U.S. Chamber of Commerce

1615 H Street, NW
Washington, DC 20062-2000
uschamber.com

October 31, 2023

Ms. Kemba Eneas Walden
National Cyber Director (Acting)
Office of the National Cyber Director
Executive Office of the President
1600 Pennsylvania Avenue, NW
Washington, DC 20500

Re: Request for Information, Office of the National Cyber Director, Executive Office of the President; Cyber Regulatory Harmonization: Opportunities for and Obstacles To Harmonizing Cybersecurity Regulations (88 Fed. Reg. 55,694-55,697, August 16, 2023)

Dear Acting Director Walden:

The U.S. Chamber of Commerce welcomes the opportunity to comment on the Office of the National Cyber Director's (ONCD) request for information (RFI) on cyber regulatory harmonization and appreciates ONCD's extension of time to provide formal comments. Harmonizing the myriad federal cyber regulations is a complex, challenging, and often thankless task. We appreciate your commitment to this endeavor, and your willingness to solicit input from private sector entities like the Chamber and its broad membership base. We believe that improved harmonization of cyber regulations will allow organizations to focus more of their time, people, and resources on improving cyber programs and responding to incidents, rather than addressing overlapping, duplicative—and sometimes contradictory—state, federal, and international regulatory requirements.

I. Introduction

Evolving cybersecurity threats are persistent and pervasive challenges to businesses and critical infrastructure across the globe. Governments and regulatory bodies have introduced new cybersecurity regulations to address the growing threat landscape. The U.S. Government (USG) took several significant actions to create or update cybersecurity requirements following the SolarWinds vulnerability exploit and Darkside and REvil ransomware campaigns. These actions included issuing Executive Order 14028, Improving the Nation's Cybersecurity, and promulgating numerous Security Directives related to pipeline, rail, and aviation security issued by the

Department of Homeland Security's Transportation Security Administration, the passage of the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (and forthcoming implementation regulations), the U.S. Securities and Exchange Commission's new final rule on cyber risk management, governance, and incident disclosure, and Second Amendment to DFS's Cybersecurity Regulation, 23 NYCRR Part 500. However, there still exists a fragmented regulatory environment that needs more cohesion and consistency.

II. The Fragmented Regulatory Landscape

These new requirements often result in organizations diverting resources from cyber risk management to programs that prove compliance with new security measures. Unfortunately, the current state of cybersecurity regulations is a fragmented landscape with varying standards, requirements, and compliance frameworks across jurisdictions. While regulators often use consensus standards as a baseline, modifications, variances, or amendments specific to a jurisdiction metastasize into unharmonized requirements across sectors.

This fragmentation poses several challenges:

a) **Compliance Burden**: Businesses operating in multiple jurisdictions must navigate complex regulations, leading to increased compliance costs and administrative burdens.
b) **Inefficiency**: Fragmentation can result in redundant or conflicting requirements, leading to inefficiencies in cybersecurity efforts.
c) **Inadequate Coverage**: Gaps in coverage can occur when regulations fail to address emerging threats or evolving technologies.

The U.S. Chamber of Commerce's International Cyber Law Project, supported by extensive desk research from Wiley LLP and the National Security Institute at George Mason University, is an online reference tool that maps the cybersecurity and cybersecurity-related policy landscape. This tool tracks cyber policy across ten high-level criteria, including definitions for covered entities, security measures requirements, threat information sharing, localization requirements, government access, and sanctioning or penalty schemes. Since creating the tool in 2019, the U.S. Chamber has observed several jurisdictions updating their core cybersecurity legal structures, which has resulted in several new laws and regulations for global businesses to attest compliance with.

Over that same period, the Biden Administration took several significant actions to update federal cybersecurity requirements for critical infrastructure, software providers, and government contractors. While some of the actions were tied

to federal contracting authorities, others seemed more reactive and had the ability to cause confusion or conflict between state and federal regulatory frameworks. For example, a letter to state governors in March 2022, encouraged state and local utility commissions to leverage their authorities to "set and enforce cybersecurity baseline standards for utilities." While undoubtedly sent with noble intent, this requested action could have resulted in the establishment of individual state or local cybersecurity requirements wholly out of balance with those in other states and localities. Likewise, in December 2022, New York Governor Kathy Hochul signed Legislation A.3904B/S.5579A, a new law to strengthen the cybersecurity of the energy grid from threats. While well-intentioned, such laws are a prime example of the deep concern the Chamber has with state-by-state approaches to addressing federally regulated critical infrastructure and interstate national critical functions.

Competing laws, regulations, and frameworks at the state and international level threaten to fragment the digital economy, confuse cybersecurity compliance efforts, and imperil the ability of American companies to compete globally. To address an increasingly fragmented compliance dynamic, the U.S. Chamber believes that the Administration and Congress should work with industry to pass legislation that carefully balances regulatory compliance with consensus standards and incentives to increase U.S. security and resilience commensurate with the present threat levels. Such legislation should establish a common high-level standard for cybersecurity in the U.S. and provide a legal framework (1) to establish security measures routed in technical, international, consensus standards; (2) to protect covered entities from frivolous lawsuits and provide an affirmative defense; (3) to preempt substantially similar state-level cybersecurity rules; and (4) to create a White House office to drive state, federal, and international harmonization.

A national cyber law would ensure a coordinated and cohesive federal approach to national cybersecurity. It could help streamline efforts and resources across different government agencies, creating a more effective response to cyber threats and incidents, and it would head off an increasingly fragmented state-by-state approach we have seen develop first on data breach notifications, state privacy laws, and now cybersecurity rules for businesses. A national law would provide confidence to state and global governments that federal agencies are authorized to mandate security minimum for covered entities and are authorized to negotiate mutual recognition agreements leveraging technical, international, and consensus standards.

III. Outcome Focused, Risk-Based, Consensus Standards Are Critical for Driving Regulatory Cohesion

Cybersecurity requirements, assurance, and certification approaches based on outcome focused, risk-based, consensus standards reflect global best practices

developed with industry, regulators, academia, civil society, and government. Internationally recognized standards development organizations (SDOs) promulgate consensus standards based on technical merit and not based on nationality, employer, or person originating them. They enable safe, secure, reliable, and interoperable global technology, products, and processes. Regulator use of outcome focused, risk-based, technical consensus standards will simplify compliance, enhance cyber resilience, scale globally, and adapt to emerging threats and new technologies.

The U.S. Chamber is pursuing a regulatory framework that enables compliance activities that can be performed once and recognized multiple times by different regulators in different jurisdictions with customization. Such a cohesive regulatory regime would reduce the resources an organization must expend or divert to cybersecurity compliance, allowing it to invest those resources in cyber risk management programs.

IV. Case Studies in Harmonization

Several initiatives and case studies highlight the benefits of harmonized cybersecurity frameworks:

a) NIST Cyber Framework: The National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) in the U.S. is a reference point for organizations seeking to harmonize their cybersecurity practices domestically and internationally. There is broad consensus that the CSF is a sound baseline for cybersecurity practices and risk management. The CSF has been translated into multiple languages, and the U.S. Chamber actively promotes its use internationally to comply with foreign cybersecurity rules.
b) Financial Services Sector Cybersecurity Profile (the Profile): The Profile is a shared baseline developed by the Financial Services Sector Coordinating Council and representatives from key agencies and is the financial services sector's global standard for cyber risk assessments. Based on NIST's Cybersecurity Framework, the Profile creates efficiencies and flexibility for cybersecurity risk management and provides adequate assurance to government supervisors.
c) ISA-62443 is a series of international standards and technical reports developed by the International Society of Automation (ISA) for industrial automation and control systems (IACS) cybersecurity. These standards provide guidelines and best practices for enhancing the security of industrial processes and systems. Organizations that operate critical infrastructure or rely on industrial control systems use ISA/IEC-62443 for cybersecurity regulatory compliance to demonstrate their commitment to cybersecurity best practices and compliance with relevant regulations.

Automation suppliers can have their systems and devices certified to the ISA/IEC-62443 standard by 3rd-party accredited certifiers, enabling organizations to choose systems based on cybersecurity robustness and features.

d) ISO/SAE 21434 is an international standard providing a minimum baseline for cybersecurity engineering of all road vehicles and their components. Such a standard is increasingly important as vehicles become more connected and offer greater functionality, particularly automation, to their drivers. Compromised vehicles not only result in financial and privacy losses but can also present a major safety hazard to drivers, passengers, and pedestrians in that there is potential for attackers to weaponize security-breached vehicles.

e) ISO 24089 is an international standard providing a minimum baseline for software update engineering for road vehicles. This standard is related to ISO/SAE 21434 in that regular patching is an important aspect of maintaining cybersecurity after a vehicle rolls off the production line. As vehicles become more and more reliant on software (a new era of vehicles we are now entering known as the "software defined vehicle"), updated software is critical to ensure the ongoing safe operation of such vehicles.

V. International Cooperation is Critical to Creating a Cohesive Global Cyber Regulatory Framework

The U.S. Chamber and its members monitor, analyze, and comply with more than 100 worldwide cybersecurity-related laws, frameworks, standards, and regulations. Building off the U.S. government's foreign policy and international engagement with non-U.S. cyber agencies, standards development organizations, and government bodies, we urge the U.S. government to take the lead on harmonizing regulations.

We offer the following recommendations:

a) **Digital Trade Agreements (DTAs).** Digital trade agreements can play a crucial role in including cybersecurity regulations and harmonization by setting the framework for how countries handle cybersecurity-related issues in international trade. Future DTAs may include one or more of the following cybersecurity priorities:

   i. Define the agreement's cybersecurity objectives and goals reflecting commitments to preserving an open, interoperable, reliable, and secure internet that fosters efficiency, innovation, communication,

and economic prosperity while respecting privacy and guarding against business disruption, fraud, and theft.

ii. Establish cybersecurity principles. Title 19 of the United States-Mexico-Canada Agreement (USMCA) includes quality cyber risk management language, confirming that, “the Parties recognize that risk-based approaches may be more effective than prescriptive regulation in addressing those threats. Accordingly, each Party shall endeavor to employ and encourage enterprises within its jurisdiction to use risk-based approaches that rely on consensus-based standards and risk management best practices to identify and protect against cybersecurity risks and to detect, respond to, and recover from cybersecurity events.”

iii. Consensus global standards. Developed by industry, government, and technical experts across sectors and regions through standards development organizations, these technical standards reflect international best practices. They are subject to validation and testing before use.

iv. Regulatory mutual recognition or reciprocity. Aligning and using consensus standards will simplify establishing a framework for international mutual recognition or reciprocity where one regulator will accept another regulator's finding that a regulated entity conforms with or certifies to using a certain consensus standard(s).

v. Threat information sharing and structured data exchange. DTAs should promote the international exchange of structured and unstructured information between Computer Emergency Response Teams, competent cyber agencies, law enforcement, and other public sector bodies for cybersecurity purposes and defensive measures. Legal frameworks should ensure that threat data and vulnerability information are authorized for sharing and covered by appropriate privacy, disclosure, and regulator rules.

vi. Cross-Border Data Flows: Preserve and authorize cross-border data flows, including the free flow across borders, while considering national security and privacy concerns.

vii. Dispute Resolution Mechanisms: Establish mechanisms for resolving cybersecurity disputes, which may involve creating a dedicated cybersecurity dispute resolution body or using existing trade dispute resolution mechanisms.

viii. Public and Private Sector Collaboration: Promote collaboration between public and private sectors to strengthen cybersecurity. Engage technology companies, critical infrastructure entities, multinational businesses, small businesses, industry associations,

and civil society organizations in discussions and initiatives related to cybersecurity in digital trade.

ix. Periodic Review and Updates: Recognize the digital landscape and cybersecurity threats continually evolve. Build mechanisms for periodic reviews and updates of the digital trade agreement to adapt to new challenges and opportunities in the cybersecurity space.

b) **Oppose Digital Sovereignty Requirements.** The U.S. government must continue to lead the charge in ensuring that governments worldwide keep cybersecurity requirements rooted in technical consensus standards. Increasingly, markets are promulgating rules, regulations, standards, frameworks, and certifications that protect local companies and discriminate against foreign suppliers. Examples of negative requirements that are imposed under cybersecurity, national security, or protection against unlawful access justifications, include:

i. Headquarters and ownership. A foreign company must establish its head office or global headquarters in a market.
ii. Data localization. A requirement that forces data to reside and process in a market, resulting in higher cyber risk and reduced resilience.
iii. Domestic workforce for data processing. A requirement on foreign suppliers to leverage only domestic employees for data access and processes for global operations.
iv. Required choice of law provisions. A requirement on foreign supplier's states that a company must affirm that it shall only be governed solely by the law of the market in which it operates.

Digital sovereignty requirements that restrict cross-border data flows have unintended consequences on national security and organizational resilience. They fail to distinguish between foreign companies that are subject to control by a foreign government, without independent judicial review, from foreign companies who adhere to democratic rules that respect privacy. Excluding foreign suppliers from markets narrows customers' choices and aggregates supply chain risks into a select group of vendors. We encourage the U.S. government and governments worldwide to embrace technical consensus standards and other technical measures to build confidence in foreign companies' cybersecurity and trustworthiness.

c) **Support Regulator-to-Regulator Memoranda of Understanding or Bilateral Cybersecurity Mutual Recognition or Reciprocity Agreements**

These agreements should leverage consensus standards and may offer several significant benefits:

i. Facilitate Cross-Border Trade: Agreements should streamline the process for companies operating internationally to comply with cybersecurity regulation, reduce the need for redundant compliance efforts, and allow for more efficient cross-border data flows and trade.
ii. Market Access: Companies can gain more access to international markets by complying with recognized international standards, boosting their credibility and competitiveness.
iii. Stable and Predictable Regulatory Environment: Businesses, especially those considering new market entry, succeed in jurisdictions with stable, predictable, and transparent regulatory requirements. A mutual recognition or reciprocity agreement provides greater regulatory certainty for businesses, as they clearly understand the cybersecurity requirements they need to meet when operating in multiple jurisdictions.
iv. Cost Reduction: Businesses can reduce compliance costs by adhering to a consensus standard recognized across multiple jurisdictions or between regulatory agencies, eliminating the need to adapt to different, potentially conflicting regulations in various markets.
v. Efficient Compliance: Companies can adopt a proactive approach to cybersecurity compliance by certifying the use of consensus standards to regulatory agencies. Simplifying the compliance process through mutual recognition or reciprocity agreements can make it easier for businesses, particularly small and midsized enterprises, to demonstrate cybersecurity compliance.
vi. Enhanced Cybersecurity: Mutual recognition or reciprocity agreements often involve adherence to high-quality, widely accepted consensus standards, leading to improved cybersecurity practices and better protection against cyber threats.
vii. Global Interoperability: Alignment with consensus standards encourages the development and use of technologies and systems that are globally interoperable, benefiting both businesses and consumers by ensuring that products and services can seamlessly function across borders.
viii. International Cooperation: These agreements can foster international cooperation on cybersecurity issues by bringing countries together to agree on common standards and principles, leading to better

information sharing, collaborative threat response, and joint efforts to combat cyber threats.

ix. Consumer Trust: Recognized cybersecurity consensus standards can build consumer trust by assuring them that foreign companies' products and services meet a certain level of cybersecurity protection.

A more harmonized and aligned global approach to cybersecurity requirements for multinational companies has numerous benefits, including increased security and resilience in the digital economy. While there are many advantages to such agreements, it is important to note that achieving consensus among participating countries and aligning their regulatory frameworks can be a complex and time-consuming process. Additionally, ongoing monitoring and enforcement of compliance with standards are essential to ensure that the benefits of such agreements are realized.

VI. Significant Challenges Have Created Barriers to Regulatory Harmonization

While the need for harmonization is clear, achieving it poses challenges:

a) Sovereignty Concerns: Some jurisdictions may resist harmonization due to concerns about sovereignty and control over their cybersecurity regulations. State, county, or region-specific cybersecurity standards increase resource requirements for security compliance and decrease the available resources for cyber risk management. In foreign markets, the U.S. Chamber has observed jurisdictions use non-technical measures like ownership, immunity from non-domestic law, and localization requirements for cybersecurity purposes. Sovereignty requirements are discriminatory and result in technical barriers to trade and the closure of markets to foreign suppliers.

b) Workforce and Differing Priorities: Over the past several years, regulations and global government activities have increased exponentially. In August alone, various U.S. agencies promulgated four different RFI's or proposed regulations. While the U.S. Chamber and its members appreciate that agencies may have specific missions and unique policy objectives, addressing each agency with quality, actionable, and impactful feedback is extraordinarily challenging. We are committed to public-private collaboration, but we need to figure out a new approach to focus on outcomes and not just processes.

c) Agency (or Regulator) Personalization of Cybersecurity Requirements: The U.S. Chamber advocates for governments globally to align cybersecurity requirements to the NIST CSF, international standards (e.g., ISO/IEC 27001, ISA/IEC 62443, IOS/SAE 21434), sector profiles, or NIST Special

Publications 800.53, 800-171. However, we have observed that U.S. regulators promulgate rules and cybersecurity requirements that go beyond these consensus standards, which suggests that they have identified that these global best practices need to meet their regulatory objectives. Seemingly well-intentioned regulators write new cybersecurity requirements based on one or more consensus standards without using their exact language, leading to regulatory fragmentation.

d) **Mitigating Emerging Risks:** As new technologies emerge, there will likely be cases where consensus standards do not adequately mitigate risks identified by regulators or practitioners. In these cases, we urge regulators to adopt an outcome-focused approach to security requirements, which are not biased to specific technologies or controls, but enable practitioners to implement traditional or innovative techniques to manage risk. International standards should then codify best practices to ensure consistency worldwide.
e) **Length of Time to Develop Consensus Standards.** Today, industry-driven consensus standards are set by international standards development organizations (SDOs). Because SDOs are consensus organizations, it can take significant time for new workstreams to be introduced and adopted by a global community as an industry best practice. This can sometimes frustrate regulators whose policy objectives must be aligned with SDO's work plans.
f) **Lack of a Common Taxonomy and Lexicon.** While NIST, through the CSF and special publications, has developed a common taxonomy for cybersecurity controls and a common lexicon for security, we often see regulators create different interpretations of substantially similar definitions.
g) **Implementation Complexity:** Harmonizing regulations across diverse jurisdictions requires careful planning, coordination, and international cooperation.

VII. The White House Should Establish a Regulatory Harmonization Office and Create Policies and Procedures for Regulatory Cohesion

The White House should establish a regulatory harmonization office to create a coherent regulatory system and harmonize cybersecurity requirements for regulated entities. The office's responsibilities should include:

a) Establishing expertise and competence of existing cybersecurity requirements from federal, state, independent, and international stakeholders;

b) Establishing policies and procedures for regulators to leverage consensus standards in writing new regulations in consultation with sector risk management agencies, the Cybersecurity and Infrastructure Security Agency, and the private sector;
c) Regularly convening independent and state regulators to share best practices on leveraging consensus standards and educate regulators on mutual recognition programs;
d) Leveraging technical assistance from the National Institute of Standards and Technology and Standards Development Organizations and provide that technical assistance to regulators during rulemaking processes; and
e) Pursuing opportunities for digital trade agreements to include cybersecurity chapters and international agreements to mutual recognition or reciprocity of cybersecurity requirements in consultation with the U.S. Department of State, the Office of the United States Trade Representative, and the U.S. Department of Commerce.

Similar to the U.S. Department of Homeland Security's Cyber Incident Reporting Council (CIRC), the office should undertake a comprehensive evaluation of federal, state, independent, and international cybersecurity requirements. The office should analyze cybersecurity requirements across sectors and publish a public report on how existing cybersecurity requirements align with, use, or diverge from consensus standards, identify existing authorities that regulators can use to harmonize or mutually recognize consensus standards-based conformance or certification, and make recommendations to Congress on changes to authorities that would further cyber regulatory harmonization.

In consultation with relevant offices and stakeholders, the office would promulgate White House policies and procedures to drive regulatory harmonization. Such Presidential Policy Direction may, at a minimum, require:

a) Federal civilian executive branch agencies issuing new or updating existing cybersecurity rules to use consensus standards. An issuing agency must include a cost-benefit analysis on the impact of compliance with the new regulations;
b) Agencies issuing cybersecurity rules to provide the Office of Information and Regulatory Affairs (OIRA) in the Office of Management and Budget (OMB) with a written justification in the rare circumstance when a consensus standard is not used and an explanation of how and why there is a divergence. It is vital to address this root cause for regulatory fragmentation and to create policy barriers to well-intentioned regulators writing new cybersecurity rules without using consensus standards or

picking and choosing a derivative of cybersecurity requirements from a standard;

c) The regulatory harmonization office must provide an assessment of each cybersecurity regulatory rulemaking describing a proposed rule's alignment or divergence from consensus standards and make recommendations on how to harmonize the regulation. The assessment should also consider the extent to which the proposed rule is substantially similar to existing rules for similar covered entities. It should also detail where an interagency memorandum of understanding should recognize other certifications based on consensus standards or develop policies that enable agencies to accept security assurance to be performed and accepted multiple times without customization
d) OIRA must consult with SRMAs, CISA, NIST, ONCD, and the office to resolve disputes and divergences with consensus standards before an agency publishes a proposed rule in the Federal Register; and
e) A significant challenge to U.S. regulatory harmonization efforts are independent regulatory agencies. The U.S. Chamber respects the independent status of these agencies, and their role in protecting consumers, consistent with the authorities and responsibilities Congress has delegated to each agency. However, efforts at creating a cohesive and comprehensive cybersecurity framework would fall short should independent agencies not be included in future planning. In consultation with industry and the Administration, the U.S. Chamber urges Congress to consider legislation to address this challenge. Narrowly scoped legislation authorizing the President's designee to convene independent regulatory agencies to exchange best practices on cybersecurity regulations would be a meaningful first step. Any U.S. regulatory agency should submit its proposed cybersecurity regulations for review to ensure consistency and alignment with consensus standards.

VIII. Conclusion

The evolving cyber threat landscape necessitates an active and coordinated approach to cybersecurity that carefully balances regulatory compliance with industry-recognized standards and positive incentives. Harmonizing cybersecurity regulations is not only a pragmatic response but also a critical step in safeguarding businesses and critical infrastructure from both emerging cyber threats and any undue expansion of the cost of regulatory compliance. By addressing the challenges and promoting international cooperation, stakeholders can work together to create a unified and robust cybersecurity regulatory framework that enhances resilience in the face of ever-evolving cyber threats.

Thank you for the opportunity to provide ONCD with comments on cyber regulatory harmonization. If you have any questions or need more information, please do not hesitate to contact me directly.

Sincerely,

Vincent M. Voci
Vice President, Cyber Policy and Operations
Cyber, Space, and National Security Policy
U.S. Chamber of Commerce