BR Business Roundtable

1000 Maine Avenue, SW, STE 500
Washington, DC 20024
202.872.1260
brt.org

October 12, 2023

Kemba E. Walden
Acting National Cyber Director
Office of the National Cyber Director
The White House
1600 Pennsylvania Avenue, NW
Washington, DC 20500

Comments of Business Roundtable on the Request for Information on Cybersecurity Regulatory Harmonization

Docket No. ONCD–2023–0001 // 88 Fed. Reg. 55694 (Aug. 16, 2023).

Dear Acting National Cyber Director Walden:

This letter is submitted on behalf of Business Roundtable, an association of more than 200 chief executive officers (CEOs) of America's leading companies representing every sector of the U.S. economy. Business Roundtable CEOs lead U.S.-based companies that support one in four American jobs and almost a quarter of U.S. GDP. We appreciate the opportunity to respond to the Office of the National Cyber Director's (ONCD) Request for Information (RFI) on Cybersecurity Regulatory Harmonization.

Introduction

Business Roundtable member companies across sectors—financial services, communications, energy, health, public safety and security, defense, manufacturing, technology, retail, hospitality, insurance, and others—face significant and growing cyber threats. As the RFI notes, companies across the economy have an interest in regulatory harmonization. This includes a significant number of businesses, such as online retailers, that do not qualify as critical infrastructure. Given the RFI's particular interest in critical infrastructure, we would note that BRT member companies own or operate infrastructure in at least eleven of the sixteen critical infrastructure sectors identified in Presidential Policy Directive 21: Chemicals; Commercial Facilities; Communications; Critical Manufacturing; Defense Industrial Base; Energy; Financial Services; Food and Agriculture; Healthcare and Public Health; Information Technology; and Transportation Systems. BRT member companies also provide technology solutions to owners and operators in the remaining critical infrastructure sectors.

BRT member companies operate comprehensive risk-based cybersecurity programs to address cybersecurity threats and regularly collaborate with the U.S. government to strengthen the cybersecurity of private and public systems. Our member companies, for example, have partnered with the federal government on the development, implementation and refinement of the NIST Cybersecurity Framework, voluntary sharing of cyber threat information under the Cybersecurity Information Sharing Act of 2015, and collaborative sector-specific partnerships developed in the defense industrial base, the energy industry, communications and IT, and other key sectors. Several of our member companies also served as founding partners in CISA's Joint Cyber Defense Collaborative, which has since expanded to cover most critical infrastructure systems.

These collaborative partnerships between the public and private sectors have greatly strengthened our collective cybersecurity posture. The NIST Cybersecurity Framework has become a market baseline for cyber risk management, for example. The voluntary information sharing regime likewise has enabled the successful development of information sharing and analysis centers (or "ISACs") that support virtually every industry. These collaborative, risk-based approaches have allowed companies to maintain cybersecurity programs that are tailored to the specific use cases and risks that they face. They are also sufficiently flexible to support continuous innovation in information technology, operational technology and cyber-physical and other systems, which drives tangible advances in cybersecurity capabilities and outcomes. We believe that such collaborative, flexible, technology neutral and risk-based approaches to cybersecurity policy are the best way to address the cyber threats ahead.

In contrast, duplicative, conflicting or unnecessary regulations require companies to devote more resources to fulfilling technical compliance requirements without improving cybersecurity outcomes or customer protection. They also incentivize companies to treat cybersecurity as a checklist-based compliance activity, rather than maintaining tailored cyber risk management programs. This is a real and present concern. Companies are subject to an ever-expanding web of cybersecurity regulations imposed at the state and federal level, as well as internationally.[1] As the National Cybersecurity Strategy acknowledges, it is important to address these concerns: "Where Federal regulations are in conflict, duplicative or overly burdensome, regulators must work together to minimize these harms."[2]

Business Roundtable consequently applauds ONCD for soliciting comments on cybersecurity regulatory harmonization. Below, we provide specific responses to ONCD's questions posed in the RFI.

---

[1] While out of scope for this RFI, we note that it is critical that the Administration also address duplicative and burdensome cyber incident reporting obligations.

[2] National Cybersecurity Strategy 9 (March 2023).

Responses to Questions Posed in ONCD's RFI

I. Reduction of Undue Regulatory Burden

[Q1] Identification of conflicting, mutually exclusive, or inconsistent regulations.[3]

American companies navigate a range of overlapping and unduly burdensome cybersecurity regulations. For example, financial institutions already face complex cybersecurity requirements imposed by multiple federal agencies as well as state regulators. A range of state-level regulations also apply to the protection of personal information: Massachusetts imposes security requirements for handling its residents' data,[4] as do California[5] and other states. Meanwhile, the Federal Trade Commission (FTC) has undertaken enforcement actions and issued guidance imposing a requirement to maintain reasonable security measures through its authority under Section 5 of the FTC Act, which permits the FTC to protect against unfair or deceptive acts or practices. These requirements unfortunately are neither clear nor consistent with each other, forcing companies to navigate an unnecessarily complex and burdensome web of regulatory requirements and expectations. For example:

- The Department of Defense (DoD) and Department of Homeland Security (DHS) have different requirements for the protection of Controlled Unclassified Information (CUI), including differences in standards, definitions, assessment requirements and incident reporting obligations. As a result, government contractors supporting defense and military operations must maintain two models and systems toward the same end goal of protecting CUI.

- Definitions of several protected data types — including sensitive personal information, protected health information and personally identifiable information — vary significantly by state and by agency. For example, depending on the state, health records may or may not qualify as sensitive personal information. This means that cybersecurity solutions for the same data may be compliant with certain regulations or contracts but not others.

- The lack of coordination between state and federal agencies in conducting audits and assessments of companies' cybersecurity practices can lead to gaps in regulatory harmonization. Each entity often has their own criteria, process and timeline for evaluating cybersecurity measures. This results in duplicative efforts, confusion and inconsistencies in compliance requirements.

---

[3] We summarize the questions here for concision, highlighting the relevant portions that we address.
[4] *See* 201 CMR 17.00.
[5] *See* Cal. Civ. Code § 1798.81.5(b).

These excessive and duplicative cybersecurity regulations have a direct negative impact on businesses. While cybersecurity audits and examinations serve an important function, duplicative attestations, audits and examinations require companies to incur undue compliance costs without meaningfully strengthening security. In fact, they will require companies to divert resources towards compliance activities, reducing the resources and staff available for those companies' security programs. In particular, the pressure to expand cyber teams for compliance purposes is challenging and potentially harmful in a labor market in which it is already difficult to find workers to fill essential cybersecurity roles. Currently there are more than 650,000 job openings in cybersecurity roles across sectors,[6] and demand outstrips supply by about one-third.[7] For companies subject to multiple regulatory frameworks, requirements may be different even for similar cyber functions which prevents companies from finding efficiencies in control design across their organization and instead can force them to maintain separate procedures for different areas.

ONCD should work to reduce regulatory burdens that distract from companies' security work. ONCD should not impose extraneous requirements or conditions on this undertaking or introduce other topics into this work. For example, ONCD should define the goal of reducing undue regulatory burden broadly and not limit its focus to instances of direct conflict between regulatory requirements. To this end, ONCD should include reducing unnecessary regulation within the scope of its regulatory harmonization work. ONCD, for example, should work to prevent agencies across jurisdictions from each requiring "reasonable security" in ways that, while perhaps consistent on paper, vary widely in practice. Reducing regulatory duplication and unnecessary regulation in this manner would have concrete benefits for companies, allowing them to dedicate more of their resources towards security work (e.g., strengthening systems and monitoring risks) with direct consumer and public benefits rather than to compliance administration.

In addition, ONCD should not tie the goal of regulatory harmonization to the Administration's separate goal of closing regulatory gaps. Although this goal is not expressly stated in the RFI, ONCD explains that "'[h]armonization' as used in this RFI refers to a common set of updated baseline regulatory requirements that would apply across sectors."[8] But there is no need to establish any such regulatory floor before reducing existing regulatory duplication, inconsistency and burden. ONCD should take on the immediate work of regulatory harmonization — for which there is bipartisan support — rather than tie regulatory relief to another far more complex and debated goal.[9]

---

[6] Cybersecurity Supply And Demand Heat Map (cyberseek.org)
[7] NCWES-2023.07.31.pdf (whitehouse.gov)
[8] RFI at 2-3.
[9] We would ask ONCD to publish a separate RFI if it wishes to solicit comment on closing perceived regulatory gaps.

[Q6] Oversight—Reliance on regulatory reciprocity [Q6(i)-(j)], self-attestation [Q 6(k)], and third-party assessments [Q6(l)].

The Administration similarly can provide valuable regulatory relief without taking on more complex policy questions of *how* to regulate cybersecurity in each sector of the economy. Here, ONCD builds on its premise that regulatory harmonization means establishing a consistent regulatory floor by asking about different mechanisms through which such requirements might operate in practice. But this is not the optimal process for addressing complex questions such as the role of third-party auditing and self-attestation in cybersecurity regulatory frameworks. These are extremely nuanced questions that merit close study in the context of a specific proposal and use cases, and answers are not essential before ONCD can provide concrete relief from duplicative and unnecessary cybersecurity regulations.

In the same vein, ONCD should not condition regulatory harmonization on the establishment of complex regulatory reciprocity mechanisms. While the creation of regulatory reciprocity mechanisms may yield benefits in the future, ONCD should initially focus on more readily achievable goals that will streamline regulations and provide immediate, tangible benefits to companies burdened by unnecessary and duplicative cybersecurity regulations. ONCD should focus on reducing undue regulatory burden through known mechanisms (e.g., enforcement discretion, updated guidance from regulators) before establishing a complex system of reciprocity. This approach is also likely to produce useful and specific lessons that can be applied in the context of future reciprocity work.

[Q7] Cloud and Other Service Providers

For the same reasons, this process is not the right context for evaluating whether and how cloud services should be subject to direct regulation. While undoubtedly an important topic, we urge ONCD to focus more narrowly on reducing the regulatory harms that the Administration highlighted in the National Cybersecurity Strategy. ONCD should launch a separate process if it wishes to consider whether and how to regulate cloud services.

II. Take a Forward-Looking, Risk-Based Approach to Regulatory Harmonization

[Q1] Conflicting, mutually exclusive, or inconsistent regulations—Future regulation [Q1(i)-(j)]

[Q4] Third party frameworks

The number of cybersecurity regulations is likely to continue to grow in the coming years, both within the United States and internationally. It accordingly is critical that ONCD chart a clear path towards effective and harmonized cybersecurity regulation in the future.

To achieve this goal, ONCD should encourage all agencies, across jurisdictions, to take a common approach to cybersecurity regulation wherever possible. ONCD should encourage regulatory harmonization around existing regulatory approaches that encourage risk-based and technologically neutral cybersecurity requirements. In particular, ONCD should emphasize regulatory approaches built around the NIST Cybersecurity Framework, broadly adopted international standards and other widely accepted, risk-based approaches to cybersecurity.

In contrast, ONCD should avoid encouraging regulators to move towards a checklist-based approach to cybersecurity regulation. No checklist will ever be adequate to address cybersecurity risk and no regulator will ever have the expertise necessary to dictate specific cybersecurity practices across an industry. ONCD should be careful not to inadvertently weaken cybersecurity by pushing companies to treat it as primarily a compliance exercise in this manner.

Finally, ONCD should not encourage an approach under which regulators will add their own distinct requirements onto a common regulatory baseline. Such an approach would result in exactly the type of conflicting and burdensome regulatory requirements that ONCD is seeking to eliminate[10] but then suggests that sector regulators "could go beyond" this harmonized baseline "to address cybersecurity risks specific to their sectors."[11] This approach would permit the type of regulatory fragmentation and duplication that ONCD should seek to prevent. Allowing multiple regulators to impose the same common standard will lead to unnecessary compliance activities as a single business must demonstrate compliance to multiple agencies and potentially respond to differing agency interpretations of compliance with the common standard—siphoning time and resources away from direct security work. Authorizing different agencies to add on further requirements of their choosing will inevitably result in overlap and conflict between the various regulators' incremental requirements. ONCD should not encourage such an approach.

III. Coordinate Closely with Regulatory Partners

Working with other regulatory partners will be a critical part of ONCD's work on regulatory harmonization. Key regulatory partners with which ONCD should engage include independent federal agencies; state, local, tribal and territorial authorities; and international partners. We welcome ONCD's recognition of the important role these regulatory partners play in establishing cybersecurity requirements. We ask the Administration to work closely with them to develop harmonized approaches to cybersecurity regulation.

---

[10] *See* RFI at 3 ("Sector regulators could go beyond the harmonized baseline to address cybersecurity risks specific to their sectors.")
[11] RFI at 3.

[Q8] State, Local, Tribal, and Territorial (SLTT) Regulation

ONCD should initially focus on harmonization of existing regulatory conflict or overlap. For example, we recommend engaging with the New York Department of Financial Service, which is currently in the process of updating its cybersecurity requirements, on harmonization of its cybersecurity regulation with other requirements that apply to financial institutions under federal law and other state laws. Likewise, as the RFI notes, California has enacted a "reasonable security" requirement for Internet of Things devices.[12] The interaction of this requirement with federal law and other states' laws is by no means clear, creating significant regulatory harm and uncertainty. Other examples of risk and/or harm created by conflicts and overlap between state and federal regulations include:

- Gaps in cybersecurity redundancy. Redundancy, which refers to having multiple layers of protection against cyber threats, is critical to safeguarding cyber assets and eliminating threats. However, inconsistent regulations between state and federal entities require companies to implement different security measures, which can distract from strengthening effective security through strategic redundancy.

- Telecommunications companies operating in multiple states must navigate a patchwork of state and federal regulations across various issues. Inconsistencies and misalignments across requirements increase the risk of confusion, compliance errors and non-compliance. For example, companies are forced to use multiple encryption standards to be responsive to different federal mandates and state preferences. Federal and local guidelines for assessing vendor cybersecurity also differ.

ONCD should work to address these, and other examples of regulatory harms caused by a lack of harmonization between state and federal regulations.

[Q9] International

As discussed above, ONCD has a significant task ahead as it sets out to better harmonize cybersecurity regulation. Much can be accomplished within our borders (e.g., cross-agency harmonization to improve internal alignment). As a result, ONCD should focus its regulatory harmonization efforts domestically at first.

At the same time, we recognize the importance of international regulatory harmonization, particularly for our globally engaged member companies. To the extent that ONCD does work on international harmonization of cybersecurity regulation, it should focus those efforts on large U.S. trading partners that take similar approaches to cybersecurity regulation. In particular, ONCD should focus any initial efforts on encouraging key partners in the EU, UK and

[12] *See* RFI at 13.

Canada to harmonize their regulations with U.S. approaches where possible before expanding its efforts to a broader group of nations."[13]

Conclusion

Business Roundtable looks forward to continued engagement with ONCD and other thought leaders and policymakers on these important topics. To discuss our response or these issues at any time, please contact Amy Shuart, Vice President of Technology & Innovation, Business Roundtable, at ashuart@brt.org or 202-496-3290.

[13] *See* National Cybersecurity Strategy at 34.