ide

Information Technology Industry Council (ITI) Opening Remarks
Parliament of Australia Joint Committee on Intelligence and Security
Review into the Security Legislation Amendment (Critical Infrastructure) Bill 2020 and Statutory Review of the Security of Critical Infrastructure Act 2018
Submitted by Courtney Lang, Senior Director of Policy
July 5, 2021

Thank you for the opportunity to testify today with regard to the Parliamentary Joint Committee on Intelligence and Security's Review into the Security Legislation Amendment (hereafter Critical Infrastructure) Bill of 2020.

ITI represents the world's leading information and communications and 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. Nearly 25% of ITI's members are headquartered outside of the U.S.

We congratulate the Australian Government on its leadership in promoting cybersecurity risk management toward Critical Infrastructure (CI) and express our support for Australia's efforts at reform with the goal of "ensuring the resilience of Australia's critical infrastructure is clear, effective, consistent and proportionate." We previously submitted feedback on the Department of Home Affairs (DHA) Consultation Paper, the DHA Exposure Draft of the Bill in November 2020, and the follow-up Review of the Bill in February 2021. We are pleased to appear today to serve as a resource for the Committee and to answer any follow up questions pertaining to our submitted remarks for this hearing or on our previous submissions.

Today, we would like to highlight three main ongoing concerns with the current draft CI Bill:

1. Government Assistance Under Part 3A

In our previous comments on the CI Bill, we provided input outlining our concerns with Part 3A of the Bill allowing "take control" power, which allows the government to take control of a CI asset (either by request or by force). We continue to have concerns surrounding the intervention authority that may be granted to the government, as it continues to constitute a broad use of discretionary power which is, in our view, unnecessary for companies, such as ITI's members, which have invested significant resources in establishing and utilizing robust cyber risk management practices, technologies, and security.

We appreciate that the cyber incident reporting process requires close collaboration between the government and industry, and that the aim of this intervention authority is to ensure that such collaboration occurs. However, such an extreme approach may serve to undermine this goal, instead putting companies on the defensive and having the opposite of the intended effect. Should the Australian government choose to maintain these powers in future iterations of the legislation, we urge it to provide regulated entities with an appeals or other type of review process of the merits of the Government's use of "assistance" powers.

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

Further, this broad proposed government intervention regime has no precedent globally and may create security and compliance concerns for impacted CI owners/operators, including global cloud providers. Permitting the Australian government to obtain sensitive information relating to global providers' cybersecurity and data protection or otherwise interfere with the operation of providers' systems may disrupt the integrity and security of cloud services, including as 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.

2. 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. We also appreciate that incident reporting can play an important role in responding to incidents and containing or preventing further impacts. However, 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.

In particular, the Bill requires an 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 continue to recommend that the legislation utilize a more flexible reporting threshold with respect to timing (e.g., language such as "without undue delay") for both practical and security reasons. Among other things, it is unlikely that a business would be able to provide a full assessment of the incident to authorities within such a short timeframe, which could lead to misinterpretation of the issue. Indeed, within 12 hours, a company may still be determining the nature of the problem. With such a short reporting timeframe, it is possible that the impacted entity provides to the government either inaccurate or inadequately contextualized information in a situation where context is of great importance. This could, in turn, undermine the ability of both the impacted entity and the government to effectively respond to or remediate the incident. We continue to recommend that the reporting timeframe is extended to at least 72 hours, allowing businesses more time to execute a full assessment of the incident's impact and prevent the Australian government from intervening and/or wasting limited resources on processes that ITI's members are well-equipped to perform. Alternatively, the reporting threshold (i.e. 72 hours) could commence only after companies have completed a full assessment as to the severity of an incident or its impact.

Outside of establishing a more flexible time period, the government could also provide more detail for how "significant impact" is defined when assessing "critical" incidents. 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 determination, we think a baseline definition would still be useful.

Finally, although we appreciate that the Bill has extended the timeframe for reporting of "other" cybersecurity incidents to 72 hours, we continue to recommend against mandatory reporting of "other" cybersecurity incidents that have a "relevant" impact on the asset. Such a requirement 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.

3. Inclusion of Data Storage/Processing as a CI Sector

In our prior submissions, we noted our concerns with the inclusion of data storage/processing as a critical infrastructure sector and encouraged further narrowing of the definition. Our concerns persist, particularly because the scope of data storage/processing remains enormous, including everything from enterprise data centers to cloud service providers. As such, in its effort to take a risk-based approach to critical infrastructure protection in this legislation, we continue to encourage Australia to consider that the risk profiles of services that fall under this sector vary significantly, and as such, may require different approaches. Including such a varied array of service providers under this definition will make it challenging for the government to take a risk-based approach and may end up undermining its objectives. We also continue to encourage the government to narrow the definition of "cloud services" considered a part of CI. 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.

Additionally, 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 positive security obligations (PSOs) data processing/storage providers would be required to follow as a result of this bill.

***

We once again would like to express our support for Australia's efforts to reform its critical infrastructure framework while taking a risk-based approach. ITI and our member companies are pleased to see that the Committee is taking seriously inputs from the private sector, including related to our ongoing concerns with the bill. ITI stands ready to provide you with any additional input that may be helpful in your consideration of this legislation, particularly as you consider ways in which to address any outstanding issues.

I thank the Chair and Members of the PJCIS Committee for inviting me to testify today and for their interest in and examination of this important set of issues. I look forward to your questions.