ITI Promoting Innovation Worldwide

ITI Submission to Australia Cyber and Critical Technology International Engagement Strategy (CCTIES) Consultation

June 16, 2020

Contact:
Naomi Wilson
Senior Director of Policy, Asia
Information Technology Industry Council
nwilson@itic.org
+1 (202) 626-5733

About ITI

The Information Technology Industry Council (ITI) appreciates the opportunity to submit this response to Australia's Department of Foreign Affairs and Trade. ITI is the premier advocate and thought leader 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.

Overview

As a respected global cybersecurity partner and highly regarded player in the Indo-Pacific region, 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, practices, as well as assessments of threats and risks.

Comments and Recommendations

We provide the below high-level recommendations along with more detailed comments following this section.

- Promote effective and international best practices and standards for cybersecurity and discourage country-unique standards and certifications.
- Uphold a multi-stakeholder approach to cybersecurity and coordinate on information and threat sharing as well as vulnerability disclosure.
- Prevent misguided data localization policies across the region and promote the free flow of data and the growth of global business.

- Oppose policies that mandate forced transfers and disclosure of technology, source code, algorithms, or encryption keys.
- Promote the benefits of AI with international and regional partners to establish common principles and prevent premature or overly burdensome regulation.
- Advance the development of secure 5G infrastructure in partnership with the private sector throughout the Indo-Pacific region.

International Engagement and Objectives

Promote International Best Practices on Cybersecurity

In an increasingly digital world, the full potential of the modern economy cannot be realized without cybersecurity. Both technology and cybersecurity threats are evolving globally, and neither technologies nor threats are bound by national borders. However, problematic cybersecurity laws, regulations, and standards continue to emerge in the Indo-Pacific region, including country-unique testing and certification requirements that are often redundant and create trade barriers. ITI would caution against the creation of additional certification prior to comprehensive assessment of existing mechanisms and rules and would discourage schemes that deviate from international standards and best practices. Instead, we recommend that governments identify how any new certification schemes would link to existing relevant global schemes. ITI encourages the Australian government to continue to promote the use of existing international standards and support industry leadership in standards development.

We recommend that the CCTIES 2020 include international industry-backed approaches to risk management, such as the ISO/IEC 27000 family of information security management systems standards and the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity[1]. We applaud Australia's engagement and initiative to establish robust Computer Emergency Response Teams (CERTs) in the region and hope that Australia will strengthen both the operation of CERTs and other technical assistance in the Indo-Pacific region as a means of promoting best practices. We suggest focusing on Vietnam, Indonesia, Thailand, Malaysia, and India.

Uphold a Multi-stakeholder Approach

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.

Public-private Partnerships (PPPs) and other multi-stakeholder 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

[1] NIST Framework for Improving Critical Infrastructure Cybersecurity. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

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.

We would encourage Australia to continue leveraging its mechanisms for domestic engagements, such as the Critical Infrastructure Center and the Australian Cyber Security Center, in promoting similar mechanisms to other countries in the Indo-Pacific. Australia can share experiences, approaches, and best practices around PPPs as a means of boosting overall capacity building in the region.

Strengthen 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. We encourage the Australian government to continue utilizing trade negotiations to encourage cybersecurity cooperation with important trading partners, as was done through the E-Commerce chapter in the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP). Further, we encourage continued enhancement of CERT-to-CERT partnerships to facilitate timely sharing of vulnerability indicators and patches.

Bolster Coordinated Vulnerability Disclosure (CVD)

Sensible vulnerability disclosure and remediation practices by all parties are essential to the security of the digital ecosystem and important facets of information-sharing. Since Australia's 2016 Cybersecurity Strategy, the Australian government has focused critically on strengthening partnerships with the ICT sector to disclose vulnerabilities and enable companies to better protect against cybersecurity attacks. We hope Australia will continue to encourage responsible disclosure of vulnerabilities by security researchers to technology vendors and align with broadly adopted industry best practices. Australia could also take advantage of its cybersecurity leadership in the Indo-Pacific region to promote such best practices as articulated in the ISO/IEC 30111 (2013) and 29147 (2018).

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

Coordinate on 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 Agreements or Treaties (MLAA/Ts) and the Clarifying Lawful Overseas Use of Data Act (CLOUD Act). We recognize Australia's recent efforts to amend the Telecommunications Interception and Access Act to support and enable negotiations for a potential U.S.-Australia CLOUD Act agreement. We

urge Australia to work closely with industry and the public to ensure that any amendments Australia adopts are appropriately scoped to balance the needs of law enforcement as well as privacy and security concerns of the private sector and individuals. We commend Australia's leadership in the region to leverage existing multilateral agreements and mechanisms, such as the Budapest Convention on Cybercrime and Interpol's Cybercrime Center. We hope that Australia also continues to prioritize both using and strengthening these mechanisms.

ITI also appreciates Australian participation in the UN Group of Governmental Experts (GGE) process to advance international cyber norms. We encourage the Australian government to continue to work multilaterally to advance these processes and outline steps for implementation of key norms of behavior in cyberspace. Australia can continue to build on these efforts and provide a model for the Indo-Pacific region.

Promote International Standards

We recommend that Australia's cyber and critical technology 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 Framework[2] 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.

Where a comprehensive assessment of existing rules points to a need for voluntary certification, the government of Australia should promote the use of international standards. Reliance on international standards will help to avoid the creation of duplicative, overly burdensome, or divergent schemes that are challenging for companies to comply with. Where international standards may not exist, we recommend recognizing other compliance schemes that are equivalent to Australia's national programs to increase choice in the market and lower market entry barriers. DFAT should consider the benefits of accepting alternative but equivalent means of demonstrating compliance for certification schemes and consider advancing these principles in its international engagement. In building up cybersecurity expertise and capacity, we also encourage the government of Australia to look to international standards and best practices and consider tools like the NIST NICE Framework.[3]

Prevent Data Localization Policies and Facilitate Cross-Border Data Flows

We are grateful for Australia's global leadership on enabling cross-border data flows and preventing data localization, including its adoption of the APEC Cross-Border Privacy Rules (CBPR), its convening role in the ongoing WTO E-commerce Joint Statement Initiative (JSI), and various regional and bilateral trade policy initiatives. Australia is in a unique position in the Indo-Pacific to promote free flow of data across borders as a party to the CPTPP, which contains high-standard language on ensuring the cross-border flow of data and the prevention of data localization

[2] NIST Cybersecurity Framework. https://www.nist.gov/cyberframework

[3] "National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework" https://csrc.nist.gov/publications/detail/sp/800-181/final

measures. We would encourage Australia to continue promoting CPTPP language and the principles inherent to APEC CBPRs as it expands trade negotiations in the Indo-Pacific region.

Australia's partnership in this area is particularly important as economies across the Indo-Pacific region are increasingly drawn to regulations and legislation that would require companies to localize data. Data localization policies are not only ineffective in enhancing cybersecurity but create a "single point of failure" that increases the risk of data compromise. While they are also barriers to international trade and are often motivated by protectionism and the desire by governments to have greater control over content and political commentary, countries use a number of different justifications for their adoption, including privacy, cybersecurity, and law enforcement concerns. Unfortunately, many Indo-Pacific countries are seeking to develop or implement deeply problematic localization measures, including in India, Indonesia, and Vietnam.

Governments in the region are likely to find that such policies do not achieve their intended objectives and create undue harm to their economies. In addition to robust advocacy around data flows in trade negotiations, we encourage Australia to strengthen exchanges among technical, policy, and legal experts to address countries' concerns with data security and privacy and identify sound policies to achieve objectives. It is critical that Australia continues to show leadership in this area as ensuring open data flows while maintaining security of information will be a pre-requisite to success in an increasingly data-reliant global economy.

Risks and Opportunities

Artificial Intelligence

Artificial intelligence (AI) is an active research area with numerous applications and great potential for a variety of applications across nearly all sectors of the economy. The technologies are constantly evolving and improving, as are the tools to address some of the challenges around explainability, bias, and fairness.

We are already experiencing the benefits of AI in an array of fields. Startups, small and medium-sized enterprises (SMEs), and larger tech companies have all developed AI systems to help solve some of society's most pressing problems. Many others are using AI to improve their business, provide better public services and advance ground-breaking research that saves lives. This is particularly important in the age of COVID-19, where artificial intelligence is contributing to recovery, contact tracing, and groundbreaking research for treatments. Further, AI and machine learning are essential tools in cybersecurity to address today's automated, complex, and constantly evolving cyberattacks. In an increasingly sophisticated cyber landscape, attackers improve methods to penetrate organizations and evade detection. The main response to the large number, diversity, and sophistication of attacks is the application of machine learning to detect and automatically prevent malware, network intrusions, phishing sites, and many more.

The Australian government has done robust work to develop ethics principles and we commend the government's efforts to develop a framework that will build Australia's AI capacity. Australia should further the ethical development and use of AI globally by cooperating with its international partners to promote a shared understanding and common norms. As the AI ecosystem is global and the technology is not developed in regional siloes, Australia should also promote a reliance on industry-led, voluntary, consensus-based international standards for AI where appropriate. We

recommend that DFAT actively promote the benefits of AI and focus on technical assistance to key countries in the Indo-Pacific so that countries do not rush to regulate out of fear or misunderstanding, which could result in unintended, negative consequences.

Supply Chain Security

Supply chain risk management (SCRM) remains a multifaceted challenge that is growing more complex in a highly interconnected global trading system. While SCRM is an issue for all sectors, there are a number of new considerations for both governments and organizations in an increasingly digitized world. 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. Global cooperation is crucial in the age of deeply intertwined global supply chains. As governments in the Indo-Pacific and long-standing allies begin to seek more progressive SCRM policies, the Australian government can play a guiding role.

Supporting Lawful Access

Protecting and defending against national security and terrorist threats and upholding and enforcing criminal laws are fundamental missions of governments around the world. The tech sector is engaged in many collaborative efforts with governments to: improve the technical competencies of their workforce; build capacity; understand the rapidly evolving nature of technology; help prioritize resources; and leverage technological innovation to assist in conducting lawful investigations. At the same time, strong 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.

ITI supports rule-of-law based efforts on law enforcement needs, with strong privacy and cybersecurity protections to enable effective cooperation between tech companies and governments on issues related to encryption. In its engagement with other governments in the Indo-Pacific region, DFAT can promote collaboration with the tech sector that protects privacy and cybersecurity, rule-of-law based law enforcement access, and transparency. ITI also supports the Australian government's pursuit of trade agreements that continue to enshrine the importance of protecting code, algorithms, or encryption keys or other proprietary information relating to cryptography.

[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

Secure 5G Infrastructure

5G promises transformative mobility by offering an enhanced mobile broadband experience and enabling the mass digitization of businesses and industries. The early stages of 5G evolution will revolve around delivering higher data speeds, latency improvements and the functional redesign of mobile networks to enable greater agility, efficiency and openness. While 5G will be transformative across sectors, the increased interconnectedness brought about by 5G will also increase security risks for both operators and end users. Furthermore, the convergence of mobile and fixed line network infrastructures' may also increase risk due to insecure interconnectivity points. These new risks are relevant not just to the telecommunications and service provider sector, but also the wide swath of industries and critical infrastructure providers that will rely on 5G. As nations continue to roll out 5G infrastructure, it is important that they seek to deploy 5G networks that are secure and trusted. This approach may help to avoid some of the challenges we have securing today's 3G and 4G networks.

We recommend that DFAT work with the private sector and regional counterparts to highlight the importance of 5G network security. DFAT should also emphasize the importance of taking a holistic approach to 5G security, encouraging governments to focus on threats beyond those associated with supply chain actors and equipment and instead considering the full range of security risks to mobile network infrastructures, applications, and services.

Conclusion

In a time of rapidly evolving tech and a dynamic threat landscape, ITI and its members believe that Australia has been, and can continue to be, a cyber leader in the Indo-Pacific region.

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.