R Street
Free markets. Real solutions.

R Street Policy Study
No. 306
June 2024

Decoding Organizations' Responses to U.S. Cybersecurity Regulatory Harmonization Efforts with Data Science

By Amy Chang, Mumtaz Fatima, and Haiman Wong

A common theme emerged from our review: Most of the responding organizations expressed a preference for sector-specific, collaborative cybersecurity regulations over a one-size-fits-all approach.

Table of Contents

Executive Summary

The U.S. cybersecurity regulatory landscape is complex, with overlapping and inconsistent regulations across federal, state, and local levels. Naturally, this creates challenges for organizations that are trying to comply with the patchwork of laws and regulations while also reserving enough resources to safeguard their cybersecurity. To improve this landscape, the White House Office of the National Cyber Director (ONCD) sought feedback through a request for information (RFI) on regulatory harmonization. That RFI received 86 unique responses.

We reviewed these responses, grouped them into five sectors (critical infrastructure organizations, trade associations, consulting firms, cybersecurity organizations, and technology companies), and delineated sector-specific and aggregate findings. A common theme emerged from our review: Most of the responding organizations expressed a preference for sector-specific, collaborative cybersecurity regulations over a one-size-fits-all approach. Our understanding, however, is that ONCD (in conjunction with regulators and other federal agencies) has been working

on developing baseline cybersecurity measures rather than sector-specific approaches. With the insight gathered from the RFI responses, we encourage the U.S. government to generate buy-in for a consistent vision for harmonization and align priorities and expectations with stakeholders to create a more efficient and effective cybersecurity regulatory environment that both enhances national cybersecurity resilience and balances sector-specific needs.

Key findings of our analysis include the following:

- The U.S. government's intent to pursue regulatory harmonization may not have been clear in the RFI and other scoping documents, or respondents may not have fully comprehended the government's definition of harmonization, as many suggestions outlined in the responses did not fully align with the document's proposed goal of harmonization.

- Despite ONCD's intent that harmonization be the creation (or consolidation) of a common set of cybersecurity baseline requirements across sectors, many respondents suggested that regulations be tailored to each sector's unique needs through collaboration between regulators and industry.

- Respondents explained that overly prescriptive, checklist-based regulations divert resources from addressing real cybersecurity threats; they also expressed that regulations struggle to keep pace with the rapidly evolving cyber landscape and become outdated quickly.

- Respondents believed that consolidating reporting and auditing requirements under fewer regulatory bodies could reduce compliance burdens.

When considering next steps for harmonization efforts, we recommend that the U.S. government:

- Harmonize definitions and intent across the federal government (potentially by designating a coordinating body or continuing to leverage ONCD's position as a convener of stakeholders) to provide clear guidance and avoid misunderstandings;

- Conduct more targeted RFIs, apply additional analysis techniques to the existing data, or gather further information to gain deeper insights on the topic;

- Ensure that the needs and concerns of smaller organizations, which may lack resources to respond to RFIs, are considered in regulatory discussions;

- Align priorities and expectations with stakeholders such as policymakers, regulatory bodies, industry professionals, and cybersecurity experts.

Introduction

The cybersecurity regulatory space is crowded. Regulations for standards, compliance, and enforcement exist across state, local, tribal, territorial, and federal entities, and these regulations are often duplicative, redundant, or conflicting—particularly across different levels of government. Not only does this make it difficult for organizations to comply with all the necessary regulations, but it also impedes their ability to reach the optimal desired end state of materially improved cybersecurity.

The White House Office of the National Cyber Director (ONCD), along with other government entities, is seeking to improve the cybersecurity regulatory landscape.

The White House Office of the National Cyber Director (ONCD), along with other government entities, is seeking to improve the cybersecurity regulatory landscape. This effort stems, in part, from an objective put forth in the March 2023 National Cybersecurity Strategy and its implementation plan.[1]

To support these efforts, in July 2023, ONCD announced a request for information (RFI) on cybersecurity regulatory harmonization, regulatory reciprocity, and assessments and audits of regulated entities.[2] It invited comments on "cybersecurity regulatory conflicts, inconsistencies, redundancies, challenges, and priorities."[3] The RFI received 86 unique responses.[4]

In this paper, we analyze and synthesize the responses to provide clear insight on themes policymakers should consider when approaching cybersecurity regulatory harmonization. We start by explaining our methodology for grouping and evaluating the RFI responses and then provide specific insights for each of the five sectors into which we categorized the responses. We also analyze the responses in aggregate to uncover broader trends and potential areas for further research with the hope that such insights will serve as jumping off points for improving the cybersecurity regulatory environment.

Methodology

To begin our analysis, we downloaded each of the 86 responses from the RFI repository hosted on regulations.gov.[5] We then categorized the responding entities into one of the following five sectors: critical infrastructure organizations, trade associations, consulting firms, cybersecurity organizations, and technology companies. There was minor overlap across these categories. For example, the critical infrastructure sector could have included information technology

1. "Fact Sheet: Biden-Harris Administration Announces National Cybersecurity Strategy," The White House, March 2, 2023. https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/02/fact-sheet-biden-harris-administration-announces-national-cybersecurity-strategy; "Fact Sheet: Biden-Harris Administration Publishes the National Cybersecurity Strategy Implementation Plan," The White House, July 13, 2023. https://www.whitehouse.gov/briefing-room/statements-releases/2023/07/13/fact-sheet-biden-harrisadministration-publishes-thenationa/.l-cybersecurity-strategyimplementation-plan.
2. "Fact Sheet: Office of the National Cyber Director Requests Public Comment on Harmonizing Cybersecurity Regulations," Office of the National Cyber Director, July 19, 2023. https://www.whitehouse.gov/oncd/briefing-room/2023/07/19/fact-sheet-office-of-the-national-cyber-director-requests-public-comment-on-harmonizing-cybersecurity-regulations; "Request for Information on Cyber Regulatory Harmonization; Request for Information: Opportunities for and Obstacles To Harmonizing Cybersecurity Regulations," Office of the National Cyber Director, Aug. 16, 2023. https://www.federalregister.gov/documents/2023/08/16/2023-17424/request-for-information-on-cyber-regulatory-harmonization-request-for-information-opportunities-for.
3. "Request for Information on Cyber Regulatory Harmonization; Request for Information: Opportunities for and Obstacles To Harmonizing Cybersecurity Regulations." https://www.federalregister.gov/documents/2023/08/16/2023-17424/request-for-information-on-cyber-regulatory-harmonization-request-for-information-opportunities-for.
4. Ibid.
5. Ibid.

organizations, but given the nature of the topic, we analyzed those as two distinct categories: cybersecurity and technology corporations. After categorizing the responding entities, we used a combination of machine learning and natural language processing (NLP) to analyze each RFI response.

To ensure the accuracy and efficiency of the model, we prepared the raw data by conducting text preprocessing. Preprocessing included steps such as cleaning the text of characters that did not qualify as words (including URLs) and removing punctuation and numerical digits, tokenization, and stemming/lemmatization.[6] We also conducted named-entity recognition to identify and classify key information in the text and allow for deeper and richer analyses.[7]

In the exploratory phase of our study, we used a variety of data-analysis techniques. We evaluated the RFI responses within the category groupings and generated word clouds of the most prominent themes.[8] We also completed latent Dirichlet allocation topic modeling, which is a technique that scans a set of documents, detects patterns, and identifies topics that characterize the dataset.[9] Finally, we conducted sentiment analysis, a machine learning technique that can determine the emotional tone or sentiment of text, to assess whether the responses in each category conveyed a more positive or negative sentiment toward regulatory harmonization.[10]

Analysis

As noted previously, for our sector-specific analysis, we categorized RFI responses into one of five groups: critical infrastructure organizations, trade associations, consulting firms, cybersecurity organizations, and technology companies. In the sections that follow, we discuss our sector-specific findings, as well as aggregate findings and themes.

To set the stage for these discussions, Figure 1 presents a word cloud to visually represent the top 50 words used within the entire dataset of responses.

Combining this information with topic modeling analysis enables us to gain insights into key themes and issues that emerged from our analysis. For example, the prominence of the word "compliance" (the third most frequently used word, 594 instances) could suggest that respondents deemed compliance and adherence to regulatory frameworks and standards to be a worthwhile topic to discuss in depth. In addition, topic modeling for the cybersecurity sector noted that "compliance" frequently occurred with words such as "burden" and "overlapping," indicating concerns about challenges posed by overlapping and conflicting cybersecurity compliance requirements. Similarly, terms like "sector" (408 instances) appeared

Figure 1: Word Cloud of Entire Dataset

Figure created using RSI analysis.

6. "Text Preprocessing," Codecademy, last accessed May 20, 2024. https://www.codecademy.com/learn/dsnlp-text-preprocessing/modules/nlp-text-preprocessing/cheatsheet.
7. "What is named entity recognition?," IBM, last accessed May 20, 2024. https://www.ibm.com/topics/named-entity-recognition.
8. "Generating WordClouds in Python Tutorial," DataCamp, last accessed May 20, 2024. https://www.datacamp.com/tutorial/wordcloud-python.
9. "What is Topic Modeling? An Introduction With Examples," DataCamp, last accessed May 20, 2024. https://www.datacamp.com/tutorial/what-is-topic-modeling.
10. "NLTK Sentiment Analysis Tutorial for Beginners," DataCamp, last accessed May 20, 2024. https://www.datacamp.com/tutorial/text-analytics-beginners-nltk.

frequently alongside "management" (343 instances) and "agencies" (355 instances). The prominence of these terms, especially when listed together in topic analysis, indicated the frequent use of the term "sector risk management agencies" or SRMAs, which are agencies responsible for delineating unique risk profiles and implementing regulations and strategic guidance across different critical infrastructure sectors. This suggests that many respondents discussed the challenges of managing cybersecurity risks and harmonizing frameworks, controls, and assessments across critical infrastructure sectors, especially with the involvement of multiple stakeholders such as SRMAs. It also signals that respondents likely viewed cybersecurity regulatory harmonization through the lens of sector-specific frameworks and regulations, which is a theme we will see repeated in the sector-specific analysis below.

Critical Infrastructure Organizations

We classified 21 RFI responders as critical infrastructure organizations (either directly or indirectly), which included financial services, energy, telecommunications, and health care organizations.[11] Although information technology is also critical infrastructure, given the nature of the RFI, we considered that sector to be significant enough to warrant its own groupings (we classified such organizations as either cybersecurity or technology organizations in our analysis).

The prevailing theme that emerged from this sector's responses was the need to revise existing standards and frameworks to meet contemporary cybersecurity requirements. One RFI response from this group suggested that regulators prioritize aligning existing regulations to cybersecurity guidelines (e.g., NIST SP 800-53B) instead of introducing new harmonized regulations.[12] Other responses criticized the slow pace at which existing regulations are updated, particularly given the rapidly evolving landscape of cyber threats.[13] The sentiment analysis of this group's responses indicated heavy negative sentiment (71 percent) toward regulatory harmonization, which correlates with some of the concerns detailed herein.

Companies expressed concern of harmonizing auditing procedures, noting the high cost and challenge of having to provide different types of reporting to different regulators, often with different requirements.

Because this category includes government, health care, energy, telecommunications, and finance-related organizations, topic modeling revealed some notable sub-themes emerging within these individual categories. For example, health care entities expressed concern over the cybersecurity of legacy medical devices, highlighting the high cost of retiring functioning medical devices when manufacturers discontinue support and calling for facilitated conversations between regulators, health care delivery organizations, and medical manufacturers to address this risk management issue.[14] Energy sector respondents noted a need to

11. "Critical Infrastructure Sectors," Cybersecurity and Infrastructure Security Agency, last accessed May 20, 2024. https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors.
12. "Comments of Kaiser Permanente in Response to Request for Information on Cyber Regulatory Harmonization," Docket No. ONCD-2023-0001-0050, Oct. 30, 2023. https://www.regulations.gov/comment/ONCD-2023-0001-0050; Computer Security Resource Center, "Control Baselines for Information Systems and Organizations: NIST Publishes SP 800-53B," National Institute of Standards and Technology, Oct. 29, 2020. https://csrc.nist.gov/news/2020/control-baselines-nist-publishes-sp-800-53b.
13. See, e.g., "Comments of Department of Interior in Response to Request for Information on Cyber Regulatory Harmonization," Docket No. ONCD-2023-0001-0060, Oct. 30, 2023. https://www.regulations.gov/comment/ONCD-2023-0001-0060.
14. See, e.g., "Comments of Premier Inc. in Response to Request for Information on Cyber Regulatory Harmonization," Docket No. ONCD-2023-0001-0078, Oct. 29, 2023. https://www.regulations.gov/comment/ONCD-2023-0001-0078.

protect not just information technology but also operational technology systems.[15] Financial services companies expressed a primary concern of harmonizing auditing procedures, noting the high cost and challenge of having to provide different types of reporting to different regulators, often with different requirements.[16] One respondent suggested that, instead of companies having to respond to requests from multiple regulators, a primary regulator take requests from various regulators and compile a list of documents and specifications that the institution would need to provide.[17] This information could be stored with the central body and provided to regulators each time certain information is requested.

Trade Associations

This was the largest category of RFI respondents (35), and these associations and councils represent thousands of member organizations. The analysis of responses from this sector revealed the desire for consolidating existing regulatory entities into a single point-of-contact agency for reporting, auditing, and compliance purposes. The sentiments of the responses in this category conveyed a nearly even split between positive (55 percent) and negative (45 percent) attitudes toward regulatory harmonization.

Some associations noted that their member executives and staff spent a disproportionate amount of budgetary resources and time to maintain compliance with multiple regulatory regimes, rather than on other core focuses of their job (like chief information security officers defending their networks and systems).[18] Other organizations expressed the belief that implementing regulatory harmonization, adopting consistent terminology, and streamlining regulatory entity oversight and involvement would translate into a reduction in time spent and costs incurred by businesses and entities represented in this category.[19] Instead of responding to data requests, audits, and compliance checks from multiple agencies, businesses could redirect efforts toward promoting effective cybersecurity practices.

Member executives and staff spent a disproportionate amount of budgetary resources and time to maintain compliance with multiple regulatory regimes, rather than on other core focuses of their job.

Another recurring theme was the desire to create standard definitions and consistent terminology for key terms across different regulations.[20] Using accepted standard definitions would enable organizations to streamline compliance procedures and fill gaps, and consistent terminology would enable organizations to map similar regulatory requirements across different jurisdictions, allowing for more effective risk management. The responses also recognized

15. See, e.g., "Comments of Edison Electric Institute in Response to Request for Information on Cyber Regulatory Harmonization," Docket No. ONCD-2023-0001-0039, Nov. 1, 2023. https://www.regulations.gov/comment/ONCD-2023-0001-0039.
16. See, e.g., "Comments of BITS/Bank Policy Institute and American Bankers Association in Response to Request for Information on Cyber Regulatory Harmonization," Docket No. ONCD-2023-0001-0069, Oct. 30, 2023. https://www.regulations.gov/comment/ONCD-2023-0001-0069.
17. "Comments of National Defense Industry Association in Response to Request for Information on Cyber Regulatory Harmonization," Docket No. ONCD-2023-0001-0085, Oct. 30, 2023. https://www.regulations.gov/comment/ONCD-2023-0001-0085.
18. See, e.g., "Comments of Financial Services Sector Coordinating Council in Response to Request for Information on Cyber Regulatory Harmonization," Docket No. ONCD-2023-0001-0052, Nov. 1, 2023. https://www.regulations.gov/comment/ONCD-2023-0001-0052.
19. See, e.g., "Comments of U.S. Chamber of Commerce in Response to Request for Information on Cyber Regulatory Harmonization," Docket No. ONCD-2023-0001-0034, Oct. 30, 2023. https://www.regulations.gov/comment/ONCD-2023-0001-0034.
20. See, e.g., "Comments of National Defense Industry Association in Response to Request for Information on Cyber Regulatory Harmonization," Docket No. ONCD-2023-0001-0085. https://www.regulations.gov/comment/ONCD-2023-0001-0085.

the need for a baseline set of standards for emerging technologies like artificial intelligence (AI) and the Internet of Things (IoT).[21]

Some overlap exists between the themes that emerged in this category and the cybersecurity category. For example, both highlight the need for international collaboration between agencies like the National Institute of Standards and Technology (NIST), the Center for Internet Security, and the International Organization for Standardization (ISO) so businesses can map regulatory requirements across different markets.[22] In addition, organizations in these categories often have a multinational presence, so their ideal regulatory outcome would consider global standards and other regional regulatory frameworks.

Consulting Firms

We categorized nine responses as coming from the consulting sector. Organizations in this sector were generally not opposed to harmonized standards but were more interested in a sector-specific, outcome-focused, nonprescriptive approach to cybersecurity regulations. Because consulting firms typically help customers understand the cybersecurity landscape or assist with compliance to different regulations, words such as "compliance," "business," "cost," and "effort" appeared frequently in this sector's responses. Topic analysis revealed that these organizations were focused on finding ways to alleviate the financial and operational burdens of cybersecurity compliance for critical infrastructure organizations, particularly those in heavily regulated sectors. Compliance costs and efforts are often cited as pressing concerns by their clients.[23]

Topic analysis revealed that these organizations were focused on finding ways to alleviate the financial and operational burdens of cybersecurity compliance for critical infrastructure organizations, particularly those in heavily regulated sectors.

Key areas of focus for the respondents in this category included cost considerations, management, AI, time constraints, and privacy concerns. Similar to critical infrastructure entities, a prominent theme that emerged from topic modeling of this category was the cost of compliance. One response from this group argued that harmonizing regulations to establish baseline standards might not effectively address cost concerns for large organizations; although common risk and control libraries exist, they may not fully align with an organization's specific business and operational model.[24] Sentiment analysis conveyed a near 50/50 split between positive (44 percent) and negative (56 percent) attitudes regarding regulatory harmonization among this sector.

Consulting organizations often work with both federal and private sector agencies on cybersecurity compliance, risk management, and alignment of security solutions to business priorities. These groups understand that a cyber regulatory

21. See, e.g., "Comments of DIGITALEUROPE in Response to Request for Information on Cyber Regulatory Harmonization," Docket No. ONCD-2023-0001-0063, Oct. 30, 2023. https://www.regulations.gov/comment/ONCD-2023-0001-0063.
22. "CIS Benchmarks List," Center for Internet Security, last accessed May 20, 2024. https://www.cisecurity.org/cis-benchmarks.
23. Clark O'Niell et al., "As Budgets Get Tighter, Cybersecurity Must Get Smarter," Boston Consulting Group, April 24, 2023. https://www.bcg.com/publications/2023/navigating-the-new-cybersecurity-environment; "Regulatory productivity: Is there an answer to the rising cost of compliance?," Deloitte, last accessed June 7, 2024. https://www2.deloitte.com/us/en/pages/regulatory/articles/cost-of-compliance-regulatory-productivity.html.
24. "Comments of Accenture in Response to Request for Information on Cyber Regulatory Harmonization," Docket No. ONCD-2023-0001-0070, Oct. 30, 2023. https://www.regulations.gov/comment/ONCD-2023-0001-0070.

harmonization push would represent a snapshot in time and that staying cyber secure requires continuous adaptation to maintain compliance. Respondents from this sector therefore recommended pre-mapping a set of objectives to a starter set of policies, which could help streamline the compliance process by providing a foundation for organizations to build upon.[25] They also mentioned using the NIST 800-53 and 800-171 frameworks and adapting maturity models like Cybersecurity Maturity Model Certification (CMMC) and Capability Maturity Model Integration (CMMI) to assist with harmonization.[26] Responses from this sector identified the importance of improving education and awareness around cybersecurity and equipping small businesses with resources to implement cybersecurity controls and assess risks.[27]

Another recurring theme in this category was the push for sector-specific harmonization of cybersecurity regulations. For example, one organization recommended defining sector-specific standard operating procedures, risk and control libraries, and a starter set of compliance policies.[28] Some of this sector's respondents advocated for outcome-based frameworks that allow flexibility in implementation, drawing inspiration from existing international standards like ISO and the International Electrotechnical Commission as the baseline. [29]

These groups understand that a cyber regulatory harmonization push would represent a snapshot in time and that staying cyber secure requires continuous adaptation to maintain compliance.

Cybersecurity Organizations

Fifteen organizations were classified as cybersecurity organizations in our analysis. These groups are naturally more focused on the cybersecurity landscape than other groups in the RFI response pool, so it is not surprising that they support joint efforts and insight-sharing of cybersecurity advances, best practices, and support strategies for businesses across different countries.

One of the common themes that emerged from this category of responses was the cost of maintaining compliance across duplicative, inconsistent regulations put forth by different agencies. For example, one organization outlined the lack of alignment of different specifications between frequency, scope, and internality vs. externality of penetration testing for financial institutions.[30] These organizations also favored outcomes-focused, risk-based regulations over prescriptive ones.[31]

25. Ibid.
26. Computer Security Resource Center, "NIST SP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations," National Institute of Standards and Technology, Dec. 10, 2020. https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final; Computer Security Resource Center, "NIST SP 800-171 Rev. 3, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations," National Institute of Standards and Technology, Dec. 10, 2020. https://csrc.nist.gov/pubs/sp/800/171/r3/final; Chief Information Officer, "Cybersecurity Maturity Model Certification (CMMC) 2.0," U.S. Department of Defense, last accessed May 20, 2024. https://dodcio.defense.gov/CMMC/Model; "Capability Maturity Model Integration (CMMI)," ISACA, last accessed May 20, 2024. https://cmmiinstitute.com.
27. See, e.g., "Comments of Alex Sharpe in Response to Request for Information on Cyber Regulatory Harmonization," Docket No. ONCD-2023-0001-0006, Sept. 18, 2023. https://www.regulations.gov/comment/ONCD-2023-0001-0006.
28. See, e.g., "Comments of Accenture," Docket No. ONCD-2023-0001-0070. https://www.regulations.gov/comment/ONCD-2023-0001-0070.
29. "Comments of Accenture," Docket No. ONCD-2023-0001-0070. https://www.regulations.gov/comment/ONCD-2023-0001-0070; "Comments of Boston Consulting Group in Response to Request for Information on Cyber Regulatory Harmonization," Docket No. ONCD-2023-0001-0031, Oct. 30, 2023. https://www.regulations.gov/comment/ONCD-2023-0001-0031; "Comments of Deloitte in Response to Request for Information on Cyber Regulatory Harmonization," Docket No. ONCD-2023-0001-0011, Oct. 29, 2023. https://www.regulations.gov/comment/ONCD-2023-0001-0011; International Organization for Standardization, "ISO/IEC 27001:2022," last accessed May 20 2024. https://www.iso.org/standard/27001; "ISA/IEC 62443 Series of Standards," International Society of Automation, last accessed May 20, 2024. https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards"
30. "Comments of Privacy and Security Research Team at the Georgia Institute of Technology in Response to Request for Information on Cyber Regulatory Harmonization," Docket No. ONCD-2023-0001-0059, Oct. 30, 2023. https://www.regulations.gov/comment/ONCD-2023-0001-0059; Christopher Olson, "Penetration Testing in the Financial Services Industry," SANS Institute, March 9, 2010. https://www.sans.org/white-papers/33314.
31. See, e.g., "Comments of Dragos in Response to Request for Information on Cyber Regulatory Harmonization," Docket No. ONCD-2023-0001-0081, Oct. 31, 2023. https://www.regulations.gov/comment/ONCD-2023-0001-0081.

They noted that, with prescriptive cybersecurity regulations, they have to allocate resources to meet compliance requirements instead of actively defending their systems against sector-specific cyber threats.[32] Multiple respondents highlighted the role of the NIST Cybersecurity Framework in providing a starting point for directing their cybersecurity efforts.[33] Sentiment analysis of responses in this category also reflected the challenging regulatory environment, suggesting a higher degree of negative (69 percent) than positive (31 percent) sentiment related to cyber regulatory harmonization.

The inconsistent and duplicative requirements for cloud service providers (CSPs) was another dominant topic in this category.[34] CSPs have to comply with multiple regulations and certification schemes, such as FedRAMP, FedRAMP+, FISMA, and HIPAA, which often outline different timelines for data governance purposes and different levels of data privacy. A common suggestion that appeared through topic modeling was to direct regulators' efforts toward mapping differences in terminology and establishing streamlined guidelines for CSPs to follow.

One of the common themes that emerged from this category of responses was the cost of maintaining compliance across duplicative, inconsistent regulations put forth by different agencies.

Respondents noted the importance of upskilling the workforce to understand the dynamic cybersecurity threat landscape and support cyber resilience and security.[35] In particular, some respondents in this category highlighted the complexity of the cybersecurity threat landscape and mentioned using NIST resources and (ISC)2 certifications for upskilling the workforce.[36]

Responses from the consulting and cybersecurity categories were also aligned on having outcomes-focused, nonprescriptive frameworks, as opposed to a checklist approach, because of the costs and risks of trying to meet compliance requirements, which would be better allocated to preventing cybersecurity threats unique to the company.

Technology Companies

We categorized six organizations that responded to the RFI as technology companies. A significant portion of these companies advocated for harmonizing regulations at the state and federal levels. This preference was reinforced by the results of the sentiment analysis of this sector, in which 83 percent of the language in the responses expressed positivity around regulatory harmonization, and 17 percent conveyed negative sentiments.

Cybersecurity certification for cloud-based services (particularly FedRAMP) drew particular attention for this sector. FedRAMP is a standardized government-wide

32. Ibid.
33. See, e.g., "Comments of Cyber Florida," Docket No. ONCD-2023-0001-0064, Oct. 30, 2023. https://www.regulations.gov/comment/ONCD-2023-0001-0064; National Institute of Standards and Technology, "NIST Releases Version 2.0 of Landmark Cybersecurity Framework," U.S. Department of Commerce, Feb. 27, 2024. https://www.nist.gov/news-events/news/2024/02/nist-releases-version-20-landmark-cybersecurity-framework.
34. See, e.g., "Comments of ISC2 in Response to Request for Information on Cyber Regulatory Harmonization," Docket No. ONCD-2023-0001-0056, Oct. 30, 2023. https://www.regulations.gov/comment/ONCD-2023-0001-0056.
35. "Comments of Boston Consulting Group," Docket No. ONCD-2023-0001-0031. https://www.regulations.gov/comment/ONCD-2023-0001-0031; "Comments of ISC2 in Response to Request for Information on Cyber Regulatory Harmonization," Docket No. ONCD-2023-0001-0056. https://www.regulations.gov/comment/ONCD-2023-0001-0056.
36. See, e.g., "Comments of Cyber Florida." https://www.regulations.gov/comment/ONCD-2023-0001-0064; "ISC2 Cybersecurity Certifications," ISC2, last accessed May 20, 2024. https://www.isc2.org/certifications.

certification program for the adoption and use of cloud services by the federal government.[37] One company recommended reducing fragmentation between FedRAMP and state-specific initiatives, encouraging states to directly participate in regulations similar to FedRAMP.[38] Other companies echoed the need for improved coherence between state and federal regulations.[39]

Our analysis revealed a difference of opinion among technology companies regarding the baseline framework for harmonized regulations. Some companies asserted that federal frameworks should set the standard, whereas others suggested that state frameworks serve as the baseline.[40] The latter perspective comes from the idea that the state, local, tribal, and territorial (SLTT) requirements sometimes mandate lower assurance levels than federal standards. Adopting state-level frameworks as the baseline instead of federal-level standards could potentially keep compliance costs lower for SLTT vendors, as well as for smaller companies.

Topic modeling revealed several prevailing themes among the responses of this group, such as securing IoT systems through firmware management and certification processes; enhancing cloud security and FedRAMP compliance for public sector organizations; and aligning cybersecurity regulations with international cybersecurity standards.

Aggregate Findings

In our analyses, an overarching consensus emerged: Rather than a one-size-fits-all regulatory approach, organizations desire cybersecurity regulations tailored to the unique needs and challenges of specific sectors and developed through collaboration between sector authorities and governance bodies. Interestingly, this runs counter to ONCD's original intent of the RFI where "harmonization" is used to refer to "a common set of updated baseline regulatory requirements that would apply across sectors."[41]

RFI responses also reflected the fact that the cybersecurity regulatory landscape is overwhelming for the organizations that must comply with it—a reality that is exacerbated by the pace at which federal, state, and local entities are introducing new regulations.[42] Organizations reported struggling to keep up with new regulations, preferring that existing regulations be updated and frameworks be adaptable to allow them to spend less time mapping regulations and more time ensuring stronger cybersecurity practices.

Rather than a one-size-fits-all regulatory approach, organizations desire cybersecurity regulations tailored to the unique needs and challenges of specific sectors and developed through collaboration between sector authorities and governance bodies.

37. "How to become FedRAMP Authorized," FedRAMP, last accessed May 20, 2024. https://www.fedramp.gov.
38. "Comments of Amazon Web Services in Response to Request for Information on Cyber Regulatory Harmonization," Docket No. ONCD-2023-0001-0025, Oct. 31, 2023. https://www.regulations.gov/comment/ONCD-2023-0001-0025.
39. "Comments of Workday in Response to Request for Information on Cyber Regulatory Harmonization," Docket No. ONCD-2023-0001-0014, Oct. 29, 2023. https://www.regulations.gov/comment/ONCD-2023-0001-0014; Comments of Verizon in Response to Request for Information on Cyber Regulatory Harmonization," Docket No. ONCD-2023-0001-0051, Oct. 30, 2023. https://www.regulations.gov/comment/ONCD-2023-0001-0051.
40. "Comments of Verizon in Response to Request for Information on Cyber Regulatory Harmonization." https://www.regulations.gov/comment/ONCD-2023-0001-0051; "Comments of AWS," Docket No. ONCD-2023-0001-0025. https://www.regulations.gov/comment/ONCD-2023-0001-0025; "Comments of Workday," Docket No. ONCD-2023-0001-0014, Oct. 29, 2023. https://www.regulations.gov/comment/ONCD-2023-0001-0014.
41. "Request for Information on Cyber Regulatory Harmonization," Office of the National Cyber Director, Docket No. ONCD-2023-0001, last accessed May 20, 2024, pp. 2-3. https://www.whitehouse.gov/wp-content/uploads/2023/07/ONCD-Reg-Harm-RFI-Final-July-19.2023.pdf.
42. "U.S. Cybersecurity and Data Privacy Review and Outlook – 2024," Gibson Dunn, Jan. 29, 2024. https://www.gibsondunn.com/us-cybersecurity-and-data-privacy-outlook-and-review-2024; "Cybersecurity 2023 Legislation," National Conference of State Legislatures, Jan. 8, 2024. https://www.ncsl.org/technology-and-communication/cybersecurity-2023-legislation.

Our analysis also found that overly prescriptive or checklist-driven regulations can be costly for businesses to comply with and that these types of regulations divert resources from cybersecurity threats and technology gaps specific to their unique business needs. Instead, most organizations preferred descriptive regulations that establish general security requirements that allow organizations to fill in gaps as they exist within their unique cybersecurity postures.

Limitations

Although our study yielded many insights, it is important to acknowledge its limitations. Most notably, aggregating responses from a wide variety of entities and making observations or recommendations from them could overlook the nuance within individual responses. In addition, smaller organizations may have been less likely to have the time and resources needed to respond to the RFI, which could mean that their perspectives may not be represented fully in this dataset (although such companies could be represented by trade associations that submitted responses on behalf of an industry).

Different organizations also responded to the RFI questions in different ways: Some organizations answered the questions one by one, whereas others provided long-form text that offered more generalized insights on their challenges and issues. Although analyzing the data from these disparate response styles as a single dataset provided essential information at an aggregate level, this approach might have overlooked inherent differences conferred by response style.

Although ONCD's RFI described harmonization as "a common set of updated baseline regulatory requirements," our analysis found that most respondents desired sector-specific regulations.

Also of note, although ONCD's RFI described harmonization as "a common set of updated baseline regulatory requirements," our analysis found that most respondents desired sector-specific regulations. This disparity could mean that either respondents decided to frame "harmonization" according to their own understanding of the concept or that the aggregate dataset muted out potential responses that aligned with what ONCD desired.

There are also limits to using NLP techniques to analyze these issues. Sentiment analysis results, for example, reflect the proportion of text that is characterized as positive or negative and can help gauge the sentiment of a particular response, but the analytical technique itself has limitations in that the likelihood of disagreement between humans on any particular issue is high. Thus, we must be aware of this issue when generalizing these results as representing the overall sentiment toward harmonization, which may be influenced by more complex or mixed sentiments that sentiment analysis may not fully capture.

Finally, for this study, we chose to analyze and highlight the frequency with which words appeared in the RFI responses. This approach measures prominence of a term but may not accurately convey nuances of context, intent, or meaning of those terms.

Next Steps and Recommendations

The RFI responses provided insightful takeaways that ONCD, regulators, and Congress should consider when attempting to harmonize cybersecurity regulations. In particular, they highlighted the monumental challenge of cybersecurity regulatory harmonization and confirmed that most stakeholders believe that regulations should serve as one tool among many to bolster our nation's cybersecurity, rather than the sole solution. Below are five specific recommendations, drawn from our analyses, that the government and relevant stakeholders should consider when mapping out next steps for this process.

1. Harmonize definitions and intent.

Policy Recommendation 1

Our analysis revealed the potential for misunderstanding the meaning and intent of harmonization. Although all stakeholders can agree that cyber regulations are too numerous and duplicative, the federal government's end goal remained unclear until recent testimony and ONCD reporting.[43] To avoid having an ever-moving goalpost as the cyber threat landscape evolves, the government should clarify what foundational cybersecurity looks like and how baselines can be updated in a timely and effective manner. In the latest version of the National Cybersecurity Strategy Implementation Plan, the White House noted that Initiative 1.1.1 to "[e]stablish an initiative on cyber regulatory harmonization" was completed.[44] We note that while the goal of *establishing* an initiative is complete, areas for continued development still exist, including, to quote language from the Implementation Plan itself, "understand[ing] existing challenges with regulatory overlap and explor[ing] a framework for reciprocity for baseline requirements."[45] Given the number of unknowns about the challenges that still exist on this front and the yet unresolved need for coordinating, deconflicting, and harmonizing requirements, it is safe to say that that initiative is far from complete as of this writing.[46]

2. Conduct further analysis on data; inform future RFIs.

Policy Recommendation 2

The insights gleaned from this RFI's responses could be used to create more targeted RFIs to elaborate on key areas of interest. In addition, other NLP techniques could be applied to the existing data to provide new insights or confirm the observations noted in this analysis. It would also be possible to refine the existing data of this analysis by breaking it down by different demographic or organizational factors, such as industry sector, company size, geographic location, and respondent role, which could reveal new insights. Another consideration for

43. Testimony of Nick Leiserson, Senate Committee on Homeland Security and Governmental Affairs, "Streamlining the Federal Cybersecurity Regulatory Process: The Path to Harmonization," 118th Congress, June 2024. https://www.hsgac.senate.gov/wp-content/uploads/Testimony-Leiserson-2024-06-05.pdf; "Summary of the 2023 Cybersecurity Regulatory Harmonization Request for Information," Office of the National Cyber Director, June 2024. https://www.whitehouse.gov/wp-content/uploads/2024/06/Cybersecurity-Regulatory-Harmonization-RFI-Summary-ONCD.pdf.
44. "National Cybersecurity Strategy Implementation Plan, Version 2," The White House, May 2024. https://www.whitehouse.gov/wp-content/uploads/2024/05/NCSIP-Version-2-FINAL-May-2024.pdf.
45. "National Cybersecurity Strategy Implementation Plan," The White House, July 2023, p. 12. https://www.whitehouse.gov/wp-content/uploads/2023/07/National-Cybersecurity-Strategy-Implementation-Plan-WH.gov_.pdf.
46. Christian Vasquez, "White House grapples with harmonizing thicket of cybersecurity rules," Cyberscoop, Sept. 18, 2023. https://cyberscoop.com/cybersecurity-strategy-harmonization-critical-infrastructure.

further refining the data would be to choose a common topic (e.g., "FedRAMP" or "frameworks") and find the discrete references to that topic in the dataset and compare those responses. This method would exclude nonrelevant responses and allow for a closer comparison of similar responses. Finally, ONCD could highlight shared points made across most or all of the responses and assess how they may fit with or be adapted to existing cybersecurity regulatory frameworks.

3. Provide outreach to smaller entities.

Policy Recommendation 3

As noted in the limitations section, there are likely a tranche of organizations that face similar challenges with regulations and audits but do not have the resources to convey their experiences to government and regulatory entities. The government should consider how they can account for and accommodate these perspectives in their analysis of RFI responses. Ideally, harmonized cyber regulations should lessen compliance and reporting burdens—one of the most widely reported concerns in the responses. This will be especially important for smaller organizations with limited budgets and bandwidth.

4. Engage with stakeholders to align priorities and expectations.

Policy Recommendation 4

Cyber regulatory harmonization will require buy-in from additional entities. ONCD and other agencies involved should share findings from this (or their own) analysis with relevant stakeholders, such as fellow policymakers in Congress, regulatory bodies, industry professionals, and cybersecurity experts to determine the next steps toward regulatory harmonization. This could also include discussions of aligning expectations for regulatory reform among regulators, as well as between regulators and organizations who have to report to them. For example, these discussions could reconsider whether there is industry- and government-wide consensus on a desired regulatory model. Having a single baseline federal regulation with reciprocity frameworks and additional sector-specific regulatory requirements is one model under active consideration. In the interim, it may be worthwhile to institute a pause or extended consideration on the introduction of additional or new cybersecurity regulations.

5. Streamline regulatory coordination and reporting.

Policy Recommendation 5

We are unsure which entity is ultimately responsible for harmonizing existing regulations; whether they are formulating a baseline or sector-specific approaches; whether the entity would use existing or establish new authorities; and how much deference would be paid to state, local, and other authorities. Regardless of whether the federal government adopts a baseline or sector-specific cybersecurity regulatory framework, a coordinating body is needed to harmonize across agencies, regulators, state/local governments, and the organizations subject to those regulations. ONCD, CISA, and other contributing entities' have existing efforts and commitments to harmonize cyber incident reporting requirements and other cyber regulations, but designating a federal entity to coordinate regulations across

regulators and agencies may be an option to consider.[47] Other areas of engagement on this issue, such as Congress monitoring harmonization efforts or authorizing an agency to harmonize regulations could also be considered.

Conclusion

When contemplating cybersecurity regulation and regulatory harmonization, especially against the backdrop of a dynamic field with ever-evolving cyber threats, regulations that facilitate cybersecurity risk mitigation and improve cybersecurity resiliency should be prioritized, streamlined, and harmonized. In addition, the process of regulatory harmonization should be transparent, consistently incorporate stakeholder input, and avoid government overreach. If the federal government introduces new regulations, it should consider the broader context of how those regulations would fit into harmonization efforts and align with discourse on establishing cybersecurity baselines. Nonregulatory solutions, such as best practices and sector-based guidance, are also useful supplemental tools to improve our nation's cybersecurity baseline.

We are encouraged by ONCD and the broader federal government's efforts in attempting to make cybersecurity more straightforward. The next steps toward regulatory harmonization have the potential to materially and consistently improve our nation's cyber resilience and free up resources for other priority areas in cybersecurity.

We are encouraged by ONCD and the broader federal government's efforts in attempting to make cybersecurity more straightforward.

About the Authors

Amy Chang is a resident senior fellow at R Street Institute, where she integrates her academic, government, and practitioner experiences to lead research on cybersecurity, artificial intelligence, and national security issues.

Mumtaz Fatima is an undergraduate at Mt. Holyoke College; she was a policy fellow with the R Street Institute in Spring 2024.

Haiman Wong is a resident fellow at R Street Institute, where her research focuses on the connection between cybersecurity and emerging technologies.

47. "National Security Memorandum on Critical Infrastructure Security and Resilience," Cybersecurity & Infrastructure Security Agency, last accessed May 20, 2024. https://www.cisa.gov/national-security-memorandum-critical-infrastructure-security-and-resilience; "Request for Information: Cyber Regulatory Harmonization." https://www.regulations.gov/document/ONCD-2023-0001-0001/comment; 89 FR 23644 (April 4, 2024).