ITI Promoting Innovation Worldwide

August 26, 2021

ITI Comments on the Call for Views on Strengthening Australia's Cyber Security Regulations and Incentives

ITI appreciates the opportunity to provide feedback on Australia's call for views on the discussion paper "Strengthening Australia's Cyber Security Regulations and Incentives". We are grateful for the chance to remain consistently engaged in Australia's cyber security policy 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. Nearly a quarter of ITI's members are headquartered outside of the U.S.

We are supportive of Australia's efforts at reform and congratulate the Australian Government on its leadership in developing policies to protect against cyber security threats, and for recognizing that cybersecurity is a shared responsibility between the government, industry, and the community.

We previously responded to Australia's *2020 Cybersecurity Strategy Consultation* and many of the comments we provided there remain relevant in the context of this consultation, particularly:

- ***International Standards:*** ITI continue to advocate for Australian cybersecurity policies to support and utilize globally recognized and state-of-art approaches to risk management, such as the ISO/IEC 27000 family of information security management systems standards. We also recommend that Australia consider using other relevant tools that provide a common language to better help organizations comprehend, communicate, and manage cybersecurity risks (such as the U.S. NIST Framework and NIST SP800-171). Furthermore, we recommend that any approach should be implemented in a way that is adaptive and risk-based. Any approach should recognize that not all organizations are alike – in size, scope, complexity, business, cyber-risk or sophistication.
- ***Improving Cyber Hygiene, Skills, and Education****:* Broad and consistent public education on cyber hygiene and best practices is one of the important first lines of defense in network security. Consumer awareness regarding the importance of multi-factor authentication, software updates include patches, and awareness of phishing and other tactics used by hackers to access networks is foundational and should not be underestimated. Along with bolstering public awareness around

cybersecurity, ITI would also advocate for increased funding and promotion of Science, Technology, Engineering, and Math (STEM) education in Australia. Producing strong STEM students is not only valuable for creating the next generation of cybersecurity professionals, but increased funding can also help to promote vocational and mid-career education programs for STEM.

Below, we provide responses to several questions outlined in the paper. Although we do not answer every question, we have we have answered those that are most relevant to our membership.

The Current Regulatory Framework

3) What are the strengths and limitations of Australia's current regulatory framework for cybersecurity?

Given the overview provided in the Consultation Paper, it is clear that there are a myriad of policies and legislation in Australia that implicate cybersecurity in some way. The paper identifies "at least 51 Commonwealth state and territory laws that create, or could create, some form of cyber security obligation," which makes for an incredibly complex environment for businesses to navigate.

We also highlight several ongoing reforms that the Australian Government is pursuing, which add to this complex environment. Although Australia notes that the effort described in the Discussion Paper will be "complementary", we are concerned provisions contained within those pieces of legislation overlap with themes also explored in this paper. For example, the *Security Legislation (Critical Infrastructure) Bill of 2020* (hereafter *CI Bill*) contains a collection of provisions intended to improve cybersecurity across eleven critical infrastructure sectors, including related to board-level reporting on cybersecurity and supply chain risks, an expanded definition of critical infrastructure, and mandatory incident notification requirements. These provisions are expected to uplift cybersecurity across the Australian economy. Indeed, the Bill, when implemented, will capture an expanded scope of businesses as well as business of all sizes. The *Privacy Act of 1988* is also undergoing review in an effort to update the legislation to align with international best practices and will also have impacts on cybersecurity. As the Government is reviewing the current exemptions under the Privacy Act, other organizations may be brought into the Act's purview. This would likely result in improved cybersecurity across a broader array of groups, as they align their practices with the Australian Privacy Principles, including data breach notification requirements.

One of the major limitations, then, is that there is a disparate array of legislation and policy related to cybersecurity.

4) How could Australia's current regulatory environment evolve to improve clarity, coverage, and enforcement of cybersecurity requirements?

We believe there are several ways that the current regulatory environment might evolve.

First, we encourage the Australian Government to c**onsider how to streamline existing legislation to make the cybersecurity more understandable and easier to navigate.** It is clear that companies are operating in a very complex regulatory environment when it comes to cybersecurity and that navigating it can present major challenges to both businesses and the government. This is why we strongly emphasize the importance of harmonizing cybersecurity regulations, legislation, and policy to the extent possible. To be sure, it is counterproductive to create siloed, ministry/agency-specific, or country-specific approaches to cybersecurity, and we encourage governments to promote policies that break down artificial barriers that may serve to hinder cybersecurity efforts.

Second, we urge the Australian Government to **assess the impacts of legislation under review, including the CI Bill of 2020 and the Privacy Act of 1988.** The Government should assess how these reforms may impact the cybersecurity regulatory landscape and undertake a gap analysis before proposing any further regulations in this space. This will help to avoid unintended consequences, duplication and reduce the regulatory burden on the affected companies.

Finally, **we believe that the Australian Government should focus on providing incentives to achieve improvements in cybersecurity, as opposed to introducing additional regulation.** Creating and implementing new regulations can be slow, complex, and costly. In contrast, incentives are generally welcomed by industry and can be adopted into business practices and processes quickly. Incentives may offer the quickest way to uplift cyber security across the economy and do it at scale. Given the rapid emergence of cyber threats and the limited cyber maturity of Australian organisations – particularly SMEs – we encourage the Government to focus less on regulation and compliance, and instead focus on incentives and educational support to help reduce upfront costs of resource burdens on SMEs for cyber resilience. For example, Australia could amend its tax code to provide cybersecurity investment incentives, such as allowing for tax depreciation or offsets for investments in cyber security and resilience. Alternatively, Australia could consider providing digital vouchers to encourage investment in cybersecurity. Similarly, the Australian government could provide additional educational support through official guidance and best practice resources as well as free cyber 'health checks' – which could be made available through existing small business representative networks. The Government could also consider leveraging the Corporations Act -- where directors' key duty is to the shareholders and profit. Better resourcing and prioritizing of cyber people/process/technology controls would be facilitated by efforts to better quantify the risk of bad behavior and its potential impact on the financial wellbeing of the organization.

Governance Standards for Large Businesses

5. What is the best approach to strengthening corporate governance of cyber security risk? Why?

The focus of Chapter 4 is on ways to 'encourage stronger cyber security risk management within *large* businesses' [emphasis added]. As we noted above, the pending *CI Bill* will likely impact, if not directly regulate, almost all large businesses in Australia. It seems likely that many governance issues raised in this paper will be addressed by the Bill's requirement that the board sign off on risk management plans addressing cyber security, which in turn will be shared with the Federal Government. In line with our recommendations above, we encourage the Government to assess the impacts of the *CI Bill* before introducing new regulations related to corporate governance, voluntary or otherwise, and thus recommend maintaining the status quo until that assessment is finished.

6. What cyber security support, if any, should be provided to directors of small and medium companies?

The baseline public education described above (importance of multi-factor authentication, software updates include patches, and awareness of phishing and other tactics used by hackers to access networks), as well as more in-depth cybersecurity training, should be encouraged and offered to all businesses, including SMEs.

Jointly with private sector entities, the Government should seek to establish a cybersecurity information hub for Australian businesses seeking educational materials. It may also be worthwhile to partner with Managed Security Service Providers (MSSPs), Cloud Service Providers (CSPs), ISPs and cyber security companies to identify and/or create tailored offerings for SMEs that are cost effective and provide holistic security, alleviating some of the technical burden currently facing Australian SMEs. We also encourage the Government to consider subsidized support via an SME cybersecurity grants program or via tax incentives.

Standards for Smart Devices & Cybersecurity Labeling

Recognizing that governments around the world have started to consider cybersecurity labeling as a mechanism to better understand and communicate security features in ICT products, ITI released *Cybersecurity Labeling: A Guide for Policymakers* in April 2021. Indeed, we recognize that end-user awareness can play an important role in improving cybersecurity. However, end-users often have limited insight into the presence of security features in a finished product, device or services prior to purchase, which hinders informed buying decisions. Therefore, providing end-users with clear information about companies' adherence to cybersecurity standards and discrete topics such as the security features/functionality in devices or services can foster market competition based on security, build trust, and help end-users fulfill their role in maintaining security.

We encourage Australia to consider many of the recommendations we include there, as they are directly relevant to Australia's efforts to establish a labeling program. As a general matter, however, we recommend against establishing a mandatory standard for smart devices. Indeed, we believe that a voluntary approach to labeling is more appropriate, as it will allow for necessary flexibility and will better facilitate innovation.

Specific answers to questions

11) What is the best approach to strengthening the cybersecurity of smart devices?
12) Is ETSI EN 303 645 appropriate?

The best approach to strengthening the cybersecurity of smart devices is one that is multi-faceted. We encourage stakeholders to take thoughtful, holistic approaches to managing both the security of devices and the networks and complex ecosystems that comprise global IoT security.

To strengthen cybersecurity for smart devices, we recommend that any policy Australia chooses to develop, whether voluntary or mandatory, aligns its scope and definitions with international standards and best practices.

We note that the consultation proposes that Australia adopt key provisions of ESTI EN 303 645 v.2.1.1 to "ensure international consistency and adoption of best practices" in a mandatory standard. While EN 303 645 is likely to inform forthcoming requirements in the EU, it is unlikely that it will be widely adopted by governments outside of the EU, given its vertical nature. In line with the Australian government's commitments under the WTO TBT Agreement, wherever possible, we strongly encourage reference to international standards and encourage Australia to adopt global best practices on smart devices, especially related to IoT security. Many governments are currently following and participating in the development of horizontal international standards governing IoT security and privacy – device baseline requirements (ISO/IEC 27402), which may help to inform future requirements in this space.

We also recommend referencing commonly used process standards in the ICT space such as the ISO/IEC 27000 series and the IEC62443 suite of standards. To ensure alignment, we encourage Australia to take these international standards into account when finished, while leaving open the possibility of referring to other international standards in the future. It is important to emphasize that any deviations from international standards can have a serious effect on trade, such as requiring suppliers to meet different technical specifications, forcing duplication of testing and requirements, delaying the entry of goods into market, and inevitably reducing innovation and competition.

In terms of scope, we encourage Australia to utilize the following definitions: an ***IoT device*** is a device that has at least one **transducer** (*sensor or actuator*)[1] for interacting directly with the physical world and at least one **network interface**[2] [a notion accepted by the ISO/IEC SC41 IoT Device definition in 20924] and **is not** a conventional Information Technology device (e.g., smartphones and laptops). Ultimately, ITI recommends that all definitions align with international standards and best practices, particularly as a means of distinguishing between IoT devices and general-purpose computing devices (such as laptops, personal computing systems or smart phones) for the purposes of potential new requirements. Drawing this distinction will better address the computing and security capabilities of in-scope IoT devices and will allow for the development of an approach that is more readily actionable and easy to apply.

It is our strong view that for any legislative proposal to facilitate innovation, it must be accompanied by the necessary policy flexibility to allow regulators and industry alike to leverage, global, industry-driven, voluntary consensus standards. This is increasingly relevant as technological advances render regulators' task of keeping pace with corresponding policy questions more difficult. To the extent that any new requirements are predicated on either country or region-specific standards, or only consider a limited range of available international standards, this will inevitably lead to regulatory divergence that will not only affect market access but may have a detrimental impact on cybersecurity for products and services marketed in multiple jurisdictions.

We also encourage Australia to consider that even if security requirements are uniformly set, such requirements are not adequate to respond to all security challenges and users cannot always be protected. As such, we recommend that as a follow-on body of work in the future, Australia also consider how it can develop and promote policies to secure IoT at the network level, in addition to the device level.

An IoT device might be built to the strongest security standards at the time of deployment, but at the end of the day problems can still occur, including unforeseen technical challenges, human errors, exploited vulnerabilities, or lack of good cyber hygiene. Thus, outcome-based operational security requirements are essential.

We recommend that Australia consider including technical recommendations at the network level in the future, including:

[1] ***Transducer***: A portion of an IoT device capable of interacting directly with a physical entity of interest. The two types of transducers are *sensors and actuator*. ***Sensor***: A portion of an IoT device capable of providing an observation of an aspect of the physical world in the form of measurement data; ***Actuator***: A portion of an IoT device capable of changing something in the physical world. *Cf*. ENISA's definition of an IoT in the ISD context: Internet of Things (IoT) as a cyber-physical ecosystem of **interconnected sensors and actuators**, which enable decision making. [See ENISA, Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures].

[2] In contrast, the proposed term 'network-connectable' ("has one or more network interfaces that can receive and/or transmit digital data") **does not include** the actuating, sensing function that distinguishes the IoT ecosystem (compare also to ENISA approach) and therefore is not appropriate.

- Enable Constant Visibility of All Devices and Their Behaviors at All Times
  Organizations leveraging IoT devices and systems need to have constant real-time visibility and granular control across traffic passing through their networks. Only then can they detect and stop malicious threats and activities, such as IoT-based botnets. The Government should encourage organizations to leverage technology on a voluntary basis to enable complete and continuous visibility of their networks and to enable discovery, identification, security, and optimization of their connected IoT devices.
- Adopt a Zero Trust Approach
  Under the Zero Trust concept, an organization should not automatically trust any unauthenticated activity inside or outside its network perimeters. Instead, an organization must authenticate every user or device trying to connect to its systems before granting access, including IoT devices. That level of granular control around key critical infrastructure and data allows cybersecurity risk management to become more effective.
- Segment Networks Where IoT Devices are Deployed
  Organizations that apply micro-segmentation of IoT devices based on device risk profiles are more likely to avoid cross-infections between IT and IoT systems. Through segregating and limiting the ability of legacy, low-patched and generally high-risk IoT devices to communicate with other IT assets, organizations can prevent threats from spreading across their networks.

16) What is the best approach to encouraging consumers to purchase secure smart devices? Why?

We believe that the best approach is to improve consumer education regarding secure smart devices, particularly around assessing levels of risk. Helping consumers identify when it is practical to employ smart devices with built-in security features will enable consumers to make more informed decisions when considering anticipated risk levels and financial costs.

17) Would a combination of labelling and standards for smart devices be a practical and effective approach? Why or why not?

While labeling can be a beneficial way to communicate the security features of smart devices to consumers, it is also not a one-size-fits-all solution nor a silver bullet solution. We believe that labels can help to incentivize the adoption of underlying security features and practices, but labels can only do so much. Cybersecurity is an iterative process that requires a diverse set of practices. Labeling should not act as a substitute for these other important practices intended to build trust and improve cybersecurity, like undertaking secure development lifecycles. We recognize that labels can provide useful information to consumers that they may not otherwise have access to and can therefore help to inform purchasing decisions. We are supportive of voluntary labeling schemes for finished consumer products in certain verticals (e.g., consumer IoT), where a clear benefit is established (e.g., increasing end-user awareness). However, in more sophisticated verticals (e.g., enterprise), where end-users do not have the same "information asymmetry" problem as exists between manufacturers and consumers, voluntary labels may have no discernible benefit.

20) Should a mandatory labelling scheme cover mobile phones, as well as other smart devices? Why or why not?

This would be difficult to achieve in practice given the variables involved and how interaction between hardware, operating system software, and applications make the difference between secure and vulnerable. For example, a brand-new smartphone running an outdated version of an operating system could be less secure than an older phone running the latest fully patched operating system.

21) Would it be beneficial for manufacturers to label smart devices both digitally and physically? Why or why not?

ITI supports digital formatting in particular to indicate risk because it allows for a more flexible system that is more easily updated than a physical label in response to changes to the risk environment and standards. As we mentioned in response to Q11 above, however, we discourage Australia from mandating adherence to specific standards.

Privacy

8) Would a cyber security code under the Privacy Act be an effective way to promote the uptake of cyber security standards in Australia? If not, what other approach could be taken?

It is not clear to us that leveraging the Privacy Act would be an effective way to promote the uptake of cyber security standards across the economy. A code under the Privacy Act would not apply to small enterprises, as the Privacy Act has exemptions for companies who have a turnover of less than 3 million annually. This would mean that more than 30% of the Australian economy would not be covered by the Code.[3] Larger companies are already handling personal information in a manner consistent with the Privacy Act and in many cases are also compliant with other robust international frameworks, such as General Data Protection Regulation (GDPR). Some of these companies will also be subject to, and impacted by, the CI Bill and the impacts of these regulations should be assessed before further regulatory action is taken.

9) What cost effective and achievable technical controls could be included as part of a code under the Privacy Act?

[3] https://www.asbfeo.gov.au/sites/default/files/ASBFEO%20Small%20Business%20Counts%20Dec%202020%20v2.pdf

As we mention in our answer to the question immediately before this, we have some reservations about whether this approach is the most sensible to achieve improved cybersecurity. A single set of security controls is not applicable to all organizations or to all situations – instead, such controls should be risk-based and commensurate. Beyond that, most small businesses will not have the capital or expertise to comply with these controls, meaning the impact will be net negative. It is our view that implementing changes based upon available information and free GOTS software would be less impactful to the bottom line of business and more effective in improving security

That being said, if Australia decides to include technical controls in the Privacy Act, Australia should ensure that any required controls align with the technical controls mandated under the European Union's GDPR, particularly the new technical measures required under the Standard Contractual Clauses (SCCs) issued by the European Commission on 4 June 2021 governing the transfer of personal data from the European Economic Area (EEA) to third countries pursuant to GDPR. From an international standpoint, it becomes difficult and often confusing for both individuals and companies to adhere to multiple standards, regulations, and law. As GDPR has become the de facto international privacy standard, Australia should ensure that it is aligned with GDPR.

Health Checks

23) Would a health check program improve Australia's cybersecurity?

To the extent that the Government could offer free, voluntary health checks, this could be an additional helpful resource. ITI does not believe a mandatory health check would provide meaningful incentives or next steps for businesses to enhance their security.