wiley

ALERT

Calls for Cybersecurity Regulatory Harmonization Ramp Up in Congress, White House

June 7, 2024

The proliferation of cybersecurity regulations has the White House and Congress calling for harmonization to streamline regulations, focus on reciprocity, and decrease compliance costs. Senator Gary Peters (D-MI), chair of the U.S. Senate Committee on Homeland Security and Government Affairs (HSGAC), is working on legislation to harmonize the patchwork of cybersecurity regulations imposed by federal regulatory agencies on regulated sectors, particularly critical infrastructure sectors. Senator Peters chaired an HSGAC hearing on June 5, 2024 on "Streamlining the Federal Cybersecurity Regulatory Process: The Path to Harmonization," to explore harmonization after the Office of the National Cyber Director (ONCD) issued its *Summary of the 2023 Cybersecurity Regulatory Harmonization Request for Information* (RFI Summary) on June 4. As we noted in our June 5 client alert, ONCD received 86 comments on its RFI with many calling for a solution to the lack of cybersecurity regulatory harmonization and reciprocity, which results in costly, duplicative compliance obligations and harms cybersecurity outcomes.

The *Cybersecurity Regulatory Harmonization Act*, which has not been introduced yet, would require the ONCD to establish an interagency "Harmonization Committee" to harmonize information security and cybersecurity regulations issued by regulatory agencies. Given the bipartisan nature of cybersecurity, the bill may be a candidate for inclusion in the 2025 National Defense Authorization Act (NDAA), the annual defense authorization legislation that consistently draws cybersecurity amendments.

Authors

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Jacqueline F. "Lyn" Brown
Partner
202.719.4114
lbrown@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
Government Contracts
Privacy, Cyber & Data Governance
Telecom, Media & Technology

The Bill Seeks to Harmonize Information Security and Cybersecurity Regulatory Regimes

Under the bill, the ONCD will chair the Harmonization Committee, which will develop a baseline regulatory framework that regulatory agencies will use to harmonize information security and cybersecurity regulatory regimes. The Committee will be comprised of a representative from each regulatory agency with authority to issue cybersecurity regulations, the Office of Information and Regulatory Affairs of the Office of Management and Budget (OMB), each Sector Risk Management Agency (SRMA), and other appropriate agencies, as determined by the Chair.

No later than one year after the bill is signed into law, the Harmonization Committee must develop a cybersecurity regulatory framework for achieving harmonization between each regulatory agency. The framework must, at a minimum, achieve the following:

1. Establish a reciprocal compliance mechanism for baseline cybersecurity requirements for entities regulated by more than one regulatory agency;
2. Identify information security or cybersecurity regulations that are overly burdensome, inconsistent, or contradictory; and
3. Develop recommendations for updating regulations to address those requirements that are found to be overly burdensome, inconsistent, or contradictory.

The bill does not address regulations or guidance relating to information security or cybersecurity issued by SRMAs. Such SRMA guidance includes the voluntary, baseline Cross-Sector Cybersecurity Performance Goals issued by the Cybersecurity and Infrastructure Security Agency (CISA), which are being applied to a critical infrastructure sector by at least one regulatory agency, the Federal Communications Commission.

Pilot Program to Test the Regulatory Harmonization Framework

Under the bill, once the Harmonization Committee completes the regulatory framework and it is published in the Federal Register, the Committee will create an implementation pilot program by selecting at least three regulatory agencies and a minimum of three regulations containing information security or cybersecurity requirements. The regulations selected for the pilot program must have "substantially similar" or "substantially related" cybersecurity requirements such that a regulated entity would be subject to at least two of the regulations simultaneously. Each agency and regulated entity must voluntarily agree to participate in the pilot.

The bill also requires the head of the regulatory agencies to "consult" with the Harmonization Committee prior to issuing new or updated information security or cybersecurity regulations. The purpose is to "ensure that the regulation is aligned to the greatest extent possible with the regulatory framework." By limiting the Harmonization Committee to consultation on new or updated regulations and establishing a voluntary pilot program based on a cybersecurity framework, the bill artfully avoids Constitutional problems.

By directing the ONCD-led Harmonization Committee to develop the framework and establish a pilot program, the bill may be able to achieve greater policy change than the Cyber Incident Reporting Council (CIRC) – which was established pursuant to the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) to address harmonization of cyber incident reporting regulations, but which is limited to making recommendations. If the Harmonization Committee creates a harmonization framework mechanism that begins to consolidate the patchwork of cybersecurity regulations, it will be a much-needed and positive first step towards harmonization and deconfliction of the myriad of regulations critical infrastructure entities now face.

The bill's authors folded in a provision on the CIRC, which requires the U.S. Department of Homeland Security to provide the relevant congressional committees with an update on the CIRC's efforts on harmonizing cyber incident reporting within 180 days and every 180 days thereafter. It would be even more encouraging, however, if Congress would simultaneously act on some of the recommendations CIRC issued earlier this year, including removing statutory barriers to incident reporting harmonization and expanding the Freedom of Information Act exemptions under CIRCIA to any cyber incident reports submitted to the federal government.

Congressional Testimony Focuses on Alignment and Reciprocity

The HSGAC hearing reflected the broad, bipartisan consensus on the importance of addressing cybersecurity regulatory harmonization. Nick Leiserson, Assistant National Cyber Director for Cyber Policy and Programs, ONCD, provided an overview of the Administration's prioritization of cybersecurity regulatory harmonization in the National Cybersecurity Strategy, the National Cybersecurity Strategy Implementation Plan versions 1 and 2, and the National Security Memorandum 22 on Critical Infrastructure and Resilience.

According to Mr. Leiserson, regulatory harmonization must be tied to agencies reaching alignment on what risks require controls and then agreeing on a common framework for cybersecurity. This will enable reciprocity or mutual recognition between the regulators "allowing entities to demonstrate conformance once and then reuse that finding for multiple regulators." A minimum cross-sector framework is feasible, he indicated, because the technology and risks related to information and communications technology (ICT) and "business systems" are consistent across sectors. The unique risks of a sector, he said, can be addressed by sector-specific regulations built on top of the baseline framework.

ONCD has already begun to build a reciprocity framework on which to base a pilot. Mr. Leiserson testified, however, that Chairman Peters' legislation would "allow ONCD to better carry out our mission by bringing independent regulatory commissions to the table in a policymaking process, which would ... [allow for the development of] a cross-sector framework more quickly for harmonization." It would also include helpful "limited-scope pilot authority."

David Hinchman, Director of Information Technology and Cybersecurity at the U.S. Government Accountability Office (GAO), echoed the February 2024 GAO Report, which recommended "outcome oriented" performance measures" to measure the progress made under the National Cybersecurity Strategy. Mr. Hinchman said developing definitive goals to measure against will be essential to gauging harmonization efforts. Mr.

Hinchman testified in support of using the National Institute of Standards and Technology (NIST) Cybersecurity Framework as a baseline for cybersecurity regulations.

Critical Infrastructure Entities May Not See Regulatory Harmonization Anytime Soon

Since HSGAC's last hearing on cybersecurity harmonization in 2017, the regulatory framework surrounding cybersecurity has become overly burdensome, inconsistent, and even contradictory at times – creating a complicated and risky situation for critical infrastructure entities that are already in a difficult position trying to protect their companies' ICT and data and for some entities, that of customers. Compliance burdens have skyrocketed and detracted from organizational efforts to manage increasingly sophisticated cyber threats. There is no indication that this lack of harmony will improve anytime soon absent intervention from the Harmonization Committee or a congressional oversight committee.

For the Defense Industrial Base and other government contractors alone, already on the horizon are new cybersecurity regulations from the U.S. Department of Defense and Federal Acquisition Regulatory Council and secure software attestation requirements from CISA and OMB. These are in addition to the current U.S. Securities and Exchange Commission, Federal Acquisition Regulations, Defense Federal Acquisition Regulations on cybersecurity measures, and the Federal Risk and Authorization Management Program cybersecurity accreditation requirements that many government contractors are already subject to. There are also numerous sector-specific cybersecurity regulations promulgated by the Federal Trade Commission, Consumer Financial Protection Bureau, U.S. Department of the Treasury, Office of the Comptroller of the Currency, Financial Industry Regulatory Authority, U.S. Department of Health and Human Services, and Federal Communications Commission, among others, that need to be considered as well.

It has become increasingly clear that regulatory agencies will not voluntarily harmonize or deconflict with each other. Instead, the burden has fallen on Congress to take meaningful steps to declutter the landscape and make it easier for covered entities to protect against nation-state and other criminal threat actors. There has already been bipartisan support for these efforts, including through the 2022 passage of CIRCIA and the Administration's National Cybersecurity Strategy and Implementation Plan versions 1 and 2. This bill is a next step.

***

Wiley's Privacy, Cyber & Data Governance; Telecom, Media & Technology; and Government Contracts practices counsel clients on the evolving landscape of cybersecurity regulations. We engage with key government stakeholders in this area and will stay abreast of any developments as this bill progresses through Congress. Please reach out to the authors with any questions.