U.S. CHAMBER OF COMMERCE

Comments on the Department of Home Affairs Consultation Protecting Critical Infrastructure and Systems of National Significance

September 2020

The U.S. Chamber of Commerce ("Chamber") is the world's largest business federation, representing 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. In the spirit of our past fruitful international collaboration with the Department of Home Affairs ("Home Affairs") and the Department of Foreign Affairs and Trade (DFAT) on critical infrastructure cybersecurity, code of practice, and 5G security issues, we offer here a few thoughts. 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 Protecting Critical Infrastructure and Systems of National Significance Consultation of the Home Affairs. Overall, we support the Home Affair's continuous efforts to enhance its cybersecurity leadership and collaboration towards protecting critical infrastructure. We appreciate the Government of Australia's willingness to consult with industry throughout the process. The Chamber believes that considering industry voices strengthens the 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 digital infrastructure's security.

The Chamber recognizes that managing cyber risk in all critical infrastructure sectors is vital to the U.S. and Australia's economic and national security. The Chamber and our members also recognize the national security importance of managing supply chain risk for critical technologies and ensuring that these technologies are resilient and secure from a nation-state and other malicious actors who attempt to sabotage or disrupt their availability and integrity is a vital priority. However, we would like to re-emphasize several fundamental principles that encourage Australia to promote cyberspace, critical technology, and infrastructure.

- **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 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. They 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. Such an approach will foster innovation since the framework will be able to adapt to new technologies.

- **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. The Chamber supports Australia's desire to build on and not duplicate existing frameworks and best practices and urges Australia to continue to purse alignment with any regulations and standards it issues with industry-backed approaches to risk management. Private industry greatly benefits when governments leverage existing cybersecurity framework best practices as a starting point, such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework or the International Organization for Standardization/International Electrotechnical Commission ("ISO/IEC") 27103:2018 (or ISO/IEC 27101, a forthcoming standard that will incorporate ISO/IEC 27103:2018), for any future policy enactments.

    - Given that the NIST Cybersecurity Framework, ISO/IEC 27103, and ISO/IEC 27101 apply to organizations across critical sectors, such best practices are essential for interoperability across regions and interdependent sectors. For technology providers, ISO/IEC 27001:2013 also provides foundational guidance and assurance artifacts that can strengthen security and efficiency.

    - Approaches to cybersecurity must adhere to industry-vetted actions that businesses can take to assess and enhance their security state over time. Allowing CII operators to combat evolving cyber threats with evolving best practices and standards permits a more flexible, current, and risk-based cybersecurity approach. 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.

- **Security measures alignment to sector-specific best practices**. The Chamber urges the Australian Government to leverage existing industry-led risk management frameworks that build interoperable cross-sector baselines for sector-specific applications. For example, the

Financial Services Sector-Specific Cybersecurity Profile is a scalable and extensible assessment that financial institutions of all types can use for internal and external (i.e., third party) cyber risk management assessment and as a mechanism to evidence compliance with various regulatory frameworks (a "common college application for regulatory compliance") both within the United States and globally. The Financial Services Sector-Specific Cybersecurity Profile is also consistent and aligned with the NIST Cybersecurity Framework and ISO/IEC 27103:2018. Other sector-specific profiles can similarly be developed in a way that leverages international best practices but address sector-specific risk scenarios and governance needs, as highlighted in *Seamless Security: Elevating Global Cyber Risk Management Through Interoperable Frameworks*.

- **Compliance and enforcement**. The Chamber is sympathetic to the Government's proposal for Board-approved (or equivalent level) attestation of a regulated entity's cybersecurity compliance. However, we strongly oppose policies that create a point in time perspective on an organization's cybersecurity. This proposal should be carefully considered and narrowly tailored to cover the disclosure of financially material cyber risks and cyber events. In the U.S., the Chamber has opposed changes to The Sarbanes–Oxley Act of 2002 that would require cybersecurity attestation. Such a proposal would likely generate tens of billions in implementation costs. Unlike financial accounting standards, which are relatively static, cybersecurity standards are inherently dynamic. Organizations should not be biased away from or improving cyber controls based on threats and cyber risk because of the expense of documenting changes and forced reporting. As with any form of enterprise risk, cyber risk is a shared responsibility that requires a whole-of-organization approach. In this regard, and as a general best practice, an organization's board should receive regular cybersecurity briefings and provide oversight and direction to company executives in dealing with cyber risk as an enterprise risk.

- **Build multi-stakeholder engagement forums for the joint industry and government collaboration.** The Chamber applauds Home Affairs' strong commitment to the multi-stakeholder process for policy formulation. We further recognize that governments are increasingly focusing on the security of supply chains. Within our government, we are tracking up to 30 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 its membership's collaborative efforts. 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.

- **Emphasize capacity building and information sharing.** Everybody is vulnerable, and cyber threats must be met with global information sharing and collaboration to improve and safeguard critical infrastructure and systems of national significance. The Chamber

encourages capacity-building and information sharing between the public and private sectors. We believe that information sharing makes companies and Governments alike stronger while weakening adversaries and bad cyber actors. We encourage active sharing of threat intelligence and known vulnerabilities between relevant stakeholders as a critical aspect of protecting critical infrastructure and strengthening the ecosystem's defense against bad actors. While governments (e.g., computer emergency response teams, national cybersecurity centers) and 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. In contrast, threat data on vendor- or product-based risk (e.g., the insertion of malicious code 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 competent national authorities share targeted intelligence and involve relevant suppliers in assessing risks to specific products? (4) What legal or policy barriers to bi-directional information sharing exist, including substantial countervailing risks of IP loss and inadvertent dissemination of security vulnerabilities? The Chamber firmly supports the notion that a real-time threat picture, including intelligence insights and trends, will empower owners and operators of systems of national significance to take appropriate and timely action on their systems.

- **Provision information about networks and systems to contribute to the government's threat picture**. The Chamber respectfully opposes global and domestic government mandates for mandatory cyber incident reporting. Such requirements violate sound cyber risk management principles and unravel the consensus that information sharing between industry and the Government must be based on collaborative partnerships to work effectively. These arrangements are flawed for several reasons, including:

    - First, mandatory reporting insufficiently considers the increased costs and misallocated businesses' resources (e.g., human and technical) due to forced reporting.

    - Second, the Chamber rejects policies that require reporting on a fixed timeframe. Among other considerations, what may be understood in the first few days of a cyber incident investigation can be dramatically different from what is learned in the weeks and months that follow.

    - Third, several critical infrastructure sectors (e.g., financial services and energy) have existing legal obligations to report significant cyber incidents to government regulatory bodies. It is challenging to discern what increased value would flow to the federal government when such information is seemingly available to federal agencies.

- **Cybersecurity activities**. The Chamber appreciates the Government's sensitivity to critical infrastructures proactive steps to cyber risk management. The Chamber maintains that any

government-directed cybersecurity activities must provide industry with safeguards (e.g., regulatory and legal liability protections and programmatic reciprocity), as well as facilitate the bilateral exchange of cyber threat data between Government and industry.

- *Independent third-party assessments*. The Chamber appreciates the Governments view that independent assessments by third-party provider may serve a role in cyber risk management. However, in the Chamber's experience policymakers have used third-party assessment requirements for different purposes (e.g., regulatory, compliance) versus actual risk mitigation. As we have previously discussed, cybersecurity activities should be mindful of the impact on regulated industries. To minimize this risk, we urge the Government to keep these principles in mind when considering third-party assessment requirements.
  - Take a risk-based approach, clearly define the purpose, and avoid one size fits all frameworks.
  - Promote alignment to international, industry-driven, voluntary consensus standards and best practices.
  - Consider alternatives, appropriate to the risk profile, to third-party assessment like self-assessment.
  - Avoid localized testing and promote mutual recognition programs.

- **Establish the capability to disrupt and respond to threats**. The Chamber is concerned with the Australian government's proposed authority to direct incident response actions on systems of national significance. We are sympathetic to Home Affair's desire for this added power to mitigate a cyberattacks effects, but several questions remain unanswered.

  - First, there is a lack of clarity regarding the breadth of the Government's access to networks and systems, the role of third-party audits, the impact of global privacy regimes, and regulatory and legal liability concerns. Access does not relieve critical infrastructure of their obligations to comply with international privacy laws, such as the EU General Data Protection Regulation (GDPR). The loss of GDPR certifications would entail considerable costs to critical infrastructure owners and operators. Requirements for an independent review and authorization of any access requests could ensure a balance of interests are considered.

  - Second, the Chamber is concerned that Government directed activities, especially those directed during a cyber state of distress, may lead to unintended consequences. For example, critical infrastructures systems of national significance are complex, globally distributed, and may have dependencies or provide essential functions that could have negative consequences if disrupted by government direction. Dependencies in a financial services entities network might not have the same functionality in an energy or communication entities system. At a minimum, the Government should consider providing liability protections for federally directed response activity. It should also consider establishing a significant threshold for any actions, in terms of both extent of disruption and interruption of private sector directed response and clarifying that activities will only be defensive.

    - Third, the Chamber supports the the need of harmonization given the globally-intertwined nature of technology and vulnerability disclosure practices. The Government of Australia should align to accepted international standards (e.g., ISO 30111, ISO 29147) given the globally-intertwined nature of technology and vulnerability disclosure practices.

- **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. It is critical to ensure that critical information infrastructure definitions and designations are clear, appropriately limited, and consistent. We urge governments to apply a rigorous, proportionate, and risk-based analysis to determine what should be designated as critical infrastructure. 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 identifying critical infrastructure is a common international best practice for global capacity building, identifying critical economic functions and detailed 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 identifying 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 the Department of Home Affairs 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 ([redacted]) or Senior Director for Global Regulatory Cooperation, Abel Torres ([redacted]).