

ITI Response to Australia 2020 Cybersecurity Strategy Consultation

October 31, 2019

The Information Technology Industry Council (ITI), appreciates the opportunity to submit the following comments in response to [Australia's 2020 Cybersecurity Strategy consultation](#).

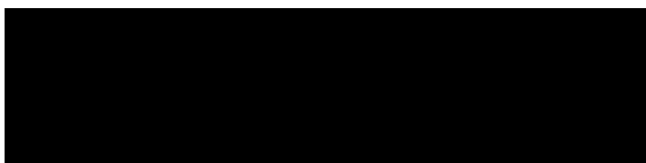
About ITI

ITI is the premier advocate and thought leader in the United States and around the world for the information and communications technology (ICT) industry, and represents leading companies from across the ICT sector, including hardware, software, digital services, semiconductor, network equipment and Internet companies. The tech industry shares the goal of improving cybersecurity, and we believe our interests are fundamentally aligned with Australia's in this area. Our members are global companies with complex global supply chains as well as robust security solutions for products and services. We look forward to bringing global best practices to this discussion in order to support Australia in developing its 2020 cybersecurity strategy.

Overview

The ICT industry has long maintained that efforts to improve cybersecurity, including supply chain security, must be based on effective risk management of a dynamic and ever-evolving set of threats. Cybersecurity is not an end state, but rather a continuous process of protecting the global digital infrastructure and its users. No sector of the economy is without some inherent risk, whether that is the result of a natural disaster, a malicious automated attack, or simple human error. As cyber and supply chain attacks become increasingly sophisticated, the adoption of comprehensive risk management strategies is critical for organizations of all sizes and across all sectors, particularly those managing complex global supply chains. By integrating technologies, people, and processes into an overall risk management framework, limited resources can be most efficiently focused on where the need is greatest. We must consider the large and growing number of threats and the number of ICT products and services ICT companies globally in order to understand the scope of the risks that must be managed and the associated policy challenges.

In ITI's view, Australia has made significant progress since releasing its 2016 Cybersecurity Strategy. We agree with the priorities identified in the 2020 Cybersecurity Strategy, and particularly appreciate the focus on increasing public-private partnerships (PPPs). In our comments below, we also provide recommendations on cyberthreat information sharing, coordinated vulnerability disclosure, cybercrime, supply chain security, cyber hygiene and education, encryption, and international engagement.



@ info@itic.org

www.itic.org

@iti_techtweets

Comments and Recommendations

Shared Management

Cybersecurity is a shared responsibility – neither governments nor companies can address it alone. Well-intended policies may have unintended consequences on security, innovation, and competitiveness – which is why public-private sector cooperation is imperative. The private sector owns and operates most networks as well as elements of critical infrastructure. Those owners and operators must be viewed as essential partners in ensuring the protection of this critical infrastructure.

PPPs and other multistakeholder approaches are essential to addressing supply chain security. Government and industry often have access to unique information sets – only when this information is shared can all relevant stakeholders see the complete picture. These partnerships are essential to 1) identify potential threats; 2) understand how and whether the risk can be managed; and 3) determine what actions should be taken to address risks without yielding unintended consequences. The private sector ICT community has been foundational in developing the infrastructure of cyberspace and for well over a decade has provided leadership, innovation, and stewardship in all aspects of cybersecurity, including helping to develop and participating in numerous PPP structures and efforts.

Many countries have launched multi-stakeholder initiatives to address cybersecurity challenges. For example, the EU has appointed the European Network and Information Security Agency (ENISA) to create a private sector working group to develop the consumer IoT certification scheme. In the United States, the Department of Homeland Security (DHS) has established an ICT supply chain risk management task force¹ with IT and telecommunication sectors, which ITI co-leads on behalf of the IT sector. The task force is convened by the DHS's Cybersecurity and Infrastructure Security Agency (CISA) and includes more than 60 organizations from across the ICT industry and federal government to develop workstreams and policy recommendations to tackle global supply chain security issues. We recommend Australia continue its efforts to build and maintain strong partnerships with the private sector and seek active participation of the private sector in order to direct resources appropriately.

Cyberthreat Information Sharing

ITI encourages the voluntary sharing of relevant, actionable threat information between and among parties. This helps address cybersecurity holistically by allowing the appropriate stakeholders to take measures to protect networks and mitigate risks that may have repercussions across networks.

Coordinated Vulnerability Disclosure

Sensible vulnerability disclosure and remediation practices by all parties are essential to the security of the digital ecosystem is an important facet of information-sharing. The ICT sector takes timely action to analyze and mitigate the risk of identified vulnerabilities and follows responsible disclosure practices to notify suppliers, resellers, customers, and others as appropriate. We are

¹ DHS ICT Supply Chain Task Force. <https://www.dhs.gov/news/2018/11/15/dhs-announces-ict-supply-chain-risk-management-task-force-members>

supportive of the Australian government in its continued adoption of transparent policies to disclose vulnerabilities to technology vendors in a timely fashion to enable them to better protect against cybersecurity attacks and that encourage responsible disclosure of vulnerabilities by security researchers to technology vendors.

Furthermore, we recommend that Australia increase awareness and encourage use of Australia's automated indicator sharing (AIS) system. If the system does not already do so, we recommend establishing an anonymized threat indicator sharing system to ensure broad awareness of potential threats.

We would also support the Australian government in establishing processes and mechanisms through which companies can disclose vulnerabilities and patches, as appropriate, to encourage prompt and widespread measures to secure networks.

These relationships and processes also enable governments and private sectors to discuss appropriate next steps, including potential surveillance of bad actors and/or sharing information with other nations' computer emergency readiness teams (CERTs).

Law Enforcement to Tackle Cybercrime

Governments investigating criminal activities increasingly require extraterritorial access to electronic evidence. To increase public safety and security and make investigations and prosecutions more efficient, governments should expand investment in staffing law enforcement assistance offices and request mechanisms, including those that handle Mutual Legal Assistance Treaties (MLATs). We also encourage governments to leverage existing multilateral agreements and mechanisms, such as the Budapest Convention on Cybercrime and Interpol's Cybercrime Center. We commend Australia for its leadership on global cybersecurity and hope that it also continues to prioritize both using and strengthening these mechanisms.

International Standards

We recommend that Australia's cybersecurity policies continue 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. ITI would 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 Framework² 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. The government of Australia should continue the promotion of existing international standards for developing certification schemes, so as to avoid the creation of duplicative, overly burdensome, or divergent schemes that are challenging for companies to comply with. In building up cybersecurity expertise and capacity,

² NIST Cybersecurity Framework. <https://www.nist.gov/cyberframework>

we also encourage the government of Australia to look to international standards and best practices and consider tools like the NIST NICE Framework.³

Supply Chain Security

Supply chain risk management (SCRM) remains a multifaceted challenge. On the one hand, SCRM is one element of an organization's overall cybersecurity risk management program. On the other hand, a SCRM program must address much more than just cybersecurity threats to IP, systems and networks, but also threats that are physical (e.g. building security), personnel-based (e.g. insider threats), economic (e.g. cost-volatility), legal (e.g. weak IP laws), development or manufacturing-related (e.g. compromises in system, hardware, or software development lifecycle processes or tools), or external threats such as those related to environmental, geopolitical or workforce related factors.

Global ICT SCRM challenges ultimately call for globally scalable solutions, and we encourage cross-border collaboration on this issue. Because ICT supply chains are increasingly global, policies that exclude technologies based on vendor or product nationality not only inhibit international trade, but also harm cybersecurity by preventing cutting-edge security solutions developed across the world to be adopted within the country. In working to ensure supply chain security, Australia and other economies should take common approaches to technology-related national security risks – including through promotion of global, consensus-based, industry-led standards – to avoid harmful fragmentation of markets. The *Prague Principles on 5G Security*⁴ provide a good blueprint for this type of activity.

Due to this multifaceted challenge, SCRM is another area in which PPPs are crucial. The Australian government can consider existing models of PPPs, such as the DHS-sponsored Supply Chain Risk Management Task Force in the U.S., which is co-led by ITI on behalf of the IT SCC.

Improving Cyber Hygiene, Skills, and Education

We commend Australia's prioritization from its 2016 strategy to increase cybersecurity skills and create a "cyber smart nation." We continue to encourage the growth of this skill set and increase organizational awareness across the government and industry verticals that face increasing cybersecurity challenges as they become more connected and utilize new digital solutions to advance businesses.

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 including patches, and awareness of phishing and other tactics used by hackers to access networks is foundational and should not be underestimated. Additionally, this type of baseline education as well as more in-depth cybersecurity training should

³ "National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework"

<https://csrc.nist.gov/publications/detail/sp/800-181/final>

⁴ "The Prague Proposals: The Chairman Statement on Cybersecurity of Communication Networks in a Globally Digitalized World." May 3, 2019, available at: <https://www.vlada.cz/assets/mediacentrum/>

[aktualne/PRG_proposals_SP_1.pdf](#)

be encouraged and offered to businesses. This is particularly important for smaller companies that may not consider themselves vulnerable to cyber attacks. Additional guidance is also useful for businesses in critical infrastructure sectors that have connected information technology and operational technology.

Along with bolstering public awareness around cybersecurity, ITI also would 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.

Finally, as noted above under “International Standards” we suggest Australia promote the use of a standardized framework to categorize and describe cybersecurity work that could be used by academic institutions and vendors to standardize their curricula and certification, and employees and employers to best match needed job skills, such as the NIST NICE Framework.

Supporting Encryption

Protecting and defending against national security and terrorist threats and upholding and enforcing criminal laws are fundamental missions of governments around the world. Technology can be a central tool in furthering these missions. Consistent with the tech sector’s unwavering commitment to security and privacy, we are prepared to work transparently as a part of collaborative efforts with governments to improve the technical competencies of their workforce, to build capacity to understand the rapidly evolving nature of technology, to help prioritize resources, and to leverage technological innovation to assist in conducting lawful investigations.

At the same time, robust cybersecurity and data protection are essential to trust in technology products, services, and systems, and robust encryption is fundamental to building such trustworthy and reliable technology products, services, and systems. The tech sector does not deliberately undermine the security of its products, services, systems, or data, and it maintains the confidentiality of source code and design information to protect the security of customers, products, and services. In that sense, ITI opposes imposing legal mandates on technology providers to decrypt information when they do not retain physical possession of encryption keys or other technical means to decrypt such information, as well as other requests to circumvent or compromise the security features in those products or services, including requests to escrow encryption keys or source code. We welcome continued engagement with the Australian government over implementation of the recently passed Assistance and Access Bill.

International Engagement

Along with Australia’s efforts to protect its own networks and citizens, Australia can also fortify cybersecurity efforts in the Asia-Pacific region in particular. As a respected global cybersecurity partner and highly regarded player in the Asia-Pacific region, ITI acknowledges that Australia has a unique, valuable role in the region to engage in dialogue with other governments on these issues and prevent the proliferation of policies that may unintentionally curb cybersecurity efforts and economic growth. Since Australia launched its inaugural International Cyber Engagement Strategy in 2017, the country has developed deeper partnerships in the region and across the world to increase awareness of risks, which has been imperative to help other governments facing similar


challenges and also helps Australia to better anticipate threats. We hope that Australia can continue to deepen cooperation with other governments on cybersecurity issues by sharing technical training, best practices, as well as assessments of threats and risks.

Conclusion

Thank you for receiving our comments. ITI and its members hope to be strong partners of the Australian government going forward, and we would welcome further discussion of any of the above.



Promoting Innovation Worldwide

 itic.org