U.S. CHAMBER OF COMMERCE

June 16, 2020

Dr. Tobias Feakin
Ambassador for Cyber Affairs
Australia Department of Foreign Affairs and Trade
RG Casey Building., John McEwen Crescent
Barton, ACT 0221
Australia

Subject: Public Consultation on Cyber and Critical Technology International Engagement Strategies

Dear Ambassador Feakin:

The U.S. Chamber of Commerce ("Chamber") is the world's largest business federation, representing the interests of more than three million businesses and organizations of every size, sector, and region. Many of the Chamber's members have longstanding, substantial investments in Australia and collectively employ thousands of Australian citizens. We are strong supporters of a productive and economically vibrant U.S.-Australia relationship and appreciated the insights into global cyber challenges that you presented to the Chamber's cyber mission to Israel's Cyber Week last year. In the spirit of that continued dialogue, we offer here a few thoughts, and we would welcome the opportunity to convene a virtual discussion with you and your team to explore them further.

The Chamber welcomes the opportunity to respond to the International Cyber Engagement Strategy update of the Department of Foreign Affairs and Trade (DFAT). Overall, we greatly support DFAT's continuous efforts to enhance its cybersecurity leadership and collaboration, and we appreciate the willingness of the Government of Australia to consult with industry throughout the process. The Chamber believes that taking industry voices into consideration strengthens the end result.

Our goal is to foster a more resilient ecosystem through the creation of industry-led, market-based cybersecurity solutions. We strongly believe that a multi-

stakeholder approach to cybersecurity is the most effective way to encourage economic activity while ensuring the security of digital infrastructure.

The Chamber broadly supports the inclusion of critical technologies as part of a strategy to guide international engagement across the full range of Australian interests in cyber affairs. The Chamber and our members recognize the critical national security importance of managing supply chain risk for critical technologies. Ensuring that these technologies are resilient and secure from efforts by nation state and other malicious actors to sabotage or disrupt their availability and integrity is a vital priority. However, we would like to re-emphasize several key principles that we encourage Australia to promote regarding cyberspace and critical technology:

- **Continue to pursue a risk-based approach that fosters innovation**. The Chamber strongly believes that risk management is foundational to effective cybersecurity. As governments enact cybersecurity policies and frameworks, we recommend risk-based approaches that rely on best practices to identify and protect against threats to critical infrastructure, information and communication technologies (ICT), fifth generation (5G) networks, and the internet of things (IoT) security. Approaches to cybersecurity should focus on the assessment and identification of risk and methods for minimizing risk. Such an approach will foster innovation and reward security and innovation since the approaches will be able to adapt to new technologies. The Chamber has cautioned governments against a singular focus on the replacement of equipment provided by high-risk vendors. Such equipment's deployment, use, and maintenance are specific to individual cases. The isolation and monitoring of identified equipment should be set forth with specificity and shall be based on objective facts with evidence of a national security threat, be technology-neutral, and risk-based. Industry-leading solutions that are commercially available that might be appropriate for risk management use include passive vulnerability scanning, continuous diagnostics and mitigation, and intrusion detection systems.

- **Align with existing international best practices.** Government cybersecurity strategies should promote technical compatibility and interoperability to the maximum extent possible. The Chamber recommends that approaches to cybersecurity be based on industry-led international standards and frameworks. Private industry greatly benefits when governments incorporate existing foreign cybersecurity frameworks, such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework or the International Organization /International Electrotechnical Commission ("ISO/IEC")

27001:2013, into any future policy enactments. It is critical that approaches to cybersecurity adhere to industry-vetted actions that businesses can take to assess and strengthen their state of security over time. Additionally, NIST is developing "Recommendations for IoT Device Manufacturers," and recent drafts align with the risk-based measured approach for which the Chamber advocates. Other sources of existing cybersecurity frameworks and best practices include: NIST Framework for Improving Critical Infrastructure Cybersecurity; Council to Securing the Digital Economy C2 Consensus on IoT security core capabilities baseline; and NISTIR 8259.

- **Place an emphasis on capacity building and information sharing.** Everybody is vulnerable, and cyber threats must be met with global information sharing and collaboration to improve and safeguard the IoT ecosystem. The Chamber encourages capacity-building and information sharing between the public and private sector. We believe that sharing information makes companies and government alike stronger while weakening adversaries and cyber bad actors. We encourage the active promotion of global information sharing to stakeholders in the IoT device space, in order to share threat intelligence and known vulnerabilities that could strengthen the ecosystem's defense against bad actors. While governments (e.g., computer emergency response teams, national cyber security centers) or industry (e.g., commercial off the shelve threat intelligence providers, information sharing and analysis centers) routinely sharing cyber threat information (e.g., signatures, indicators of compromise, vulnerability information, remediation) with private sector stakeholders, this information is structured and formatted whereas information on vendor- or product-based risk (e.g., the insertion of malicious code and/or other forms of compromise or exploitation) is not widely available. Future frameworks for sharing information with critical technologies supply chains may consider the following: (1) What supply chain information would be most valuable for the government and industry to mitigate the risk of sabotage? (2) Does such information exist in a public or private body or sharing platform that allows it to be accessible across the supply chain for risk management purposes? (3) How will national competent authorities share targeted intelligence and involve relevant suppliers in the assessment of risks to specific products? (4) What legal or policy barriers to bi-directional information sharing exist, including from substantial countervailing risks of IP loss and inadvertent dissemination of security vulnerabilities?

- **Build multi-stakeholder engagement forums for the joint industry and government collaboration.** The Chamber recognizes that governments are

increasingly focusing on the security of supply chains. Within our own government we are tracking up to 22 different supply chain risk management activities. As the Australian Government looks internationally, we urge you to consider the work of the DHS Information and Communications Technology (ICT) Supply Chain Risk Management (SCRM) Task Force as an industry supported framework. The Chamber believes it is a valuable instrument in collaborating on analysis and developing operational and policy recommendations for the ICT Supply Chain through the collaborative efforts of its membership. For reference, members of the SCRM include 40 major information technology (IT) and communications companies, along with 20 federal agencies. The SCRM task force's four working groups relate to: (1) information sharing, (2) threat assessments, (3) qualified bidders and qualified manufacturing lists, and (4) counterfeit products. The SCRM Task Force offers a useful multi-stakeholder model for coordinated industry and government supply chain risk management work

- **Seek common definitions for critical infrastructure, vital economic functions, and essential workers.** Over the past several months, the Chamber has witnessed enormous stresses on economies and the global supply chains that ensure security, growth, and innovation. Our experience in the U.S. has shown that a common understanding of the critical infrastructure, national critical functions (e.g., food transportation and logistics, call service centers, cloud services), and the essential workers that ensure the availability and integrity of those are vitally important. While the identification of critical infrastructure is a common international best practice for international capacity building, the identification of critical economic functions and a granular mapping of the essential workers is a new risk management activity. The Chamber urges governments and interconnected supply chain partners to develop a common approach to the identification of these essential workers.

The Chamber appreciates the opportunity to comment and welcomes the opportunity to provide additional information surrounding our general recommendations. The Chamber values our ongoing close relationship with DFAT and looks forward to future collaboration. If you have any questions or if we can provide more information, please contact Executive Director for Cybersecurity, Vince Voci (vvoci@uschamber.com or Senior Director for Global Regulatory Cooperation, Abel Torres (atorres@uschamber.com).

cc: The Hon. Arthur Sinodinos, Ambassador of Australia to the United States
The Hon. Arthur Culvahouse, Ambassador of the United States