June 5, 2024

Testimony of Nick Leiserson

Assistant National Cyber Director for Cyber Policy and Programs

Office of the National Cyber Director

Executive Office of the President

10:00 A.M. EDT

United States Senate

Committee on Homeland Security and Governmental Affairs

Hearing on

"Streamlining the Federal Cybersecurity Regulatory Process: The Path to Harmonization"

Chairman Peters, Ranking Member Paul, and distinguished Senators of the Committee, thank you for the opportunity to testify before you today. The White House Office of the National Cyber Director (ONCD) is still a young organization. Thanks in part to the vision of this Committee, however, we are leaning in to tackle enduring cybersecurity challenges and better protect the nation.

One of these enduring challenges is the need to better harmonize Federal cybersecurity regulations. Since the Committee's last hearing on this topic in 2017, the digital interconnectedness of our society has only grown, as has the sophistication of threat actors in cyberspace. More regulators are stepping up to help manage the unacceptable level of risk that persists in many critical infrastructure sectors, and Congress has granted additional authorities to the government to impose minimum cybersecurity requirements. Yet, our efforts to confront cyber threats aggressively have not been anchored in a comprehensive policy framework for regulatory harmonization. In fact, many of the challenges raised in then-Chairman Johnson's hearing seven years ago continue to ring true.

The Administration is addressing these challenges. Both the National Cybersecurity Strategy (NCS) and the recently signed National Security Memorandum 22 (NSM-22) on "Critical Infrastructure Security and Resilience" prioritize cybersecurity regulatory harmonization. We have made this a priority – in fact, it is the first item in the inaugural National Cybersecurity Strategy Implementation Plan – because duplicative or contradictory cybersecurity regulations not only pose unnecessary costs on regulated entities, they also drain investment away from improvements in actual cybersecurity. By acting strategically, we can achieve better cybersecurity outcomes and lower costs to businesses and their customers.

As the Assistant National Cyber Director for Cyber Policy and Programs, I lead ONCD's regulatory harmonization work, in addition to our efforts to coordinate national cybersecurity policy related to implementation of the Strategy, critical infrastructure protection, cyber insurance, and other, similar topics. Today, I will describe for you ONCD's approach to this hard problem, which has been informed by the more than 80 responses to our request for information (RFI) last year. I will discuss the actions we are taking under the second version of the Implementation Plan, which we released last month. Most importantly, I will convey our hope that we can work closely with Congress to make meaningful progress on this important good government reform effort.

Cybersecurity Regulatory Harmonization & Reciprocity

When I talk about cybersecurity regulatory harmonization, I'm really talking about two concepts that go hand in hand: regulatory *harmonization* and regulatory *reciprocity*.

Cybersecurity regulatory *harmonization* refers to the use of a common set of requirements associated with cybersecurity or information security controls. Harmonization often occurs after efforts to *align* requirements, by ensuring that, when regulators are trying to control for the same type of risk, they are using a common taxonomy for risk management. For example, once there is *alignment* between regulations that certain systems require access controls, *harmonization* of those regulations would be agreeing on allowable forms of multi-factor authentication to access them.

A key focus of ONCD has also been the development of *reciprocity* or *mutual recognition* frameworks for regulations. *Reciprocity* would allow the findings of one regulator that an entity has met a harmonized requirement to meet the requirements of another. In other words, if one regulator found that a company's multifactor authentication was being appropriately used on an information system, another regulator would use the first regulator's finding – not their own, independent assessment – as the necessary proof that the company was complying. Reciprocity can drastically reduce the portion of compliance costs spent on administrative burdens[1] by allowing entities to demonstrate conformance to a regulation once and then reuse that finding for multiple regulators.

Congress has established numerous regulators, each with their own unique authorities, expertise, and responsibility to manage risk within their jurisdiction. Many companies are subject to multiple regulators, whether because parts of their business cross different regulatory authorities, or because they operate across jurisdictional lines (such as state, Federal, and international). While these regulations are rarely harmonized or have reciprocity between them, that is a result of the distinct equities each regulator is addressing. Banks and water treatment plants have different business, environmental, and national security regulations because the risks to each for those sectors are different.

But this all changes for cybersecurity regulations. Cybersecurity controls on information and communications technology (ICT) are unique in that, for many common enterprise ICTs, both the technology and the risk being managed are consistent across sectors. For both banks and water treatment plants, how we define and require access controls should be the same for each because the risk being addressed is the same: preventing unauthorized access. While there are certainly sector-specific technologies that need to be accounted for, business systems across sectors are more similar than different.

As I noted, both the NCS and NSM-22 highlight the importance of cybersecurity regulatory harmonization. This is driven, in part, by the Administration's recognition that we need minimum cybersecurity requirements for critical infrastructure. As National Cyber Director Harry Coker, Jr., testified in January:

> "Sharing situational awareness of [People's Republic of China (PRC)] threat actors – which itself is an objective of the Strategy – is necessary, but not sufficient to meet the magnitude of the threat posed by the PRC and other malicious actors. When it comes to matters of national security, there is a clear need for mandatory cybersecurity requirements to both mitigate risk and to level the playing field to ensure that companies that do make investments in cybersecurity are not disadvantaged in the marketplace."

The stakes are simply too high for us to maintain the regulatory status quo. At the same time, when setting requirements, we must be laser-focused on the outcomes we seek to achieve. Effective cybersecurity regulations minimize the cost and burden of compliance while

[1] Per the OECD: "Administrative burdens can be defined as the costs of complying with information obligations stemming from government regulation. Information obligations can be defined as regulatory obligations to provide information and data to the public sector or third parties." https://www.oecd-ilibrary.org/governance/oecd-regulatory-compliance-cost-assessment-guidance_9789264209657-en.

maximizing their cybersecurity risk reduction effect. Harmonization and reciprocity are key ways to do just that.

By statute, ONCD advises the President on cybersecurity policy and strategy related to the coordination of, among other things, programs and policies intended to improve the cybersecurity posture of the United States. ONCD leads the coordination of implementation of national cyber policy and strategy, including the NCS. Our statutory remit also extends to "the streamlining of Federal… regulations relating to cybersecurity."[2] In alignment with our mission, both the NCS and NSM-22 assign ONCD the responsibility for coordinating cybersecurity regulatory harmonization across the U.S. Government.[3]

ONCD's Efforts on Cybersecurity Regulatory Harmonization & Reciprocity

ONCD began addressing these challenges by developing a vision for regulatory harmonization and reciprocity to mitigate cyber risk. That vision was grounded in the National Cybersecurity Strategy, and included as principles:

1. Baseline cybersecurity requirements should be harmonized across sectors and regulators and should leverage existing cybersecurity frameworks, voluntary consensus standards, and guidance.
2. Proof of compliance with baseline requirements should be reciprocated across regulators.
3. Individual regulators should, when necessary, develop or retain and enforce sector-specific requirements that go beyond baseline requirements and are tailored to the unique risks within the sector that each regulator is charged with managing.

We posit that implementing these principles would produce an end-state that would: strengthen cybersecurity readiness and resilience across all sectors; simplify oversight and regulatory responsibilities of cyber regulators while enabling them to focus on areas of unique, sector-specific expertise; and substantially reduce the administrative burden and cost on regulated entities. These benefits would accrue to regulated companies, the broader public, and to regulators themselves:

- For regulated entities, harmonized and reciprocal cybersecurity oversight approaches would decrease the administrative burden tied to varying or redundant regulatory requirements for similar functions. Through eliminating differing requirements and duplicative examinations, regulated entities could instead devote those additional resources and effort to improving their cybersecurity posture.
- For the American people, the use of a common cybersecurity baseline with reciprocity would lead to the development of standardized tools or services, increasing compliance with the baseline while decreasing cybersecurity costs and helping drive the adoption of the baseline protections beyond regulated sectors. For instance, ICT services that were adapted to meet baseline cybersecurity requirements would be available in other contexts,

[2] Section 1752 of P.L. 116-283 (6 U.S.C. § 1500(c)(1)(C)).
[3] Pursuant to the *Cybersecurity Incident Reporting for Critical Infrastructure Act of 2022* (Division Y of P.L. 117-103), the Cyber Incident Reporting Council coordinates, deconflicts, and harmonizes Federal incident reporting requirements.

including to consumers or small and medium-sized businesses that are not in critical infrastructure sectors.

- For regulators, harmonization and reciprocity would reduce resources needed to perform oversight activities with respect to the common baseline (reciprocity would mean that regulators could divide the waterfront and not examine every control) and provide an opportunity to focus oversight on their key concerns and areas of greatest expertise. By avoiding duplication of effort, regulators would have more time and resources to devote to their individual oversight or supervisory responsibilities.

Pursuant to the National Cybersecurity Strategy Implementation Plan, ONCD began to explore a framework for reciprocity for baseline requirements in conjunction with interagency partners that participate in the Cybersecurity Forum for Independent and Executive Branch Regulators (Cybersecurity Forum). We also released an RFI intended to gather input from industry, civil society, academia, and other government partners about our approach.[4]

Analysis of the RFI Responses

ONCD received 86 unique responses to the RFI, representing 11 of the 16 critical infrastructure sectors, as well as trade associations, nonprofits, and research organizations. In all, the respondents, many of which are membership organizations, represent over 15,000 businesses, states, and other organizations.

Respondents overwhelmingly agreed that the lack of cybersecurity regulatory harmonization and reciprocity posed a challenge to both cybersecurity outcomes and to business competitiveness. For instance, the Business Roundtable, an association of more than 200 chief executive officers of America's leading companies, noted that: "Duplicative, conflicting, or unnecessary regulations require companies to **devote more resources to fulfilling technical compliance requirements without improving cybersecurity outcomes** [emphasis added]." These sentiments were shared across sectors and for businesses of all sizes. The National Defense Industry Association, representing nearly 1,750 corporate members as well as 65,000 individual members from small and mid-sized contractors, highlighted: "Inconsistencies also pose barriers to entry, **especially for small and mid-sized businesses** [emphasis added] that often have limited resources available to establish multiple compliance schemes."

Respondents raised concerns not only about a lack of harmonization and reciprocity across Federal agencies, but also between state and Federal regulators and across international borders. Many lamented a lack of reciprocity to date, noting that investments in compliance across multiple regulatory regimes intended to control the same risk resulted in a net reduction in actual programmatic cybersecurity spending. The Financial Services Sector Coordinating Council highlighted that many sector chief information security officers report spending 30 to upwards of 50 percent of their time on regulatory compliance.

In describing the characteristics of a more harmonized and reciprocal cybersecurity regulatory landscape, RFI respondents touched on themes very similar to ONCD's initial vision:

[4] https://www.federalregister.gov/documents/2023/08/16/2023-17424/request-for-information-on-cyber-regulatory-harmonization-request-for-information-opportunities-for.

- Regulators should continue to focus on aligning to risk management approaches like the National Institute of Standard and Technology (NIST) Cybersecurity Framework.
- Coordinating among regulators to decrease overlapping requirements and collaborating with key allies (such as the United Kingdom, European Union, Canada, and Australia) to drive international reciprocity would materially improve the status quo.
- Elevating the importance of supply chain security would help ensure ICT vendors are held to the same standards as critical infrastructure operators.
- Providing Federal leadership would be essential to achieve these goals and to guide state, local, Tribal, and territorial (SLTT) governments to streamline related regulations.

These themes are consistent with our approach, especially the focus on baseline Federal ICT requirements as a first step with the ultimate goal of reciprocity or mutual recognition with SLTT and international governments, led by the U.S. Government.

Next Steps

Based on feedback from the RFI, ONCD has begun to build a pilot reciprocity framework to be used in a critical infrastructure subsector.[5] We anticipate that this pilot, which we expect to complete early next year, will give us valuable insights as to how best to achieve reciprocity when designing a cybersecurity regulatory approach from the ground up. We are also working with the Cybersecurity Forum to move from alignment to harmonization with respect to certain common cybersecurity controls. These initiatives continue to lay the foundation for more comprehensive efforts to knit dozens of regulatory regimes together.

ONCD's current work is grounded in our vision for regulatory harmonization and reciprocity, and critically informed by the RFI responses. However, this vision, shared by many RFI respondents, cannot be fully achieved without congressional action. As the United States Chamber of Commerce recommended in its filing:

> "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** [emphasis added]."

The Administration supports Chairman Peters's legislation – consistent with the views previously provided to the Committee – that would allow ONCD to better carry out our mission by bringing independent regulatory commissions to the table in a policymaking process, which

[5] Initiative 1.1.5 in the National Cybersecurity Strategy Implementation Plan Version Two states: "The Office of the National Cyber Director (ONCD), working with regulatory departments and agencies (including through the Cybersecurity Forum for Independent and Executive Branch Regulators) and building on findings from its regulatory harmonization request for information, will explore one or more regulatory harmonization and reciprocity pilot programs to establish baseline cybersecurity requirements that model approaches to harmonization and reciprocity."

would act as a catalyst to develop a cross-sector framework more quickly for harmonization and reciprocity. While our current work is piloting a reciprocity framework, our authorities to test harmonization and reciprocity more broadly are limited. Chairman Peters's bill also helpfully includes a limited-scope pilot authority which would allow us, with the consent of a regulated entity, to quickly implement proposals and see if they reduce administrative costs while producing the same (or better) cybersecurity outcomes. We look forward to continuing the dialogue with this Committee and your counterparts in the House to advance this important legislation.

We will also continue to work closely with our partners at the Department of Homeland Security and the Cybersecurity and Infrastructure Security Agency (CISA) as they implement the *Cybersecurity Incident Reporting for Critical Infrastructure Act of 2022*. This Committee provided a novel mechanism to achieve reciprocity for incident reporting in the statute and established the Cyber Incident Reporting Council (CIRC) to harmonize incident reporting regulations. We are committed to helping our partners develop these reciprocity agreements over the next year to minimize duplicative reporting once CISA's final rule goes into effect, and to supporting the CIRC's efforts. We will also continue to work with NIST as they further use of the Cybersecurity Framework 2.0 to be used with international standards and to implement regulatory requirements.

Conclusion

Cybersecurity regulatory harmonization is a problem only government can solve. It means changing how we think about and implement regulations and achieving better cybersecurity outcomes with fewer compliance dollars. By applying more effort on the front end to design strategic regulatory regimes, we can address fundamentally cross-sector cybersecurity risk in a cross-sector – and not siloed – manner.

Regulatory harmonization is a hard problem. It involves coordinating dozens of agencies, each implementing its own unique authorities. It is a problem that has existed for decades – and the trend line is generally heading toward more fragmentation, not more harmonization. National Cyber Director Harry Coker, Jr., has remarked that solving hard problems is why ONCD exists. Given our focus on Federal coherence, regulatory harmonization has been and will remain an ONCD priority.

Finally, cybersecurity regulatory harmonization is a joint problem. It affects all levels – and all branches – of government. It affects regulated entities of all sizes across the country. It requires leadership from the Administration and Congress, informed by the private sector, to together improve our national cybersecurity posture while reducing regulatory burdens.

That national leadership is urgently needed. In meetings with our international counterparts, ONCD personnel, including the Director, have heard that the world is waiting to see where the United States goes next in how it manages cybersecurity risk. They will not wait indefinitely. We have the opportunity to set the stage for more harmonized future, and I hope we will do so, together.