ITI Promoting Innovation Worldwide

February 12, 2021

ITI Comments on the Review of the Security Legislation Amendment (Critical Infrastructure) Bill of 2020

ITI appreciates the opportunity to provide feedback on Australia's Review of the *Security Legislation Amendment (Critical Infrastructure) Bill of 2020* (hereafter Bill). We are grateful for the chance to remain consistently engaged in Australia's critical infrastructure (CI) reform efforts.

ITI represents the world's leading information and communications technology (ICT) companies. We promote innovation worldwide, serving as the ICT industry's premier advocate and thought leader in the United States and around the globe. ITI's membership comprises leading innovative companies from all corners of the technology sector, including hardware, software, digital services, semiconductor, network equipment, cybersecurity and other internet and technology-enabled companies that rely on ICT to evolve their businesses.

We previously submitted feedback both on the Department of Home Affairs' (DHA) Exposure Draft of the Bill in November 2020 and the DHA consultation paper on *Protecting Critical Infrastructure and Systems of National Significance*. We are pleased to provide follow-up comments to our previous submissions.

We are supportive of Australia's efforts at reform and congratulate the Australian Government on its leadership in promoting cybersecurity risk management among Australia's CI entities. We are particularly appreciative of the Government's incorporation of industry feedback and positive changes to the Bill from its previous iterations, including:

- **Increasing the scope and of DHA's role to the de-facto regulator for several sectors and providing appropriate resources.** Per Section 7.4 in the Bill's Explanatory Document, DHA will undertake a significant hiring and retraining program, and will communicate the staffing levels needed to implement the proposed changes in this Bill to the Government for considering for future funding. We encourage the Australian Parliament to approve and/or provide this funding as needed.
- Also in Section 7.4, we are pleased the DHA included its plans to **raise awareness around the new legislation** and to provide guidance to assist industry in meeting the new obligations.

However, our previous comments that we provided for the Exposure Draft, outlined below, still reflect our key concerns and suggestions toward the proposed CI reforms. Therefore, we encourage the Parliamentary Joint Committee on Intelligence and Security to consider our comments while undergoing the review process.

General Comments

"On-Switch"

We appreciate that Australia considered stakeholder comments in designing an "on-switch" for many of the obligations set forth in the Bill. Unfortunately, there is still a high-level of uncertainty for CI owners/operators because the majority of the obligations that they will be required to meet

Global Headquarters
700 K Street NW, Suite 600
Washington, D.C. 20001, USA
+1 202-737-8888

Europe Office
Rue de la Loi 227
Brussels - 1040, Belgium
+32 (0)2-321-10-90

info@itic.org
www.itic.org
@iti_techtweets

will be set out in sector-specific rules that have yet to be designed. This is problematic, because it is not clear how onerous or burdensome the requirements will be. Beyond that, we expect the process of designing those rules to be complex and prolonged, especially because rules need to be developed for all eleven sectors. In effect, seeking compliance with this Bill would be like asking CI owner/operators to sign a contract which sets out obligations in a schedule that is not attached to the contract.

Positive Security Obligations (PSOs)

We understand the rationale behind including PSOs in this Bill. We further recognize that these PSOs will only take effect if CI owners/operators do not comply with the sector-specific rules (once they have been drafted). That said, we encourage the rules and the PSOs to be aligned with international standards. If they are designed with Australia-specific standards in mind, that approach will create compliance and operational challenges for companies that have already designed their systems to international standards. Therefore, we recommend that the Government of Australia make the details of the sector specific rulemakings public and conduct additional stakeholder consultation before moving forward on the overall legislation. We also recommend that Australia permit covered companies to use existing international standards and certifications (such as the ISO 27000 series) to demonstrate compliance, and that, if Australian national standards exist, they are mapped to existing ISO requirements and compliance controls.

Government Assistance

We provided input on the extent to which we believed the government should provide assistance to a CI owner/operator in our previous submission. However, we remain concerned with the seemingly limitless power the government has to intervene. Part 3A of the Bill provides 'take control' power, which allows the government to take control of a CI asset (either by request or by force). While there are processes that the Minister would be required to undertake before utilizing this power, there are also provisions which allow the Government to subvert these processes where they deem it necessary. This seems like a broad use of discretionary power which could, for example, result in the government taking control of private companies' systems utilizing their own personnel. The rule also does not provide regulated entities with a review process of the merits of the Government's use of "assistance" powers by a judge. We recommend that the Government of Australia seriously consider the implications of this 'take control' power.

Further, we note this broad proposed government intervention regime has no precedent globally and may create security and compliance concerns for global cloud providers (as well as other impacted CI owners/operators). Permitting the Australian government to obtain sensitive information relating to global providers' cybersecurity and data protection or interfere with the operation of cloud provider systems may disrupt the integrity and security of cloud services, including services provided to customers in other regions. Australian government access to sensitive internal systems of cloud providers may conflict with the requirements and prohibitions of the laws of foreign jurisdictions that global cloud providers may be subject to, creating difficult conflicts of law. For example, if access pursuant to the proposed government assistance scheme implicates the confidentiality, integrity, and security of information of or relating to cloud customers or end-users, various provisions of privacy and cybersecurity laws and regulations in multiple jurisdictions might create intractable conflicts of laws.

The need for information, action, and intervention powers under the proposed regime is therefore highly uncertain. Further, these powers may not be practicable as applied to the cloud industry, as

the providers' internal incident management procedures are guaranteed to be more efficient and agile than a government-directed attempt to take control of a sophisticated third-party system for which it does not have experience. Providers should be required to demonstrate that their incident and risk management procedures meet international standards, such as those contained in ISO 27000 certifications.

Definition and Scope of Critical Infrastructure

Data Processing/Storage

We noted concerns in our comments on the previous consultation paper related to the addition of "data and cloud" as a CI sector because it raised many questions, including what sorts of businesses could be captured under this category and what that would mean for Positive Security Obligations (PSOs). We appreciate that the Explanatory Memorandum to the Bill attempts to clarify some of these questions, especially by narrowing the scope of data and cloud to "data processing/storage" and providing a definition of "business critical." However, we remain concerned about the inclusion of this "sector" as CI for several reasons, and continue to request that it be removed from the Bill.

First, this seems to be out of step with the ways in which other governments globally have chosen to define CI. While we recognize that data processing/storage has taken on an increasingly important role across all economies, governments have largely avoided defining cloud and/or data processing/data storage as a separate CI sector due to its cross-cutting nature, and the fact that so many other sectors are dependent on cloud and/or data processing/storage as horizontal enablers of these other sectors. It is also unclear who the regulator for this sector would be, as there is not, in our view, an agency or regulatory authority that would be a natural fit.

Second, the breadth of services that fall in scope under the definition of data processing/storage is enormous. It includes everything from enterprise data centers to cloud services. While we appreciate that in designating such items as in scope, Australia is trying to exercise consistency, we would caution that this approach has its own set of challenges. In exercising a risk-based approach, regulators should consider risks associated with each sector. Cloud services and data centers, while related, have different risk profiles and thus, an approach that may be appropriate for an enterprise data center may not be appropriate for a cloud service provider. The Government should also re-evaluate what falls into scope for "cloud services." For example, while there may be a reason to include IaaS, there are many SaaS applications that would not qualify as critical; extending the scope of the definition to IaaS, PaaS and SaaS increases the compliance burden significantly without meaningfully protecting critical assets/workloads. As we understand it, the Bill seeks to undertake a risk-based approach to CI protection and conflating all of these disparate services could make such an approach challenging.

Finally, because data storage/processing cuts across traditional industry verticals, it is unclear how sector-specific CI rules (for example, rules in the energy sector, telecom sector, or financial sector), would interact with the PSOs data processing/storage providers would be required to follow as a result of this bill. Indeed, many CSPs have existing customer relationships with CI operators in different sectors and are therefore already held to the standards or requirements applied by that sector. It seems possible, then, that new PSOs may conflict with or duplicate the requirements a CSP is already required to meet. At a minimum, the Bill should clarify the roles and responsibilities

of CSPs and others included in this proposed sector vis-à-vis their customers in other CI sectors, particularly with respect to any proposed PSOs.

In general, while we understand the desire to designate data processing/storage as a CI sector, for the reasons articulated above we are concerned that including such a sector will set an unfortunate global precedent.

Systems of National Significance

The Bill indicates that enhanced PSOs will be required for "Systems of National Significance," Australia's most critical assets. However, these systems of national significance (SoNS) are not defined or identified in the draft legislation. We urge Australia to more clearly consider what constitutes a SoNS and additionally consider the requirements attached to such a designation. Indeed, some of the obligations appear to be more intrusive than necessary, including providing government access to systems information.

The Bill purports to introduce a power of the government to require CI operators -- including cloud service providers -- to implement government-provided security monitoring software. This software would scan resources and assets used or capable of being used to process the information of or relating to end-users and customers of cloud service providers, including user activity data and network data relating to end-user and customer use of cloud products. Permitting the government to operate such software may be inconsistent with the requirements and prohibitions of the law of foreign jurisdictions to which global cloud providers may be subject. Furthermore, adoption of third-party software in a cloud environment without appropriate security reviews and procedures is more likely to increase security risk than it is to mitigate it. At a minimum, the scope of the system information software notice requirement should be narrowed to exclude providers of cloud services and operators of cloud data centers.

Communications

We recommend adding a clarification to the Bill that only entities subject to the Telecommunications regulation in Australia -- such as licensed carriers -- will bear obligations under the Communications prong of the new regulatory regime. For example, global service providers or network operators who invested in services from licensed carriers or in international submarine cable projects should not become a potential target of compliance requests under the new regime and should not bear positive security obligations as operators of Communications CI unless they are regulated as carriers under Australian law.

Mandatory Cyber Incident Reporting Requirements

We appreciate that cybersecurity information-sharing plays a significant role in improving cybersecurity. On the proactive side, information-sharing should be a voluntary action that helps to paint a full picture of the risk landscape, potential mitigations, and possible downstream ramifications of policies intended to address those risks. On the other hand, incident reporting is a reactive measure, and its parameters should be narrow. While we are encouraged that Australia is taking steps to improve cybersecurity information-sharing, we have concerns with the mandatory cybersecurity incident reporting requirements as laid out in the Bill.

Critical Cybersecurity Incidents

The Bill requires a responsible entity to report a "critical" incident to the relevant authority (the Australian Signals Directorate, unless otherwise specified) within 12 hours. While we appreciate that this requirement is only applicable to incidents defined as "critical," we recommend a more flexible reporting threshold with respect to timing (e.g., language such as "without undue delay"). A more flexible time period is preferable for both practical and security reasons.

First, from a practical standpoint it may often be the case that an organization is not aware of enough details regarding a security incident within a short timeframe of 12 or even 72 hours to credibly make an assessment as to the severity of an incident or its impact, particularly when the draft law does not make it clear as to what triggers the tolling of the "incident clock."

Additionally, from a security standpoint it may be counterproductive to disclose details regarding an incident that is not fully understood or mitigated. If Australia chooses to keep a time-bound reporting requirement in the Bill, however, we recommend extending the time frame to at least 72 hours and clarifying when that time period begins. This approach would allow for a more reasonable amount of time to discover and report the incident.

The Bill indicates that in order to be considered critical, the incident must be having a "significant impact" on the availability of the asset. While we recognize that Australia has purposely left "significant impact" undefined and that the Critical Infrastructure Center will distribute sector-specific guidance to assist in making that sort of determination, we think a baseline definition would still be helpful here. Further, the Bill should clarify that notifications should not result in increased liability for CI entities required to report "critical" security incidents.

Relevant Cybersecurity Incidents

The Bill also requires that other cybersecurity incidents deemed to have a "relevant" impact must be reported within 72 hours. While we appreciate that the incident notification timeline has been increased from 24 hours in the Exposure Draft to 72 hours in the Bill, we maintain our prior recommendation that Australia reconsider the mandatory reporting requirement in this instance, or at a minimum adopt a more flexible approach and language such as "without undue delay," for the reasons regarding flexibility, practicality and security referenced above and particularly because relevant in this context means that the incident has *any* impact on the availability of the asset.

Indeed, this mandatory reporting requirement for "relevant" incidents could lead to overreporting in instances where a report is not specifically necessary, or otherwise divert resources that could be better spent improving cybersecurity than reporting every "relevant" incident. Such mandatory reporting requirements may also inundate the competent authority(s) with so many incident reports that it becomes difficult to distinguish key trends (which is one of the stated aims of the Australian Government) or further detract attention and resources from malicious cyber actors.

The focus should be on encouraging high-quality reports that drive accountability, improve cyber practices, and benefit end- users (e.g., through appropriate mitigation, user-awareness, improving standards, etc.)." The advantage of a voluntary reporting mechanism would be a reduced burden on the government to review significant reporting requirements (annual reports, other cyber incidents, critical cyber incidents, etc.) that result in thousands of reports, as well as potential requests for assistance by affected entities.

Further, the Bill should clarify that notifications should not result in increased liability for CI entities required to report "relevant" security incidents. In developing reporting requirements in either case, we recommend that Australia take into account relevant international standards on vulnerability management (ISO/IEC 29147 and ISO/IEC 30111).

Another concern with the reporting requirement for Relevant Cybersecurity Incidents revolves around requirements in section 30BD that require an entity to notify where a cyber security incident is 'imminent' (30BD(1)(b)(i)) or when an incident "….is likely to have a relevant impact on the asset" (30BD(1)(b)(ii)). Paragraph 658 of the Explanatory Document attempts to explain 'imminent,' but it remains unworkable to require reporting on something that has not yet happened or been confirmed. There are no attempted descriptions in the Explanatory Document of a "likely impact." These requirements are unclear and will likely result in the Commonwealth being overwhelmed by receiving thousands of reports (if not more) per day, particularly if there is uncertainty among covered companies of their obligations to report incidents that have not yet happened. This will undermine the Government's ability to provide timely and actionable advice to the CI assets as well as unnecessarily burden entities who will likely err on the side of reporting too much (or will have to spend time determining if an incident is imminent or likely to impact an asset) - which will divert information security teams' attention and limited security resources away from the essential tasks of actually examining and remediating an incident/ securing their systems.

Voluntary Incident Reporting & Information-Sharing

We also recommend that Australia consider developing a mechanism by which entities could voluntarily report relevant incidents anonymously, including additional types of cybersecurity incidents such as "near misses" and vulnerabilities. This could help to identify emerging trends or otherwise preempt attacks. There are established mechanisms for voluntary reporting and information sharing on incidents, including through Computer Security Incident Response Teams. The Trusted Information Sharing Network (TISN) is a mechanism that could potentially be leveraged to allow for voluntary, anonymous incident reporting. Australia should consider how these existing mechanisms could be better leveraged and interplay with regulatory reporting regimes that may deter voluntary reporting.

While we appreciate Australia's efforts to foster greater voluntary information-sharing through the establishment of a new engagement mechanism under the TISN, in the longer term, we recommend that Australia consult industry about the specific limitations and effectiveness of the information that is provided. It is important that the information requested can both be accessible to organizations at respective levels of capacity and protect any proprietary information of the commercial entity. Currently, the mandatory incident reporting requirement places significant responsibility of the owner or operator of the asset to report an incident to the relevant authorities, but it does not appear that the Government has the same level of responsibility to share information about threats, incidents, or vulnerabilities with asset owners. Therefore, we encourage Australia to more seriously consider how to facilitate two-way information-sharing, either in the context of this Bill or otherwise, to provide owners/operators more access to information about the threat landscape and mitigations that will enable improved cybersecurity practices. As we referenced in our previous comments, it will be especially important to consider how to share information with small and medium sized enterprises, who may have more difficulty accessing information than larger, better-resourced companies.

***

Once again, ITI appreciates the opportunity to provide our perspectives on Australia's *Security Legislation Amendment (Critical Infrastructure) Bill of 2020*. Protecting critical infrastructure is incredibly important, but it will take sustained effort from and discussion between government and industry to appropriately reform existing legislation and processes. We urge Australia to continue its stakeholder outreach as it moves forward in its CI reforms. Please view ITI as a resource – we are always happy to engage and offer our thoughts on these topics.