CHAMBER OF COMMERCE
OF THE
UNITED STATES OF AMERICA

VINCENT M. VOCI
VICE PRESIDENT FOR CYBER POLICY
CYBER, INTELLIGENCE, AND SUPPLY CHAIN
SECURITY DIVISION

ABEL TORRES
SENIOR DIRECTOR
CENTER FOR GLOBAL REGULATORY COOPERATION

August 27, 2021

Submitted Electronically via the Department of Home Affairs.

Ms. Louise Bechtel
Assistant Secretary
Cyber Policy and Strategy Branch
Cyber, Digital and Technology Policy Division
Department of Home Affairs

Dear Ms. Bechtel:

The U.S. Chamber of Commerce (Chamber) appreciates the opportunity to respond to the Department of Home Affairs call for views on *Strengthening Cyber Security Regulations and Incentives*. The Chamber welcomes the Australian government's consultation with critical industries to enhance their operational and cyber resilience.

The U.S. Chamber of Commerce is the largest business advocacy organization in the world, operating in all 50 states and in over 50 countries to promote free enterprise and advance American trade and investment globally, representing companies of every size and from every sector, working with state and local Chambers and over 100 AmChams around the world. 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.

The Chamber appreciates the opportunity to have previously commented on the Security of Critical Infrastructure Act 2018 (SOCI Act) and the Department of Home Affairs' Protecting Critical Infrastructure and Systems of National Significance consultation paper. The Chamber shares Australian policymaker's goal of enhancing the resilience of the digital economy from cyber threats. The Chamber also recognizes that managing cyber risk is vital to the U.S. and Australian economic and national security.

As the Australian government continues to build on its national cyber strategy and contemplates regulatory approaches to incentivize businesses to invest in cybersecurity issues, we encourage policymakers not to enhance powers of government to intervene by implementing mandatory requirements but instead to consult with industry throughout the process and implement a voluntary, risk management-based framework. Public-private partnerships support efforts to ensure effective, transparent, accountable, and consultative processes. Our goal is to foster a more resilient ecosystem by creating industry-led, market-based cybersecurity solutions.

We strongly believe that a multistakeholder approach to cybersecurity is the most effective way to encourage economic activity while ensuring a secure digital infrastructure.

The Chamber would like to underscore several notable positions in response to the possible new policies outlined in the discussion paper:

Advance Risk-Based Approaches to Cybersecurity

Cybersecurity threats rapidly evolve and are increasing in scale, frequency, complexity, and consequence. The Chamber believes that a risk-based approach, coupled with incentives, is more effective in managing cyber risk than prescriptive regulation. We urge governments to employ and encourage enterprises within their territories to use risk-based approaches. These approaches should rely on international, consensus-based standards and risk management best practices to identify and protect against cybersecurity risks and detect, respond to, and recover from cybersecurity incidents. Cybersecurity regulations shall, to the maximum extent possible, align with risk-based approaches best exemplified by the U.S. National Institute of Standards and Technology's (NIST) Cybersecurity Framework or sector-specific profiles such as the Financial Services Sector Cybersecurity Profile.

Implement Voluntary Labeling Schemes

Australian cybersecurity policies, procedures, and regulations should promote international alignment and interoperability with industry-backed approaches to risk management to the maximum extent possible. The Chamber encourages the Australian government to leverage public-private partnerships to develop public policy by incorporating consensus-based standards, available accreditation schemes, and globally recognized practices to meet Australian compliance interests. Government agencies can promote transparency, leverage private sector resources, and contribute to economic and job growth by working with the private sector.

As the Australian government contemplates the development of a labeling and rating scheme and corresponding evaluation requirements (e.g., testing, certifications, audits, etc.), the Chamber recommends establishing a voluntary public-private framework and strongly urges the Australian government to:

1. Build on and not duplicate existing standards, frameworks, and best practices.
2. Promote the voluntary use of cybersecurity labeling schemes.
3. Consider alternatives appropriate to the risk profile, to third-party assessments like self-assessment, vendor attestations, or accreditation of third-party assessors as a means to build and maintain confidence in conformity assessment bodies.

The Chamber encourages the Australian authorities to pursue a voluntary approach and mechanism when developing national cybersecurity policies and strategies. We encourage the Department of Home Affairs to host workshops with the private sector on the challenges and practical approaches to initiating cybersecurity labeling efforts for smart devices. For example, Section 4(t) of President Biden's *Executive Order on Improving the Nation's Cybersecurity*

directs NIST to identify IoT cybersecurity criteria for a consumer labeling program. We recommend that any requirements and enforcements for the cybersecurity labeling of devices revert to a mechanism that allows a manufacturer to undertake a self-assessment of their products and declare how the device conforms to the requirements with oversight from competent authorities. This would help ensure that products and services are secure by design without unnecessarily complicating the procedure.

Leverage Industry Led and Consensus-Based Standards

A smart device should be clearly defined and not be interpreted too broadly, layering unnecessary costs and regulatory burdens onto those devices that are not associated with sufficient risk to require labeling. The standards against which labeling programs are measured should emanate from international standards-setting bodies, according to the World Trade Organizations Technical Barriers to Trade *Principles for the Development of International Standards, Guides, and Recommendation*s.

The initiative should clearly define what constitutes a smart device and leverage existing approaches for determining the risk of such devices. The Chamber urges the government to convene a multistakeholder effort to discuss the limitations on the *Code of Practice*, which represented a first step in the government's approach to improving the security of IoT devices in Australia. The Chamber supported developing the IoT Device Cybersecurity Capability Core Baseline (the baseline), a joint industry and NIST collaboration that aligns with the risk-based measured approach the Chamber advocates. The baseline was an outgrowth of the Council to Securing the Digital Economy C2 Consensus on IoT security core capabilities baseline. The cybersecurity Specialist Committee of ISO/IEC JTC1, SC27, used C2 as one of the inputs to building an international technical standard, currently 1st Working Draft 27402

A flexible, nonregulatory framework could be widely used around the world by both industry and government stakeholders. It is critical to urge private entities to build and deploy smart devices with security features and practices aligned with international standards (e.g., ISO/IEC 27001, ISO/IEC 27103) and frameworks (*e.g.*, NIST Cybersecurity Framework). The Chamber urges secure by design practices for the business community, consumers, and the long-term viability of device makers. The Chamber wants leading sectors and companies to drive the solutions to help prevent and reduce cyber risk. The Chamber seeks to help public and private stakeholders build bridges between organizations that employ relatively sophisticated cyber practices and those that seek to develop a program and improve it over time.

Harmonization of Vulnerability Disclosure Practices

The Chamber encourages 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 the governments to work with the private sector to build on and not duplicate existing best practices and urge the Australian government to facilitate industry-wide implementation of transparent policies for coordinated vulnerability discloser. Governments, industry, and consumers benefit when existing standards, frameworks, and bests practices are leveraged as a starting point (e.g., International Organization

/International Electrotechnical Commission ("ISO/IEC") DIS 30111 and ISO/IEC 29147, work of Global Forum on Cybersecurity Expertise, ICASI, and the U.S. Department of Homeland Security's CVD program) and incorporated into any future vulnerability disclosure policy enactments and practices.

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 provide more information, please contact Vince Voci (vvoci@uschamber.com), vice president for cyber policy or Abel Torres (atorres@uchamber.com), senior director for the Center for Global Regulatory Cooperation.

Sincerely,

Abel Torres
Senior Director
Center for Global Regulatory Cooperation
U.S. Chamber of Commerce

Vincent Voci
Vice President, Cyber Policy
Cyber, Intelligence, and Supply Chain Security Division
U.S. Chamber of Commerce

Enclosure: Recommended Principles for Trustworthy ICT Suppliers

Recommended Principles for Trustworthy ICT Suppliers

1. Technical risks associated with the Suppliers' products or services are reasonably understood and properly managed:
    a. Technology is designed, developed, and deployed according to a transparent, testable, open, consensus standards-based, and process-oriented framework for identifying, assessing, and managing risk through the anticipated lifecycle of the product or service, including:
        i. Protection of development and build environments against compromises to production systems;
        ii. Adoption of a "controls framework" aligned to industry standards (e.g., ISO 27001), including implementation of granular, role-based access controls;
        iii. Scanning of code for known vulnerabilities;
        iv. Modeling of anticipated threats and risks; and
        v. Maintaining the security of software and firmware and updating mechanisms and pathways.
    b. Provenance, pedigree, and integrity of code, including open-source code, can be reasonably demonstrated to ensure securability of resulting products and compliance with intellectual property rights;
    c. Technology is capable of standards-based conformance testing of controls implemented to manage risk—and also of ensuring repeatability of build processes such that tested code can be validated against code in a finished offering deployed and used in an operating environment;
    d. Vulnerability handling, remediation, and disclosure policies consistent with international standards are adopted, transparently communicated, regularly used, and capable of assessment to ensure compliance;
    e. Information security and privacy practices for the protection of personal data and respecting individual rights are adopted, transparently communicated, and assessed to ensure compliance; and
    f. Controls, mitigations, policies, and procedures adopted by the Supplier should be communicated and flowed through to:
        i. Suppliers of components and source code included in its products;
        ii. Processors/sub-processors of confidential, proprietary, and personal data; and
        iii. Distributors, partners, and resellers who receive, install, integrate, sell, or maintain the market's suppliers' technology.

2. Suppliers demonstrate adherence to generally recognized norms of corporate behavior, including:
    a. Public "codes of business conduct" outlining the Suppliers' core values, principles, and practices;
    b. Public trading of equity, or equivalent mechanisms, to ensure decision-making per commercial considerations concerning procurement, investment, and contracting through transparency of ownership, partnerships, governance structures, and funding sources;

c. Public demonstration of compliance with auditing and accounting standards generally adopted in the marketplace (e.g., Generally Accepted Accounting Principles or International Financial Reporting Standards) designed to ensure the absence of hidden, opaque, or otherwise non-commercial sources of funding, financing, or subsidy;
d. Internal governance mechanisms clearly articulated, enforced, and subject to external review demonstrating a commitment to protect:
    i. Security and privacy of users and customers against cyber-enabled attacks or other unwarranted government intrusions;
    ii. Privacy and individual rights with transparency, fairness, and accountability;
    iii. The integrity of products, services, and data against tampering;
    iv. Intellectual property against theft or misappropriation;
    v. Fair and open competition;
    vi. Environmental resources against damaging or unsustainable practices;
    vii. Human rights against forced or unfair labor practices; and
    viii. Public health and well-being.
e. APPA (Authorized Public Purpose Access): Enable data distribution (especially in the healthcare sector) where negative effects of inappropriate data use have been mitigated through an appropriate governance model for specific data components to be available in support of a public purpose objective.

3. Suppliers operate subject to both international commercial norms and national laws but make decisions based on commercial considerations rather than undue direct government control or influence over internal governance and operations as demonstrated by:
    a. Absence of arbitrary access to company data, facilities, resources, or operations and mandates to cooperate with government directives – as demonstrated by transparency and reasonable access to due process mechanisms allowing for the challenge of such demands to be heard by an independent judiciary or another neutral arbiter.
    b. Absence of requirements to include governmental or party officials in corporate structures or decision-making processes – as demonstrated by transparency and public disclosure of organizational/governance structure, ownership interests; and

4. Suppliers are headquartered, formed, and operate under the laws of a nation that:
    a. Govern subject to the rule of law with adequate separation of powers protected by an independent judiciary or another neutral arbiter of due process and protected rights; and
    b. Uphold internationally agreed norms, standards, and treaties essential to global human development—including being good stewards of environmental resources, implementing fair labor practices, protecting intellectual property, protecting public health and well-being, and respecting privacy and human rights—in the procurement and acquisition of ICT.