wiley

ALERT

CYBER UPDATE: White House Seeks Regulatory Harmonization While Exploring a Pilot for Reciprocity Amid Proliferation of Regulations

June 5, 2024

Companies, particularly those in "critical infrastructure" sectors, have seen a dramatic increase in cybersecurity regulatory requirements in just the past few years – and the White House is looking to move faster.

At the same time, both the White House and Congress have recognized that overlapping and duplicative regulations pose real problems for companies. The 2023 National Cybersecurity Strategy tasked the Office of the National Cyber Director (ONCD) with harmonizing regulations. ONCD released a report on June 4 that discusses its efforts to develop "a comprehensive policy framework for regulatory harmonization" that aims to "strengthen" cybersecurity resilience across critical infrastructure sectors, "simplify" the work of sector-specific regulators while taking advantage of their unique expertise, and "substantially reduce the administrative burden and cost on regulated entities." Comments clearly indicate frustration with a disjointed regulatory environment that increased compliance costs without a commensurate enhancement in cybersecurity.

ONCD Recognizes Lack of Cyber Regulatory Harmonization Increases Compliance Costs and Harms Outcomes

In August 2023, ONCD released a request for information (RFI) that sought input on challenges regulated entities face from overlapping cybersecurity regulations. The report ONCD released this week includes key findings from the 86 commenters who responded to the RFI:

Authors

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Jacqueline F. "Lyn" Brown
Partner
202.719.4114
jfbrown@wiley.law

Sydney M. White
Special Counsel
202.719.3425
swhite@wiley.law

Joshua K. Waldman
Associate
202.719.3223
jwaldman@wiley.law

Practice Areas

Cybersecurity

Privacy, Cyber & Data Governance

- *First*, the administrative burden of regulatory compliance is diverting resources from cybersecurity operations. The lack of harmonization and reciprocity increases compliance costs which "harms cybersecurity outcomes."
- *Second*, challenges with cybersecurity regulatory harmonization and reciprocity extend to businesses of all sectors and sizes that cross jurisdictional boundaries. The problem of regulatory overlap, and inconsistent or duplicative requirements, extends beyond the federal government to U.S. states and other countries.
- *Third*, both Congress and the Administration can act to make the situation better.

ONCD also provided a summary of comments received on the RFI, and noted a few consistent themes:

- Regulators should focus on aligning with risk management frameworks such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF).
- Regulators should coordinate to decrease overlapping requirements and collaborate with key allies and regional organizations to drive international reciprocity. Multinational companies would see significant benefits from enabling reciprocity with like-minded international partners such as the United Kingdom, Canada, Australia, and the European Union.
- Elevating supply chain security on par with cybersecurity would help ensure information and communications technology vendors are held to the same standards as critical infrastructure operators.
- Federal leadership is needed to achieve these goals and guide state, local, tribal, and territorial governments to streamline regulations.

Critical Infrastructure Sector Comments Focus on Burden of Duplicative Regulations, Urge Alignment

ONCD received over 2,000 pages of comments in response to the RFI including the following key comments about the need for cybersecurity regulatory harmonization and reciprocity from the following critical infrastructure sectors:

- **Communications**: The Communications sector described a disjointed regulatory environment that is inflexible and risks stifling innovation, with redundancy and inconsistency that increases compliance burdens for businesses and costs for consumers.
  - USTelecom wrote that "cybersecurity is a complex and rapidly evolving domain that demands dynamic, flexible action, and collaboration between and among the Government and industry."
  - CTIA–The Wireless Association warned that "a growing patchwork of cybersecurity laws across the states and at the Federal level creates duplicative, inconsistent, or contradictory regulatory frameworks. This fragmentation presents real risks to businesses, consumers, and the overall goals of cybersecurity policy."
  - NCTA–The Internet & Television Association noted that "rigid requirements might either miss the mark or be quickly outpaced by advances in technologies and threats," and suggested that "a

light-touch harmonization process can help avoid conflicting, mutually exclusive, or inconsistent cybersecurity requirements. Such a process can also offer potential avenues, to resolve conflicts, including, if necessary, preemption of state or local requirements to ensure that they do not conflict with Federal policies."

- **Defense Industrial Base**: The Defense Industrial Base (DIB) expressed significant concern about the current structure of cybersecurity regulations and voiced strong support for harmonization of such regulations. The DIB also stressed the need for a more systemic approach to their development and implementation.
  - The National Defense Industrial Association (NDIA) and the National Defense Information Sharing and Analysis Center Policy, Standards and Regulations Working Group (ND-ISAC-WG) stressed the lack of harmonized cybersecurity regulations and the potential adverse impact on both business and national security.
  - NDIA notes that the conflicting objectives and requirements in cybersecurity regulations "pose substantial challenges for contractors and providers of the goods, services, and solutions the Government relies upon to achieve mission success. In consistencies also pose barriers to entry, especially for small and mid-sized businesses that often have limited resources available to establish multiple compliance schemes."
  - The ND-ISAC-WG warned that the "prohibitive costs [of compliance] may drive a strategy of risk acceptance, which may lead to meaningful security gaps."
  - Both NDIA and the ND-ISAC-WG expressed confusion about which federal agency plays the role of primary regulator for the DIB and urged ONCD to work with Congress to find the correct entity for managing cybersecurity standards across the DIB.
- **Information Technology**: The Information Technology sector highlighted the challenges of achieving regulatory agility in an ever-evolving cyber threat environment. The sector stressed the importance of establishing a regulatory regime that applies minimum cybersecurity requirements across all critical infrastructure sectors while accommodating sector-specific risks. The sector also highlighted the need for federal leadership to drive reciprocity at all levels of the government.
  - Dragos observed that "cybersecurity defenses have advanced in fragmented, and often reactive ways, and so has the regulatory environment guiding the implementation of those defenses." The result is that "well-meaning initiatives from myriad Government agencies have been launched without reference to one another, creating a tangled, confusing, and ultimately counterproductive compliance environment."
  - Microsoft noted that "the primary challenge [...] caused by regulatory divergence is increased complexity and costs associated with monitoring, analyzing, and managing compliance with redundant cybersecurity requirements."
  - Microsoft proposed that "ONCD should establish a single regulatory framework for applying cybersecurity standards within regulations." Microsoft added that "ONCD should also advance a

> legislative proposal to enact policies and procedures that would require all regulators, including independent ones, to use the regulatory framework to ensure broad adoption."

ONCD Highlights Need for Additional Security Measures in Supply Chain

Notably, ONCD pointed to a comment from the Energy sector that identified concerns about key suppliers, particularly information and communications technology vendors that provide critical equipment or services to critical infrastructure operators but are not themselves subject to sector-specific regulations. ONCD's highlighting of supply chain issues is consistent with its and the Cybersecurity and Infrastructure Security Agency's focus on encouraging makers of technology products to have more security built into them.

ONCD Is Developing a Reciprocity Framework for Critical Infrastructure as a Pilot Project

ONCD plans to use the report to inform its pilot effort to develop a reciprocity framework for a designated critical infrastructure sector. A companion blog post from the head of ONCD describes the pilot as seeking to "design a cybersecurity regulatory approach from the ground up." The blog calls on Congress for help to bring relevant agencies together "to develop a cross-sector framework for harmonization and reciprocity for baseline cybersecurity requirements."

Congress Begins to Focus on Cyber Regulatory Harmonization

Working on a parallel track, Congress is becoming increasingly concerned about the growing need for cybersecurity regulatory harmonization as new federal agency cybersecurity requirements, taking disparate approaches, seem to be announced every week. On June 5, the Senate Homeland Security and Governmental Affairs Committee (HSGAC) held a hearing titled "Streamlining the Federal Cybersecurity Regulatory Process: The Path to Harmonization." Chairman Gary Peters (D-MN) announced he is working on legislation that would build on the pilot efforts initiated by the ONCD to harmonize the patchwork of information security and cybersecurity regulations applicable to regulated companies particularly the 16 critical infrastructure sectors.

We will break down the bill and the hearing in our next alert. Stay tuned.

***