intervention requests. Therefore, we believe that where a decision is made to issue a written notice or direction, the legislation should provide for the entity's ability to formally request the decision- maker to reconsider.

The 'technical feasibility', 'unwillingness' or 'inability' to take reasonable steps should be subject to an independent assessment that can be triggered by the appeal of the entity in question, should that entity believe in good faith that the entity possesses the willingness and ability to address cyber threats, but disagrees with the government's intended risk- mitigation strategy or course of action.

It is proposed that the independent appeals board be stood up on an on-call standby basis, and thus stood up when the Minister for Home Affairs convenes the tri-Minister meetings to authorise directions, with a review of membership between industry and government annually. Given the national security significance of acting quickly, the appeals process would only start a 12-hour 'clock' so that if action is indeed warranted, it would not be unduly delayed. Mechanisms for defined post-event review, potentially involving the same members of the board, should also be established.

5. System information software notice

The requirement that under certain circumstances entities install a specific computer program on their computers (s30DJ(2)) – with a requirement in the latter case to 'consult' but no further recourse (s30DK) and a civil penalty equating to 200 units (s30DM) if the entity fails to comply with the system information software notice is greatly concerning to the AIC and constitutes extraordinary overreach. The mandatory installation of government-selected software in any entity's systems on pain of civil penalty is troubling in itself, but the potential impacts on global interconnected businesses such as cloud providers is of particular concern. We submit that the data storage and processing sector be excluded from exposure to system information software notices if this power is to persist in the legislation. At the least, additional safeguards and frameworks ought to be put in place, such as the entity's security teams being able to undertake an assessment of the software and an ability to seek an injunction.

The government ought also consider that if multiple critical infrastructure systems are required to install the same piece of government-mandated software, this itself can represent a vulnerability in the system.

6. Other Cyber Security Incidents

The threshold for reporting "other cyber security incidents" appears to be too low and the outcome of this provision will likely be an overreporting to the Commonwealth of incidents that may or may not be helpful. Of note:

Section 30BD(1)(b) sees the introduction of the requirement to report where a cyber security incident is not only where an incident has occurred, or is occurring but also, where a cyber security incident is "imminent". The term "imminent" is not defined in the Bill or the Explanatory Document. For example, does this refer to a scenario where there is a disclosed vulnerability, but the organisation is in the process of patching their systems? Does this require companies to report on attempted incidents? If so, this could see the Commonwealth burdened with thousands of reports per day.

The Bill also notes that the incident must have also "had, is having or is likely to have a relevant impact on the asset". It is unclear how a CI asset can determine whether an incident is likely to have a relevant impact - as likely remains undefined and guidance on the parameters here is missing.

The Explanatory Document goes further and explains that "by contrast to a critical cyber security incident, this obligation relates to any impact on availability (irrespective of significantly) alongside other forms of impact".

Reading section 30BD as whole, the reporting threshold is too low and will likely result in the Commonwealth being overwhelmed by reporting of cyber incidents – undermining their ability to provide timely and actionable advice to critical infrastructure assets.