ITI Promoting Innovation Worldwide

ITI Comments on the Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022

ITI appreciates the opportunity to provide feedback on Australia's *Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022* (hereafter referred to as "the Bill"). We are grateful for the chance to remain consistently engaged in Australia's critical infrastructure (CI) reform efforts.

ITI represents 80 of 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. Nearly a quarter of ITI's members are headquartered outside of the U.S.

We support Australia's efforts at critical infrastructure reform and congratulate the Australian Government on its leadership in promoting cybersecurity risk management among Australia's CI entities. While we understand that this Parliamentary Joint Committee on Intelligence and Security (PJCIS) consultation is focused on the SLACIP Bill, ITI would also like to raise for the Committee's awareness our ongoing concerns with the *Security Legislation Amendment (Critical Infrastructure) Act 2021*, also known as SOCI.

We remain concerned about the unprecedented and far-reaching powers in Part 3A of SOCI, which provides the Australian Government with information-gathering, direction and intervention powers that are not subject to reasonable due process. We continue to believe these "step-in powers" should be subject to a statutorily-prescribed mechanism for judicial review and oversight. In addition to our concerns over the lack of due process, we are also troubled by the global precedent that this rule may set for other governments viewing Australia's CI rules as a model.

We also reiterate our concerns with the mandatory cyber incident reporting timeline and believe it should be extended from "within 12 hours" to "at least 72 hours." As we have noted on many occasions, including in our recent testimony submitted to PJCIS, a 12-hour timeline is out of step with global norms, and may serve to undermine cybersecurity by inappropriately shifting an entity's focus from responding to and/or remediating the incident to ensuring compliance with reporting requirements.

On balance, we support the goals of the SLACIP Bill, but there are certain areas that we believe require additional clarity and which we encourage PJCIS to consider. Below, we offer more specific feedback.

Align Critical Infrastructure Risk Management Programs with International Norms

ITI supports Australia's initiative to promote cybersecurity risk management among Australia's CI entities, and we consider the additional positive security obligation for responsible CI entities to develop and maintain risk management programs a key pillar of the Government's CI reforms. Indeed, we applaud Australia's efforts to take a proportionate, risk-based approach to enhance CI

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

cybersecurity, including its efforts to engage with stakeholders in a co-design process to develop the rules governing this aspect of the CI bill.

For example, we appreciate that section 30AH is drafted in a way that allows for an entity to take a risk management-based approach that is appropriate for their business needs, ensuring that these requirements are both flexible and adaptable. These principles are key to an evergreen approach to critical infrastructure risk management. Additionally, as we have iterated in our prior responses, we stress the importance of leveraging international standards and certifications (such as the ISO 27000 series) to demonstrate compliance with Australian requirements.

Clarify Scope and Include Checks and Balances for Positive Security Requirements for "Systems of National Intelligence"

The Bill indicates that enhanced Positive Security Requirements will be required for "Systems of National Significance" (SoNS), Australia's most critical assets. However, this section does not clearly define or identify "SoNS". We urge the PJCIS to articulate more clearly what constitutes a SoNS, as Part 6A of the Bill would leave the designation entirely up to the Minister of Home Affairs and therefore engender uncertainty for industry. The criteria set forth in the Bill at present is broad, encouraging the Minister to consider "the consequences that would arise for…the social or economic stability of Australia or its people, the defence of Australia, or national security." Offering more explicit criteria that the Minister may consider in making such a determination will help to alleviate uncertainty as to whether an asset may be considered a SoNS and allow CI owners and operators to be appropriately prepared for additional obligations.

We also request that the PJCIS more clearly articulate the requirements attached to an SoNS designation, particularly for the proposed powers under Division 5, Subdivision A, which proposes "system information reporting notices." In this section, the Secretary may require by written notice that a SoNS provide both "system information periodic reporting" and "system information event-based reporting." We are concerned that this requirement for designated SoNS may lead to companies surrendering the data of their cybersecurity providers and cloud service providers without appropriate context, which may result in misinterpretation or incorrect use of the data. Although the system information is intended to exclude personal information captured under the Privacy Act, the system information laid out in the Explanatory Memorandum is sensitive in nature and these powers are substantial. Therefore, we recommend the powers provided under Subdivision A be removed from the final Bill.

We are similarly concerned with Section 30DJ, which provides the Secretary the power to require a relevant SoNS to install and maintain system information software that collects and records system information to be transmitted to the Australian Signals Directorate. While this requirement is intended as a "last resort" measure, we hold major concerns about the precedent this would set for any government intelligence agency to force private entities to install intrusive software on their private networks. Therefore, we recommend that the requirements under Section 30DJ also be struck from the Bill.

Focus Definition of "Data Storage and Processing Service"

We also have concerns about the insertion of the revised definition of "data storage and processing service." The proposed changes appear to confirm that that all forms of "as a service" computer services are captured under this definition. We recognize that Australia has inserted this amended

definition in an attempt to narrow the scope of what constitutes a "critical data storage or processing asset." However, because the requirements to notify data storage and processing suppliers are based on business-critical data, this definition may inadvertently capture a larger portion of the economy than necessary. In addition, some elements of business-critical data (e.g. risk management information) do not have the same context across different industries.

Similarly, for the definitions of "data storage or processing service" included in this Bill, we recommend retaining the "wholly or primarily" requirement when determining the eligibility of the asset, as per the definitions in section 12F of the SOCI Act. This would better target the legislation and not inadvertently capture many unrelated businesses.

It would also be helpful to build in an ongoing review process for the definitions of what constitutes a "critical infrastructure" asset. As sectors evolve or new technologies emerge, new "critical" services may emerge. It is not clear how the reforms would regard distributed assets (i.e., virtual power plants), which may constitute increasingly large parts of the relevant markets. This would also provide an opportunity for sectors and assets which no longer need to be covered by the Act to be removed from the regime.

***

Once again, we appreciate the opportunity to provide feedback as Australia seeks to reform and improve critical infrastructure risk management processes. We share in Australia's goal of improving cybersecurity and resilience across critical infrastructure. We urge Australia to consider our recommendations, which we believe will serve to improve cybersecurity and also provide certainty for businesses operating in Australia.