Summary of the 2023 Cybersecurity Regulatory Harmonization Request for Information

OFFICE OF THE NATIONAL CYBER DIRECTOR

JUNE 2024

THE WHITE HOUSE
WASHINGTON

Table of Contents

Executive Summary

Background

To achieve better cybersecurity outcomes while lowering costs to businesses and their customers, the Office of the National Cyber Director (ONCD) is working with colleagues across the interagency, and in close collaboration with industry and other key stakeholders, to lay the groundwork for a comprehensive policy framework for regulatory harmonization. The aim is to (1) strengthen cybersecurity readiness and resilience across all sectors; (2) simplify oversight and regulatory responsibilities of cyber regulators while enabling them to focus on areas of unique, sector-specific expertise; and (3) substantially reduce the administrative burden and cost on regulated entities.

Pursuant to the National Cybersecurity Strategy Implementation Plan Version 1, ONCD began to explore a framework for reciprocity for baseline requirements with interagency partners who participate in the Cybersecurity Forum for Independent and Executive Branch Regulators. On August 16, 2023, ONCD posted a request for information (RFI) to gather input from industry, civil society, academia, and other Government partners about its approach. This RFI, which can be found in Appendix B, sought public feedback on existing challenges with regulatory overlap and to explore a framework for reciprocity of baseline requirements. 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. This report provides an overview of their responses and the key findings.

Building on the findings from the RFI, ONCD has begun to explore a pilot reciprocity framework to be used in a critical infrastructure subsector. This pilot program effort is capture in the National Cybersecurity Strategy Implementation Plan Version 2, in initiative 1.1.5. The purpose of this pilot, which projects to complete next year, is to surface insights on how to achieve reciprocity when designing a cybersecurity regulatory approach from the ground up. ONCD will use findings from the pilot as well as the responses to the RFI to continue to lay the foundation for more comprehensive efforts to knit together dozens of regulatory regimes.

Analysis & Key Findings

There are three key findings from the responses:

- **The lack of harmonization and reciprocity harms cybersecurity outcomes while increasing compliance costs through additional administrative burdens**. Many respondents noted that compliance spending drew resources from cybersecurity programs.
- **Challenges with cybersecurity regulatory harmonization and reciprocity extend to businesses of all sectors and sizes and that they cross jurisdictional boundaries.** Respondents highlighted inconsistent or duplicative requirements across international and state regulatory regimes.
- **The U.S. Government is positioned to act to address these challenges**. Respondents provided numerous suggestions for how the Administration and Congress could act to increased harmonization and reciprocity.

Respondents 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, representing every sector, noted: "Duplicative, conflicting, or unnecessary regulations require companies to devote more resources to fulfilling technical compliance requirements without improving cybersecurity outcomes." 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, commented: "Inconsistencies also pose barriers to entry, especially for small and mid-sized businesses that often have limited resources available to establish multiple compliance schemes."

Further concerns detailed not only about a lack of harmonization and reciprocity across Federal agencies, but also between state and Federal regulators and across international borders. Many commented on 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 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 several overarching themes, including:

- Regulators should continue to focus on aligning to risk management approaches like the National Institute for Standards and Technology (NIST) Cybersecurity Framework (CSF).
- Coordinating among regulators to decrease overlapping requirements and collaborating with key allies and regional organizations (e.g., the United Kingdom, European Union, Canada, and Australia) to drive international reciprocity would materially improve the status quo.

- 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.
- Providing Federal leadership would help achieve these goals and guide state, local, Tribal, and territorial (SLTT) Governments to streamline related regulations.

Several respondents also provided specific recommendations for action to further harmonize cybersecurity regulations. Many highlighted ways the White House, or interagency bodies such as the Cyber Incident Reporting Council, could continue to drive progress toward harmonization and reciprocity.

Some respondents also recommended the Administration work with Congress on ways to improve harmonization. The U. S. Chamber of Commerce, the National Electrical Manufacturers Association, and CTIA – The Wireless Association all suggested that Congress consider legislation to set national, high-level standards for cybersecurity. The Chamber of Commerce also suggested that Congress consider ways to include independent regulators in future planning efforts on regulatory harmonization.

How to Read This Report

ONCD received over 2,000 pages of comments in response to the RFI, all of which are posted on Regulations.gov. This report summarizes key aspects of these comments to aid further discussions of cybersecurity regulatory harmonization and reciprocity.

The report is organized by respondent category. A full list of categories and the respondents therein can be found in Appendix A.

Each category section has a high-level summary of the respondents' comments, including representative quotes. The comments are then further analyzed across four dimensions: alignment, harmonization, reciprocity, and recommendations.

In this report, cybersecurity regulatory *harmonization* refers to the use of a common set of requirements associated with cybersecurity or information security controls. Harmonization is often subsequent to efforts to *align* requirements, by ensuring that, when regulatory agencies and regulated entities 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 information technology (IT) systems.

The RFI also focused on 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 regulator. 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 its own, independent assessment – as the necessary proof that the company was in compliance.

The summaries presented here do not represent ONCD's views on cybersecurity regulatory harmonization or reciprocity; however, they are important inputs for developing a comprehensive policy framework that mitigates cybersecurity risks. ONCD thanks all the respondents to the RFI for their thoughtful contributions.

Critical Infrastructure Sectors

Chemical

The American Chemistry Council (ACC), the sole respondent from the chemical sector, articulated strong support for an active Federal role in setting appropriate cybersecurity standards and harmonizing regulations.

Chemical sector operations are multinational in nature, involving a complex regulatory environment and compliance structure. ACC wrote that "redundant and conflicting regulations between jurisdictions or between agencies within a jurisdiction can increase costs, duplication, and inefficiency."[1] To address this issue, ACC advised that "approaches towards harmonization should include substantial consideration of existing industry efforts to manage cyber risks and the coordination of existing Government regulations and proposed regulations on the chemical sector."[2]

Alignment

ACC stressed the importance of leveraging internationally agreed upon technical standards to drive regulatory harmonization. ACC endorsed the use of the NIST CSF because it is "recognized nationally and internationally for its prioritized, flexible, and performance-based approach." The NIST CSF, ACC stated, provides guidance and best practices for cybersecurity in an automated environment and thus has been widely adopted by chemical sector organizations.[3]

Harmonization

ACC expressed concern about the current state of cybersecurity regulation, arguing that "the lack of harmonization . . . has led to a fragmented approach nationally and internationally." ACC asserted that "a fragmented landscape, with varying standards, requirements, and compliance frameworks across jurisdictions, is counterproductive to implementing risk-based approaches to cybersecurity." Consequently, organizations often end up "diverting resources from essential cyber risk management programs to potentially less effective compliance-driven activities."[4]

ACC added that an unharmonized regulatory environment "may also lead to regulatory gaps where emerging threats are not recognized in time or evolving technologies may be stifled."[5] Thus, ACC argued that cybersecurity regulatory harmonization is "a critical step in safeguarding businesses and critical infrastructure from both emerging cyber threats and any undue expansion of the cost of regulatory compliance."[6]

Recommendations

ACC recommended that the United States (U.S.) Government work with foreign governments "to embrace technical consensus standards and other technical measures to build confidence in foreign companies' cybersecurity and trustworthiness," and suggested that ONCD is particularly "well positioned to influence global Governments" on cybersecurity regulatory harmonization.[7]

ACC argued that sovereign localization requirements, "such as the mandatory siting of a headquarters or data center in a certain jurisdiction and/or compelling local employees to handle certain types of data, is counterproductive to harmonizing cyber regulations."[8]

Therefore, ACC "supports the White House taking an active role in harmonizing requirements for regulated sectors," particularly in "establishing policies and procedures for regulators to leverage consensus standards in writing new regulations in consultation with sector risk management agencies (especially [Cybersecurity and Infrastructure Security Agency] CISA) and the private sector."[9]

Communications

Four respondents – three trade associations and one corporation – submitted comments on behalf of the communications sector. Respondents described a disjointed regulatory environment that is inflexible and risks stifling innovation, with redundancy and inconsistency that increases compliance burden 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. Our nation's cyber readiness is not served by static rules across a multitude of jurisdictions that risk locking in place outdated practices and strategies, while also making it more difficult to deploy new, innovative solutions."[10] CTIA – The Wireless Association (CTIA) 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."[11]

Respondents voiced consensus on the importance of taking a risk-based approach to cybersecurity regulation that builds upon established frameworks that evolve with emerging threats and offer sector stakeholders more flexibility in implementation. CTIA wrote that "standards and frameworks are created by industry to address current or expected threats to communications networks and infrastructure," and therefore "can more readily adjust to the ever-changing cybersecurity landscape than regulatory mandates, which often tend to reflect the technology and threats at the time they are promulgated."[12] CTIA further explained that "because of the rapid pace of technological development, work on best practices and standards is continuously evolving and adapting to new threats contemporaneously to ensure that networks, infrastructure, and devices are protected. Government mandates, conversely, are often slow to respond to changes in the threat environment and/or can quickly become outdated."[13] Respondents cautioned against any regulations that "could encourage a 'check-the-box' compliance mindset instead of a dynamic and risk-based approach to cybersecurity."[14]

CTIA observed that when "companies are required to divert resources from their cybersecurity programs to "checking the box" for an array of divergent cybersecurity regulations and varying requirements across jurisdictions," it also has the effect of leaving "consumers with unclear expectations about company cybersecurity practices."[15] Instead, they promoted a tiered structure that allows "businesses to undertake their own risk and investment analyses based on each entity's unique considerations."[16]

Alignment

NCTA – The Internet & Television Association (NCTA) advised 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 to 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."[17] CTIA concurred, saying that attempts at regulatory harmonization must "recognize important sector differences that require a flexible process to reduce risks and respond quickly to emerging threats."[18]

To that end, every respondent cited the NIST CSF as a model framework for achieving risk-based performance outcomes and encouraged Federal agencies to use the CSF in their regulatory regime. CTIA championed the NIST CSF as "a particularly valuable tool for addressing and mitigating cybersecurity risk," noting that "flexibility and voluntariness are key to the NIST CSF's widespread adoption and longevity."[19] NCTA echoed this perception, saying that the CSF "has become the leading resource across all industry sectors because of its recognition that there is no "one size fits all" model for addressing cybersecurity risks and its emphasis on voluntary usage and flexible implementation. These characteristics allow companies to design and develop the best possible security solutions, and adapt them to the particular risk, network architecture, customer environment, and resources. Each of these elements is essential to the success of any cybersecurity program."[20] Noting that "the CSF is not sector-specific and thus can be applied across the economy, ensuring uniformity and continuity across all industries and sectors,"[21] Verizon argued that "the CSF is therefore an appropriate vehicle for a Government agency to use to ensure that an organization's cybersecurity practices are meaningful, without attempting to prescribe specific practices that may quickly become outdated and fail to optimize cybersecurity for a particular organization."[22]

Verizon observed that "a company's mere use of the CSF does not, on its own, ensure any specific level of cybersecurity maturity. Indeed, while some companies may use the CSF to drive sophisticated, comprehensive cybersecurity outcomes, others' use of the CSF may be nascent and minimalistic." Therefore, Verizon suggested that the Federal Government "explore ways to promote interagency collaboration to ensure minimum levels of CSF implementation by communications sector members."[23]

Recommendations

Respondents highlighted how overlapping and conflicting regulations are particularly challenging for a sector that transcends borders and operates across all levels of government. CTIA cautioned that cybersecurity is "a set of practices aimed at safeguarding the very channels of interstate commerce. Without adequate cybersecurity, an exploit or intrusion in one state can rapidly spread to other states, or can close off interstate commerce in particular sectors entirely." CTIA concluded that "a state-by-state patchwork is simply not a sensible way to regulate cybersecurity of companies with inherently interstate systems and operations. […] Moreover, given the role of state-sponsored cyber threats, the risks posed to cyber systems are increasingly international in character, and have a strong national security component." Therefore, CTIA urged Congress "to consider legislative enactments that would expressly preempt substantive

SLTT cybersecurity regulations," arguing that "the interest in promoting adequate cybersecurity is inherently Federal in nature."[24]

Critical Manufacturing

The two respondents from the critical manufacturing sector – the National Electrical Manufacturers Association (NEMA) and the Aerospace Industries Association (AIA) – highlighted the importance of cybersecurity regulatory harmonization, particularly for an industry that supports several other critical infrastructure sectors both domestically and internationally. AIA signaled the industry's commitment to cybersecurity and appealed for a regulatory regime more conscious of compliance burden, saying that "there is no desire to reduce cybersecurity measures but only to have simplification and harmonization to maximize performance and reduce waste through multiple audits and the need for adjusting systems for agency-specific requests."[25] NEMA argued that consensus-driven regulatory harmonization is necessary "so that security can be understood and effectively applied across systems, jurisdictions, and international borders."[26]

NEMA supported ONCD's initiative on cybersecurity regulatory harmonization, writing that a focused examination of the current regulatory environment "is necessary in order to identify systemic gaps; […] ideally, such an understanding will help lead to constructive, proactive, and more coordinated approaches to cybersecurity regulations."[27]

Alignment

Respondents recognized the growing need to establish minimum cybersecurity requirements for critical infrastructure in light of an ever-evolving threat environment. AIA wrote that "it is appropriate and necessary to implement regulations to ensure that a level playing field is established between all organizations and a minimum baseline security is implemented throughout."[28] NEMA noted that it "has long advocated for the need for the alignment of cybersecurity standards globally,"[29] and cautioned against modifying consensus standards or "the introduction of unfamiliar and misaligned definitions," contending that such an approach "creates difficult or impossible burdens on both the regulators, who must create a process for enforcement, and the regulated, who have to somehow comply with misaligned rules."[30] Instead, NEMA advised that "as cybersecurity becomes more of a priority for U.S. policymakers generally, they should first seek to raise security minimums to the level which these developed and recognized standards have already established."[31]

Furthermore, the sector is heavily reliant on both IT and operational technology (OT) systems, but the current regulatory regime does not effectively account for the differences between the two. AIA observed that "most frameworks available focus on traditional IT devices and adopting these standards for all applications presents issues. OT and IT have their own technical and environmental constraints that are addressed by IT standards. This limited applicability leads to inconsistencies on how security is implemented."[32]

AIA underscored the value of public-private collaboration in the regulatory process, saying that "an important factor in preventing conflicting or inconsistent regulation is ensuring that agencies are aware of other regulations in overlapping spaces, the existence of industry standards and

standards development activities, and most importantly ensuring that a dialogue is established with all stakeholders."[33]

However, AIA noted that the Federal Government has not engaged regularly with industry efforts to develop cybersecurity standards. AIA referenced the US Aviation Coordination of Cybersecurity & E-enabled Standards Strategy (US ACCESS) group, whose work is focused on "avoiding duplicate or redundant standards, generation of appropriate standards and identifying gaps in standardization for targeted closure."[34] AIA suggested that US ACCESS "has significant potential for fostering harmonization in standards and achieving recognition across the main aerospace stakeholders but as a new working group, more participation is needed – from the Government."[35]

Harmonization

Both respondents stressed that cross-sector harmonization efforts must be aligned with consensus standards while still allowing for requirements tailored to sector-specific risks. NEMA warned that "government action which is not harmonious with existing standards risks creating uneven and conflicting security postures which would be difficult to assess, manage, or audit. While a regulator may impose a rule in an effort to do good and bolster cybersecurity, the opposite might occur."[36] This is especially true if the harmonization process does not involve participation from all relevant regulatory bodies to identify and account for sector-specific regulations. AIA voiced concern that in such a scenario "non-sector-specific regulations issued by other regulatory bodies will not take into consideration industry-specific constraints and thus, have an adverse impact."[37]

AIA expressed skepticism about the current level of interagency coordination, saying "it is not believed that Federal agencies are coordinating cyber assessments or utilizing the same or similar constructs to perform assessments or accept assessments of other entities […] due to varying interests and expectations."[38] AIA wrote that "to allow a common tiered model to exist across regulated sectors, efforts must be made by regulators to ensure that the definition of terms across those tiers are consistent and agreed upon, otherwise significant variances will occur."[39]

Recommendations

NEMA wrote that "ONCD's effort to harmonize Federal reporting processes will be an ongoing, Sisyphean task in the absence of preemptive, national legislation which establishes common, high-level standards relating to cybersecurity."[40] To that end, NEMA "encourages Congress and the Administration […] to create a comprehensive legal framework which establishes an American cybersecurity regime rooted in internationally recognized consensus standards, promotes technological innovation, and firmly establishes a single government authority to oversee cybersecurity harmonization and implementation across the Federal Government and throughout the states."[41]

Defense Industrial Base

The two respondents in the Defense Industrial Base (DIB) Sector, the National Defense Industry Association (NDIA) and the National Defense Information Sharing and Analysis Center Policy, Standards and Regulations Working Group (ND-ISAC WG), expressed significant concern about

the current structure of cybersecurity regulations and voiced strong support for harmonization of such regulations and a more systematic approach to their development and implementation.

Both NDIA and the ND-ISAC WG discussed the lack of harmonized cybersecurity regulation and stressed the potential impact on both business and national security. NDIA wrote that 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. Inconsistencies also pose barriers to entry, especially for small and mid-sized businesses that often have limited resources available to establish multiple compliance schemes."[42]

The ND-ISAC WG added that the "prohibitive costs [of compliance] may drive a strategy of risk acceptance, which may lead to meaningful security gaps."[43] The ND-ISAC WG further warned that "no regulation today or pending directive allows for systems risk management based upon evolving ecosystem criticality." The complexity and pace of the Federal rulemaking process results in "cybersecurity requirements issued via contracts which remain relatively static over the contract period of performance," which "makes it challenging to integrate guidance tailored to new or emerging threats."[44]

Alignment

NDIA wrote that "industry is often subjected to multiple incongruent requirements across a multitude of cyber frameworks." In cases where a regulator has baseline requirements, NDIA observed that "they often add discretionary requirements on top of what is required or mandated," and "there is frequently little to no coordination on these unique requirements or reciprocal recognition of such requirements."[45]

The ND-ISAC WG advised that "if various Federal agencies and independent regulatory agencies continue to add new layers, frameworks, standards, and rules," then the U.S. Government "should assume a high rate of non-compliance and confusion, no matter the size of the contractor." The ND-ISAC WG noted that "the impact is particularly acute for small and medium businesses who may not have subject matter experts in contractual compliance."[46]

The ND-ISAC WG suggested the National Security Agency's (NSA) Top Ten Cybersecurity Mitigation Strategies should inform minimum cybersecurity requirements because they are based on the NIST CSF, which is widely used across multiple critical infrastructure sectors. Moreover, NSA's approach "allows for flexibility while maximizing the ability of a range of industries to combat the threat of Advanced Persistent Threat (APT) and Ransomware actors," and thus is "an excellent roadmap for small, mid-, and large companies with disparate environments."[47]

Harmonization

NDIA stated that current U.S. Government efforts "are creating a patchwork of cyber requirements depending on what sector your business belongs in or, in many cases, multiple cross-sector requirements for industries that support those sectors."[48] The ND-ISAC WG wrote that "as companies that span multiple U.S. critical infrastructure sectors and International environments (DIB, Commercial, Critical Manufacturing, Transportation, etc.) defense

contractors are often subjected to multiple incongruent cyber requirements across a multitude of varying cyber frameworks."[49]

For regulated entities with overseas operations, the plethora of competing policy and rulemaking processes is particularly problematic. The ND-ISAC WG added that beyond conflicting U.S. Federal issuances and requirements, member companies with international business operations (e.g., foreign military sales), must exercise extreme attention and care to maintain compliance between U.S. Federal requirements and other national schemas on the customer end, including the United Kingdom, Australia, and Saudi Arabia.[50] Furthermore, "foreign governments also frequently publish requirements that impact U.S. industry global operations and often without features in common with US Federal requirements."[51] NDIA remarked that "many industries also manage relationships in foreign countries which have their own cyber requirements and which include a variety of assessments based on differing cyber frameworks." As a result, NDIA warned, "unless the harmonization or equivalency to other cyber standards is developed, industry will continue to struggle to meet regulations and requirements."[52]

Both NDIA and the ND-ISAC WG opined on the value and feasibility of a common tiered model to achieve cross-sector regulatory harmonization, stating that "to allow a common tiered model to exist across regulated sectors, a significant amount of work needs to be done to ensure that the definition of terms across those tiers is consistent and agreed upon — otherwise, significant variances will occur."[53] This is particularly important when delineating between Cloud Service Providers (CSPs), Managed Service Providers (MSPs), and External Service Providers (ESPs). NDIA argued that "common terminology needs to be defined and followed across all agencies. This is an important clarification because in some arenas, MSPs are also considered CSPs. That is not always the case. Terminologies and definitions need to be harmonized across all agencies."[54]

The ND-ISAC WG also wrote that "to further ensure a whole of Government approach, new security requirements should be harmonized with the relevant Federal Acquisition Regulations (FAR) and Defense Federal Acquisition Regulations Supplement (DFARS) clauses to the maximum extent practicable. The on-going proliferation of new security requirements furthers the need for harmonization."[55]

Reciprocity

The ND-ISAC WG highlighted the importance of regulatory reciprocity given the global nature of the defense industry. Noting that "domestic and international reciprocity/equivalence is critical as IT and OT are the basis of the global ecosystem in operation today," the ND-ISAC WG argues that mutual recognition of regulatory compliance across global jurisdictions is essential for improving national security and economies of scale.[56]

Defense contractors engaging in foreign military sales "now contend with the awkward circumstance of allied countries' sovereign regulations and/or laws prohibiting compliance" with the DFARS requirements that U.S.-based companies must follow.[57] The ND-ISAC WG emphasized that "absent reciprocity agreements developed by the U.S. Department of Defense (DoD) with counterpart Ministries of Defense, U.S. defense companies are forced to independently negotiate their respective disclosures to comply with allied country regulations."[58] This problem is especially acute for legacy defense equipment because "without major product

redesign, there is currently no way for the United States to procure defense articles (and spares) […] that were designed to incorporate products manufactured from companies located in allied and partner countries when such allied countries sovereign regulations and/or laws prohibit compliance with the DFARS regulations."[59] Further, "without reciprocity/equivalence there is cost and duplication of efforts in terms of multiple/similar compliance, certification(s), and varied processes and procedures uniquely specified by regime."[60]

Recommendations

Both NDIA and the ND-ISAC WG wrote about the confusion regarding which Federal agency plays the role of primary regulator for the defense industrial base. NDIA wrote that "it is not clear to industry which agency in the Federal Government acts as the clearinghouse for cyber-related regulations and requirements. Multiple authorities are issuing guidance and requirements, often simultaneously and frequently overlapping in coverage."[61] The ND-ISAC WG added that "this appears to be an issue that lacks clarity both with DoD and among non-DoD Federal agencies."[62]

The NDIA recommended that "ONCD should work with Congress to determine the correct entity for controlling and managing the development and issuance of cyber and cyber-related guidance, standards, requirements, and regulations across the Federal Government. Without such governance, we will continue to have inconsistent, unharmonized requirements that only serve to create, sustain, or worsen vulnerabilities in Federal agencies and the Federal industrial base that supports those Government missions."[63]

NDIA also highlighted the importance of a stable and consistent regulatory environment to the ongoing business operations of the defense industrial base. NDIA recommended that "ONCD should work with the Executive Office of the President to codify many of the agreed-upon authorities established through Executive Order in order to prevent varying requirements from being changed with each new Administration. The Federal Government and the industrial base need consistent and identifiable authorities to manage, implement, and oversee the requirements that are necessary to protect the interests of the American people while providing industry and Government personnel alike a consistent and clear structure for compliance and risk management."[64]

Energy

Eight respondents across both the electricity and oil and natural gas sub-sectors provided perspectives on behalf of the energy sector, which is among the most highly regulated critical infrastructure sectors for both operational resilience and cybersecurity. Respondents described an extremely complex regulatory environment, with numerous regulators and frequent oversight activity at the Federal, state, and local levels. Exelon observed that "the information systems that support our nation's critical infrastructure are undergoing significant expansion and modernization to meet new societal goals and consumer needs. At the same time, these critical assets are subject to evolving and increasing threats. The tools and approaches critical infrastructure operators […] use to combat these threats must be advanced, not diminished, by regulation."[65]

The American Fuel & Petrochemical Manufacturers (AFPM), the American Gas Association (AGA), the American Petroleum Institute (API), and the Interstate Natural Gas Association of America (INGAA), in a joint submission (and hereafter referred to collectively as "the Associations"), wrote that for sector stakeholders, "the objective is to keep energy moving. Therefore, when developing and harmonizing cybersecurity regulations, the Federal Government should ensure that requirements are risk-informed and are crafted with the objective of protecting those elements critical to ensuring the safe delivery of energy services, protection of personal information, and other necessary functions that support the nation's economy and national security."[66]

The Edison Electric Institute (EEI) echoed the Associations' position, saying that "redundant regulations add to electric companies' already high operational costs and misdirect limited resources and personnel from electric companies' core obligation – namely, to provide safe, reliable, and affordable service to their customers. Fundamentally, it is this core obligation that is essential to national security."[67]

Respondents underscored the need for a flexible regulatory regime to enable risk-based cybersecurity strategies and investments in the energy sector. EEI stressed that "electric companies need flexibility to effectively protect the electric grid before, during, and after a cybersecurity incident," and emphasized that "as the Federal Government, states, and private sector continue to enhance cybersecurity protections of critical infrastructure, it is incredibly important that additional cybersecurity standards are developed holistically to ensure that they are not duplicative, overlapping, or inefficient – so as to not impede risk-reduction efforts."[68] The Associations agreed, saying that "to effectively achieve the end goal of robust cybersecurity for critical energy systems, there must be flexibility in the operator's ability to apply risk-informed controls to achieve certain cybersecurity requirements."[69] The Associations added that efforts to harmonize regulations should focus on "understanding the risk within each sector and the myriad of differing purposes for those regulations, be they for national security, safety, or consumer and investor protection."[70]

Respondents reported spending significant resources satisfying an ever-growing compliance burden and cautioned about the potential impact to the safe and reliable provision of energy to businesses and consumers. The American Public Power Association (APPA) and Large Public Power Association (LPPC), in a joint submission, noted that "grid security is and should be much more than a compliance exercise. Furthermore, as previous incidents across industries have shown, compliance does not always ensure security. Companies can comply with current regulations and still be vulnerable to attacks if security measures do not extend to their most critical assets."[71] APPA and LPPC highlighted the financial impact of regulatory compliance, noting that "the cost of electric service is a key factor in the nation's economic health, and the reality of varying, but finite resources and budgets suggests that over-spending on security measures may compromise grid reliability in other respects. This is especially important to consumer-owned, not-for-profit public power utilities."[72]

Alignment

Regulation of the energy sector involves myriad cybersecurity requirements that vary across regulators and activities, such as generation and distribution. The North American Transmission

Forum (NATF) said that "the complexity to achieve cybersecurity increases as disparate activities are required by various regulatory bodies, agencies, or security frameworks. These disparate activities are not necessarily conflicting, but nuances in application of the activity or in the wording of the requirement create unique requirements/actions to be addressed. Harmonization is needed to eliminate or, at a minimum, reduce the complexity to allow responders to focus on a common set of practices."[73] The Western Area Power Administration (WAPA) concurred, saying that "by aligning cybersecurity requirements, critical infrastructure entities can optimize resource allocation, focusing on effective cybersecurity measures while managing costs efficiently."[74]

Respondents recommended that regulators leverage proven frameworks like NIST CSF to shape requirements and incorporate flexibility into implementation. Exelon argued that "the key to continued effective protection of the nation's critical infrastructure is flexibility in the application of standards within a shared national security framework. While harmonization across the Federal landscape may facilitate regulatory implementation and compliance, this harmonization should not come at the expense of flexibility. Critical infrastructure operators must be allowed to select the most effective security approaches and evolve those approaches to meet changing threats."[75] Exelon suggested that regulators "focus on the 'what' — the overarching objectives and desired outcomes — rather than prescribing the exact 'how' to achieve security," and provide "regulatory guidance that outlines clear objectives, while granting the autonomy to critical infrastructure system operators to discern the best strategies and methodologies to reach those goals. This approach supports innovation and flexibility, allowing energy system operators to utilize their deep expertise to ensure effective and efficient compliance to protect our critical infrastructure."[76]

Several respondents discussed the value of the NIST CSF as a basis for regulatory requirements and adaptable risk management. Exelon noted that "while this framework wasn't specifically crafted for the energy sector, its foundational principles align remarkably well with our sector's needs. […] A universally adopted framework, like the CSF, could provide a more secure and objective standard for enhanced collaboration between critical infrastructure sectors and with the third-party vendors that support us."[77]

Harmonization

Respondents agreed that regulatory harmonization is imperative to improving the sector's cybersecurity. The Associations maintained that "the leading driver of the timely need for cybersecurity regulatory harmonization among Federal regulators is the circumvention of duplicative and conflicting requirements, which add an unnecessary administrative burden on the owner/operator and are a waste of scare Government resources." The Associations argued that "this is particularly pertinent given the increasing number of mutually exclusive and inconsistent Federal regulations impacting the oil and natural gas sector are often even within single Federal departments," such as the Department of Homeland Security and its components, the Transportation Security Administration (TSA), CISA, and the United States Coast Guard, all have some degree of jurisdiction over the oil and natural gas supply chains. The Associations clarified that "while not necessarily conflicting, especially at the Federal level, these regulations are certainly duplicative, burdensome from a compliance perspective, and are inconsistently enforced."[78]

The Associations asserted that "the more the Federal Government is able to consistently develop and apply regulations, the more operators will be able to understand and implement those requirements, definitions, and objectives, which will allow them to focus more effectively on addressing cyber threats and mitigations."[79] On the other hand, the North American Electric Reliability Corporation (NERC) warned that "duplicating requirements without incorporating efficiencies in demonstrating compliance could divert resources from maintaining security to simply managing the increased compliance workload."[80] NATF elaborated further, saying the "lack of harmonization across regulatory agencies' requirements, as well as across various security frameworks, also creates the need for unique responses to be developed for each information request. This creates resource burdens, detracting from time that could be better spent on cybersecurity." NATF contended that harmonization would "enable companies to develop responses to information requests that are applicable across agencies, thereby being able to demonstrate compliance with regulations or good cybersecurity practices without diverting resources from cybersecurity efforts."[81]

Reciprocity

Respondents observed that the current regulatory regime does not enable reciprocity due to the lack of unified requirements across regulators and the routine exercise of regulatory discretion. WAPA reported that "there is no reciprocity […] in regulator acceptance of other regulators' recognition with baseline requirements. […] NERC does not recognize other standards and will not accept another standard, even if more demanding, as compliant with or equivalent to" its own.[82] The Southwestern Power Administration (Southwestern) agreed, adding that "where regulatory reciprocity might or could occur, it is voluntary and usually at the discretion of the current auditor. Entities have no authority in leveraging results of monitoring under other frameworks."[83] The Associations made a similar observation, saying that "barriers to regulatory reciprocity are primarily due to the silos in which agencies exist. Each agency sees its mission as unique and independent from others."[84]

The Associations advocated for reciprocity based upon proven performance outcomes. They proposed that "to the extent an oil or natural gas operator is already implementing a preexisting regulatory framework, that should be considered and deemed to satisfy similar requirements in another regulatory program if the same mandated risk reduction outcomes are achieved. In so doing, new requirements would neither compete nor conflict with existing requirements, while constructively introducing regulatory oversight as appropriate."[85] The Associations went on to say that "if proactive efforts cannot be made to harmonize or rectify the disparate requirements placed upon owners/operators when developing cybersecurity regulatory requirements, agencies would be well served to take action to retroactively ensure that regulatory requirements applicable to entities regulated by multiple agencies are harmonized in a reciprocating manner. Doing so would reduce the regulatory burden on industry owners and operators and would allow the Federal agencies administering these requirements to streamline their efforts."[86]

Recommendations

Respondents voiced concern over supply chain risk management and the lack of regulation to validate that energy sector suppliers meet minimum cybersecurity requirements. EEI said that its members "must rely on third-party equipment manufacturers and vendors that are not subject to

the same cybersecurity regulation or requirements as electric companies, and electric companies have very little market influence to encourage these third parties to adopt security improvements. […] Accordingly, regulatory frameworks that seek to add requirements without appreciating the operational realities and limitations that EEI members face only exacerbate these challenges."[87] Moreover, according to APPA and LPPC, "electric utilities do not regularly have access to information from the manufacturer of a finished product about who may have sub-contracted the design and/or manufacturing of the components. The vendors and manufacturers hold this information, including the extent to which a foreign entity may play a role in their supply chain."[88]

Therefore, APPA and LPPC encouraged ONCD and the U.S. Department of Energy (DOE) to "work directly with equipment manufacturers and vendors to identify areas of concern."[89] Exelon suggested that ONCD consider "establishing more robust security frameworks for the third-party vendors integral to the critical infrastructure sector," saying that "clear security guidelines for these suppliers will bolster the security and reliability of the entire energy ecosystem in addition to providing objective standards for vendors providing service to the critical infrastructure sector."[90]

Financial Services

Financial services sector respondents broadly supported the need for enhanced cybersecurity regulation to protect critical infrastructure, but also voiced significant concern about the current regulatory environment, citing a lack of alignment among regulatory agencies at the international, Federal, and state level. As regulators have revised their rules and examinations with a stronger focus on cybersecurity risk, regulated entities report a growing compliance burden. The Financial Services Sector Coordinating Council (FSSCC) explained that "the increasing frequency and depth of U.S. and international regulatory exams requires financial firms to divert significant resources to respond to exam requests."[91] Marsh McLennan agreed, noting that "duplicative regulation diverts resources to additional audits and leads industry to focus on compliance more than security. By some estimates, large, multinational companies that are subject to many sources of regulation may spend up to 40% of their cybersecurity budget submitting regulatory compliance reports."[92]

For firms that have been designated as "systemically important," the closer scrutiny has led to them employing large numbers of staff exclusively dedicated to exam preparation and remediation, rather than risk mitigation efforts. The FSSCC went on to say that "based on recent feedback from Chief Information Security Officers and other senior cyber leaders within firms, many report spending 30 percent to upwards of 50 percent of their time on regulatory compliance. This challenge is even more pronounced for smaller and midsized firms that often do not have the same level of resources to dedicate towards exam management."[93]

The Mortgage Bankers Association (MBA) wrote that "compliance and technology officers must navigate a web of Federal and state laws and regulations to ensure compliance. This regime creates unnecessary costs to companies attempting to address shared concerns of consumer protection and can detour resources that should be focused on executing to a single Federal regime."[94] The MBA added that in the current construct, "data security requirements are

effectively set by whichever state creates the most stringent data security rules. This dynamic becomes untenable when conflicts between laws do arise. If data security laws conflict, firms could be forced to maintain separate information security compliance programs based on each regulation. This would add a considerable amount of time to monitor and make it difficult for companies to demonstrate compliance."[95]

The growing number of state cybersecurity regulations is particularly challenging for the insurance industry, as insurance is regulated exclusively by states. The Insurance Coalition said that "the patchwork of state Cybersecurity Rules can pose distinct challenges […and] the pace of new state Cybersecurity Rules is only accelerating. According to the National Conference of Legislatures, at least 25 states enacted 43 new cybersecurity laws in 2022, out of 250 bills proposed by at least 40 state legislatures."[96] Consequently, "this potentially conflicting maze creates avoidable compliance costs and uncertainties that directly impact the ability to serve policy holders as effectively, efficiently, and safely as possible."[97]

Alignment

Respondents generally agreed that setting national baseline cybersecurity requirements would be beneficial for the sector. The Bank Policy Institute (BPI) and the American Bankers Association (ABA), in a joint submission, suggested that "by leveraging established frameworks, regulated entities can prioritize resources and make well-informed security investments. Common standards also allow regulators to tailor examinations and generate comparable responses across regulated entities."[98]

Marsh McLennan wrote that common guidelines, such as those issued by the Federal Financial Institutions Examination Council, are "extremely effective and improve collective action/collective security because of the common interpretations, flexibility, and understanding they provide. A common assessment tool is beneficial for regulatory harmonization because it creates a common denominator and allows organizations to focus on what is most important to them. It also allows for prioritization and better understanding across those organizations where the standards exist."[99]

Common cybersecurity requirements can also improve communication and drive uniform implementation. Marsh McLennan argued that "another net benefit is that different organizations can understand the regulations/standards in the same way and through a common language. This improves collective security more than simply anticipating that different organizations are going to read and interpret a regulation and then apply the standards in the same way."[100]
Such a regime is particularly impactful at the state and local level given the potential to deconflict regulations and streamline compliance, especially for small and medium-sized institutions. The Insurance Coalition advocated for standardized rules, urging the ONCD "to consider, among other things, establishing: clear hierarchies that make the order of precedence clear between conflicting or potentially conflicting Cybersecurity Rules […and] unambiguous and consistent definitions that align to other applicable Cybersecurity Rules."[101] The Credit Union National Association (CUNA) proposed that "a single cybersecurity standard, reporting requirement, and examination for credit unions would streamline credit unions' the allocation of resources to cybersecurity initiatives in an efficient manner that appropriately responds to a single compliance regime."[102]

The financial services sector provides an instructive example of building a risk management framework upon a commonly accepted and understood baseline. BPI and ABA noted that "financial institutions, like many other sectors, have long leveraged the NIST CSF to inform and prioritize cyber risk management."[103] CUNA highlighted the role that the NIST CSF played in the creation of the Cyber Risk Institute (CRI) Profile, which maps sector-specific regulations to the NIST CSF and provides regulators with proof of a firm's cyber risk management program. CUNA noted that the CRI Profile, "by using a common risk framework developed in partnership between Government and industry, and also incorporating via reference international technology standards to describe risk controls, firms and regulators are better able to understand and communicate risk across the sector."[104] Furthermore, use of the Profile "enables firms of all sizes to efficiently assess and manage their cyber programs, freeing up limited cyber staff to focus on emerging technology like generative Artificial Intelligence."[105]

Harmonization

Respondents emphasized the need for regulatory harmonization to mitigate cybersecurity risk not just within the financial services sector, but across all critical infrastructure due to growing interdependencies between and among sectors. BPI and ABA stated that they "support the National Cybersecurity Strategy's focus on improving baseline security practices across industry sectors" and noted that "cybersecurity, if not carefully calibrated and aligned across Government and independent regulators, can have unintended adverse effects."[106] The FSSCC suggested that "establishing higher standards across critical infrastructure and other non-regulated entities such as third-party service providers will make the assessment of those organizations less burdensome for financial firms while improving the overall security environment."[107]

Several respondents advocated for Federal action to advance regulatory harmonization. Marsh McLennan recommended that "the Federal Government should engage with state and international regulators to limit the impact of overlapping requirements, including, where it makes sense, the use of Federal pre-emption."[108] The MBA concurred, saying "the industry supports one set of Federal rules that preempts state law and preserves flexibility for companies to address a myriad of concerns,"[109] and argued that "a single regime strengthens execution and is in the best interest of consumers and financial services providers alike."[110]

Reciprocity

Respondents largely supported the concept of reciprocity but could cite few examples in the current regulatory environment. BPI and ABA wrote that "regulatory reciprocity remains an end goal worth pursuing," proposing that "a holistic reciprocity framework with streamlined oversight requirements would relieve regulated entities from demonstrating compliance with the same or substantially similar requirements to multiple regulators."[111] BPI and ABA suggested that "successfully integrating a reciprocity model would provide regulators with the information they need to conduct rigorous oversight, but also streamline compliance burden so regulated entities can devote more time to day-to-day security activities and strategic resiliency improvements."[112]

Reciprocity is particularly important given how financial institutions operate in multiple jurisdictions and regularly interact with third party service providers. BPI and ABA wrote that

"for financial institutions with multiple overlapping regulatory requirements or service providers with customers in multiple sectors, a regulatory reciprocity model with uniform and streamlined standards for cybersecurity oversight is increasingly necessary to keep pace with dynamic cyber threats. Such an approach would promote more effective resource allocation – both for firms and regulatory agencies – while encouraging ongoing security improvements without overburdening cyber professionals and diverting attention from broader enterprise-wide risk management.[113] This is especially important at the state level, with Marsh McLennan observing that there is "no clear reciprocity" between Federal and state regulatory agencies for "accepting each other's cybersecurity requirements and/or assessments," adding that they are "encouraged by current Federal efforts to coordinate with other levels of Government that touch these various sectors."[114]

Finally, BPI and ABA also asserted that "all sectors would benefit from an increased reliance on a clearly defined primary regulator. […] A reciprocity model constructed [with a primary regulator] would be more efficient and alleviate the need for regulated entities to demonstrate compliance with the same requirements to multiple Government agencies." BPI and ABA acknowledged that "there would still need to be some mechanism for involving secondary regulators who previously conducted their own independent reviews," and therefore, "regulators could form joint oversight teams, led by the primary, allowing each agency to participate in the compliance process simultaneously."[115]

Government Services and Facilities

The sole response from the government services and facilities sector was submitted by the Chief Cyber Officer of New York State and broadly articulated the need for improved partnership and collaboration between state and Federal agencies with respect to cybersecurity regulations. New York State noted that "states play a critical role in cybersecurity oversight through regulations tailored to local risks. But better partnerships between Federal and state regulators can enhance protections while reducing compliance inefficiencies."[116] New York State proposed that Federal agencies could drive harmonization by helping states better align their regulatory regimes with Federal standards, and in areas where there is no Federal jurisdiction, by providing technical assistance and implementation guidance to state regulatory bodies.

Alignment

The Chief Cyber Officer of New York State wrote that the NIST CSF "underpins a substantial share of state-level regulation and is seen as an effective way to increase the commonality between state and Federal-level regulation."[117] The New York State Department of Financial Services (NYDFS), which works closely with the Federal financial regulatory community, is an instructive example for other states on leveraging NIST CSF to develop regulations. To this end, New York State argued that "Federal entities promoting wider adoption of proven guidelines like the CSF through policy statements, rulemaking, or technical guidance could greatly assist harmonization efforts."[118]

New York State also advocated for Federal assistance in conducting supervisory activities, saying that "states would benefit from support in training examiners on uniformly interpreting and applying common frameworks in regulations."[119] Additionally, the Federal Government

"could coordinate a public-private sector process, similar to what NIST did to develop the CSF, to identify and promote standardized assessment methods and tools for use by regulators and regulated entities alike."[120] Efforts like these to standardize assessments across Federal and state jurisdictions could help both regulatory agencies and their regulated entities better measure compliance while streamlining oversight.

Harmonization

New York State acknowledged the importance of the Federal Government in cyber regulation, particularly in facilitating coordination and information sharing on best practices, resources, and opportunities for mutual recognition to advance reciprocity. New York State suggested that "one way to better harmonize requirements would be for Federal regulators to provide guidance to states on how new cyber regulations could align with Federal baselines or frameworks."[121] This support "could help states continue to align on baseline standards while still addressing unique sector-specific risks in their respective jurisdictions,"[122] and also would afford states the chance to communicate with the Federal Government areas where states "may best substitute for national-level regulatory action."[123] Such an arrangement enables states "to respond rapidly to address emerging threats and where needed impose stricter standards tailored to their jurisdictions."[124]

Recommendations

New York State highlighted the financial services and energy sectors as examples where unique operational risks and jurisdictional limitations make Federal and state coordination especially critical. Financial institutions are chartered at the national and state level, depending on the services they provide. In 2017, NYDFS "promulgated a regulation establishing cybersecurity requirements for financial services companies. In a notable instance of state-level legislation leading national legislation, the NYDFS regulation established a regulatory model that is now used by both Federal and state financial regulators."[125]

Similarly, cybersecurity for the energy sector is regulated based on activity, with states generally exercising authority over distribution systems and the Federal Government having jurisdiction for generation and transmission.[126] In 2023, New York State enacted legislation to impose mandatory cybersecurity requirements on energy distributors, alongside regulations from the New York State Department of Public Service. These rules "demonstrate proactive oversight in the face of Federal jurisdictional limits; […] however, the complex jurisdictional and energy grid boundaries also underscore the need for continued Federal action to secure the entire energy ecosystem."[127]

To this end, New York State advocated for robust Federal-state interaction to mitigate cross-sector risk, arguing that a "more concerted effort to align or otherwise coordinate Federal plans for prospective regulations across different sectors with state plans for prospective regulations could continue to address any potential duplication in some areas and gaps in others."[128]

★ ★ ★ ★ ★ ★

Healthcare and Public Health

Respondents in the Healthcare and Public Health sector expressed concern about the current patchwork of cyber regulations and the need for minimum cybersecurity requirements across the sector as it faces a significant increase in malicious cyber activity. Cooperative Exchange wrote that the "industry is significantly impacted by the complex, fragmented, inconsistent, redundant, and sometimes conflicting security regulations. The lack of regulatory harmonization prevents interoperability, resulting in increased costs and inefficiencies as limited resources are diverted to address compliance challenges instead of focusing on security prioritization to protect our nation's critical cybersecurity infrastructure."[129]

HITRUST welcomed efforts on regulatory harmonization and endorsed a cross-sector approach with "a focus on reciprocity and accountability not only across existing regulations supporting different industries but with private sector assurance systems that can provably and transparently deliver high-quality and reliable outcomes."[130] HITRUST argued that "such a partnership and approach will improve cybersecurity for our nation through the uptake of public standards across multiple industries, leverage of existing private sector investments to harmonize and unify those standards, and the acceptance of constantly updated, reliable, and transparent assurance mechanisms that guide and demonstrate effective cybersecurity."[131]

Alignment

Several respondents agreed on the importance of setting minimum cybersecurity requirements. The College of Healthcare Information Management Executives (CHIME) and Association for Executives in Healthcare Information Security (AEHIS), in a joint submission, stated, "We are encouraged that the administration plans to take a collaborative approach between industry and regulators, and agree that setting minimum cybersecurity requirements is important and indeed is a shared responsibility."[132] Cooperative Exchange suggested "healthcare regulatory agencies in partnership with industry should establish the requirements for a common set of requirements upon which a conformity assessment program would be built."[133] Kaiser Permanente recommended that "government agencies and regulators work together to create a common control set as recommended guidance for regulated entities in specific sectors to utilize based on their statutory and regulatory requirements," while also allowing for some flexibility and innovation.[134]

Respondents consistently referenced the NIST CSF as an appropriate model for baseline standards. CHIME and AEHIS noted they are "strong supporters of the NIST CSF" and highlighted that their members "rely on the CSF to help guide their cybersecurity practices and leverage it as a foundation for improving their overall cyber posture." They contended that "due to the risk-based and business-operations approach of the CSF […] it is much more easily grasped and used by non-IT and non-security executives. This drives more engagement, participation, and interest in security than those frameworks which are more technically focused and controls based."[135]

Cooperative Exchange also recommended Federal agencies and regulatory bodies leverage NIST CSF for cybersecurity requirements, requesting changes from NIST if needed.[136] HITRUST argued that regulators "could effectively mandate the 'core' good hygiene/best practice control

baseline and the risk-based tailoring requirement while allowing the use of voluntary frameworks such as the NIST CSF […] to tailor the baseline as needed."[137] Similarly, Kaiser Permanente responded that "rather than creating a new model, we recommend supporting frameworks that already exist and are widely utilized, such as the NIST CSF."[138]

Harmonization

Respondents broadly endorsed the concept of harmonization but also articulated the need for a certain amount of flexibility to account for differences among critical infrastructure sectors. The Medical Imaging and Technology Alliance (MITA) voiced support for more robust cybersecurity efforts to secure critical infrastructure but emphasized that "harmonization should strive to integrate seamlessly with existing regulatory requirements" and "avoid creating duplicative or conflicting requirements with existing regulatory expectations."[139] MITA argued that redundant regulations increase compliance burden and costs for regulated entities, and "this issue would be compounded if requirements deemed appropriate for some industries were applied to all industries without careful assessment."[140] Therefore, MITA advised that regulators "ensure any foundational cybersecurity regulatory framework truly reflects a baseline risk profile shared by each industry it supports, without unnecessarily restricting an organization's ability to develop solutions tailored to their unique industry needs.[141]

Kaiser Permanente noted that it is "critically important to promote additional and sustained collaboration, coordination and communication among regulating entities to reduce redundancies, confusion, and operational complexities."[142] Kaiser Permanente observed that in the healthcare and public health sector, "current cybersecurity requirements are generally aligned with existing standards and frameworks," but suggested that "to promote further harmonization, […] regulators map regulatory requirements to appropriate cybersecurity guidance and requirements."[143] To mitigate cross-sector risk, Kaiser Permanente recommended "utilizing a risk-tiered approach that establishes a minimum baseline of cybersecurity control requirements applicable to all 16 critical infrastructure sectors with increasing controls commensurate with the risk level."[144]

Reciprocity

Respondents generally supported the concept of reciprocity but noted challenges with the current regulatory environment and compliance regime. HITRUST argued that "formal reciprocity with such reliable third-party approaches to assurance (i.e., assessment, certification, and reporting)" can provide "more robust assurances that demonstrate the outcomes required for our nation."[145] However, Cooperative Exchange noted that "third-party audit certification vendors are primarily private entities, over which no regulatory certification requirements exist nor do they provide customer indemnification provisions."[146] Furthermore, many Federal and state regulatory entities issue regulations and requirements yet "no Government programs either recognize the validity of many private audits and certifications that clearinghouses undergo or offer guidance to oversee the quality of these audits and certifications."[147]

Cooperative Exchange therefore proposed "that there be a comprehensive security control framework designed for clearinghouses and approved by the Federal Government. This framework should be implementable for all states and include all major Federal regulation

controls and standards as applicable and promoting use across the industry. This would save time, effort, and cost for an organization, while avoiding multiple audits of a similar type."[148]

Additionally, Cooperative Exchange highlighted a recommendation from the Healthcare Sector Coordinating Council that calls for the creation of a "conformity assessment model for evaluating cybersecurity hygiene that regulatory agencies and industry could rely on" and which would streamline the audit process by having a federal agency "nominate a panel of certified and tested audit firms with specialized cyber security expert audit teams." These teams would assess entities against the comprehensive security framework and provide implementation guidance to help organizations improve their cybersecurity posture.[149]

Information Technology

Fifteen respondents from the information technology sector, ranging from individual companies to industry organizations, provided their perspectives on how regulatory harmonization can improve cybersecurity. The Information Technology Sector Coordinating Council (IT SCC) posited that "resolving the overlapping regulatory morass is one of the most efficient ways to enhance cybersecurity."[150] Respondents articulated the value of adopting a risk-based approach to enable entities to best manage their resources commensurate with their unique risks. Red Alert Labs said that "properly designed regulations will promote (and even require) this allocation."[151] Respondents also called for Federal leadership to advance harmonization through greater regulatory cohesion.

Respondents highlighted the challenges of achieving regulatory agility in an ever-evolving cyber threat environment. 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." Critical infrastructure entities "are often subject to multiple regulatory frameworks, each with unique compliance and reporting requirements. These same industries are often given additional cybersecurity guidance from various Government entities, in addition to regulators, that lack synergy with one-another, creating confusion about Government priorities, what is expected of organizations, how, and to whom, to communicate in the event of an incident." 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."[152]

Several respondents described the compliance burden that arises from unharmonized regulations. BSA | The Software Alliance (BSA) described the compliance challenges that confront both companies and customers, saying "companies must invest heavily in identifying new and changing regulations; analyzing which regulations they must comply with and when; and making changes or documenting activities to comply with regulations, which may include reengineering products. Additionally, customers must invest in efforts to ensure that their third-party service providers are meeting any of the regulatory requirements that flow down from their regulators. The resources lost on these compliance activities cannot be invested in security improvements."[153]

★ ★ ★ ★ ★ ★

Compliance is especially burdensome to small and midsized enterprises and can stifle innovation. The App Association wrote that "a lack of harmonization in cybersecurity requirements across states and Federal agencies not only causes administrative burden but also has serious implications to the small business innovator community we represent. With fewer resources than larger entities, our members struggle to track and comply with the consistently-expanding number of cybersecurity-related regulations (e.g., cybersecurity incident reporting) at the Federal and state level; further, increased compliance complexity and costs effectively create barriers to entry to markets where our members innovations will drive competition."[154]

Alignment

Respondents stressed the importance of establishing a regulatory regime that applies minimum cybersecurity requirements across all critical infrastructure sectors while accommodating sector-specific risks. Microsoft emphasized that cross-sector harmonization of cybersecurity requirements is a necessary precursor to enabling reciprocity, cautioning that "reciprocity alone will not advance regulatory harmonization because it will not address the root cause of regulatory divergence - the promulgation of unharmonized requirements across sectors."[155]

Microsoft elaborated that "the primary challenge […] caused by regulatory divergence is increased complexity and costs associated with monitoring, analyzing, and managing compliance with redundant cybersecurity requirements. We define redundant requirements in this context as those intended to achieve the same security objective but use varying language, enable different implementations, or have separate enforcement mechanisms. […] The source of this complexity often stems from regulators separately writing their regulatory requirements to achieve similar security objectives but using different language."[156] Google recommended "aligning baseline requirements while allowing for the addition of sector-specific requirements on top of, but not duplicative of, those baseline requirements. The goal of such an approach should be to enable the expansion and adoption of key principles of security across the Federal ecosystem, critical infrastructure, and the private sector."[157]

SAP identified a similar need at the state and local levels, noting that "cybersecurity is not a one-size-fits-all issue. […] We've observed that local governments have unique needs and challenges that can differ significantly from those of the Federal Government. Cyber threats can affect everything from municipal utilities and emergency services to state health systems and tribal land management. These regional entities need the autonomy to tailor their cybersecurity regulations to address their specific concerns while still adhering to a broader, nationally cohesive framework."[158] The Information Technology Industry Council (ITI) agreed, saying that "cybersecurity harmonization across states is of paramount importance in our increasingly interconnected digital world. While states often have distinct needs and priorities when it comes to cybersecurity, a clear framework for Federal regulation is necessary to ensure consistency and effectiveness. Inconsistencies in regulations between states can create vulnerabilities that attackers can exploit, further highlighting the need for a centralized and preemptive Federal approach."[159]

Reciprocity

Respondents highlighted the need for Federal leadership in driving reciprocity at all levels of government, and proposed concrete steps for ONCD to pursue. The Cybersecurity Coalition asserted that "reciprocity among Federal agencies is key for lessening the burden of redundant

compliance efforts," and recommended that "ONCD consider developing a shared framework for incorporating cybersecurity standards in regulations and assessments, and establishing policies and procedures to foster the interagency coordination needed to successfully use the shared framework."[160] BSA wrote that "ONCD should encourage or incentivize state, local, tribal, and territorial (SLTT) Governments to allow companies to satisfy the SLTT government's cybersecurity requirements by complying with existing cybersecurity laws or certifications."[161] Workday said that "while full-throated reciprocity may not be feasible in the short term, we encourage ONCD and its interagency partners to explore identification of a core set of controls that are already present in many foreign frameworks that could be the basis for baseline requirements endorsed by multiple governments. This is a sensible first step in developing international consensus around baseline requirements in the long term."[162]

Recommendations

Respondents proposed several recommendations focused on promoting Federal leadership in cybersecurity regulatory harmonization. BSA asserted that "without a shared framework, there is no foundation from which the U.S. Government or any Government, can drive harmonization."[163] Microsoft proposed that "ONCD should establish a single regulatory framework for applying cybersecurity standards within regulations."[164] 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."[165]

Dragos noted that "multiple Federal agencies have different authorities and capabilities that are vital to implement and oversee cybersecurity-related policy and regulation," and suggested that "establishing a single front door for the Federal Government on cybersecurity issues could help alleviate this challenge. […] This entity should also lead coordination of an interagency process to ensure proposed new regulations are in harmony with existing rules and carry out a process to streamline rules when duplication or conflicting guidance exists."[166]

Workday offered that "one challenge of particular importance is that individual agencies own many of these requirements and are charged with oversight for their particular sectors. We therefore encourage ONCD to leverage its unique convening power to drive an interagency process focused on harmonization. As ONCD will need buy-in from individual agencies in order to make meaningful progress on harmonization, we see this convening power as the most important tool at ONCD's disposal to drive tangible improvements on regulatory harmonization."[167]

BSA agreed, saying that "ONCD should compel agencies to harmonize existing and new regulations. How ONCD does this, e.g., the creation of an office with the mission of harmonizing regulations as recommended by the President's National Security Telecommunications Advisory Committee (NSTAC), matters less than that those agencies are required to harmonize existing and new regulations. Without this commitment efforts to harmonize regulations are unlikely to succeed."[168]

★ ★ ★ ★ ★ ★

Nuclear Reactors, Materials, and Waste

The Nuclear Energy Institute (NEI) was the sole respondent from the Nuclear Reactors, Materials, and Waste Sector and indicated confidence in the existing regulatory environment. NEI stated that "the current regulatory framework, applicable to nuclear power generation facilities in areas like cybersecurity, provides comprehensive protection strategies for safety-related structures, systems, and components that are vital to the safe and secure operation of nuclear power."[169]

Reciprocity

NEI expressed support for regulatory reciprocity, particularly for supervision of third-party service providers. NEI noted that such a model would reduce duplication of oversight and "would be useful in third-party assessments of cybersecurity compliance, such as FedRAMP [Federal Risk and Authorization Management Program] […] for cloud services."[170] NEI also argued that a FedRAMP-style approach would enhance information sharing within the nuclear sector.

The FedRAMP program has been implemented by many Federal agencies "to meet security requirements for use of the cloud or cloud-based applications, which applies to this information sharing approach. Regulatory reciprocity with this security mindset for cloud services in the nuclear sector would provide opportunities for sharing information seamlessly and efficiently."[171]

Transportation Systems

In the transportation sector, regulatory requirements related to cybersecurity are diverse and complex, often directing regulated parties to adhere to numerous standards and frameworks. In their responses, Airlines for America (A4A) and the Association of American Railroads (AAR) advocated for adopting standardized cybersecurity frameworks to ensure that regulation improves cybersecurity outcomes, not merely increases compliance costs.

A4A and AAR also argued that harmonization of existing regulations is essential to address cybersecurity challenges effectively. Both respondents stressed the importance of regulatory reciprocity, calling for efforts to deconflict duplicative regulatory burdens and promote reciprocity between Federal and state regulators, streamline compliance processes, and enhance cybersecurity measures across the aviation and rail industries.

Alignment

A4A and AAR emphasized the need for cybersecurity regulations to have a common baseline that allows for flexibility to accommodate unique operational risks. A4A stated that the aviation industry is subject to regulatory requirements from several Federal agencies, including the Federal Aviation Administration (FAA), TSA, and DoD. These agencies require airlines to implement numerous controls, with specific guidance from some regulators and general direction from others to use existing frameworks. A4A recommended that Federal regulators adopt a standardized cybersecurity framework (e.g., NIST CSF) to "ensure outcome-focused objectives

do not evolve into a checklist compliance framework," while also providing operators "the flexibility to select the right measure based on their risk assessment and evolving threat."[172]

AAR wrote that "various regulations and laws governing cybersecurity in the rail industry create a mosaic of fragmented and competing rules" that complicate compliance.[173] These include regulations from the Federal Railroad Administration (FRA), Environmental Protection Agency (EPA), TSA, and DoD. AAR suggested that regulators recognize the success of existing voluntary standards in the rail industry and the value of voluntary cyber risk management frameworks such as the NIST CSF. AAR supports NIST CSF because it "provides cyber risk management guidance and is outcome-based and process-focused, ensuring that attention is placed on how an organization manages risk rather than specific prescribed technical measures that may or may not apply to a particular organization's threat or operational environment."[174]

Harmonization

A4A stated that public-private collaboration is critical to driving improvement in cybersecurity, and "harmonizing existing regulations is foundational to this work."[175] AAR advised ONCD to examine opportunities for deconflicting regulations[176] but also argued that regulatory harmonization "should not be limited to existing or proposed regulations."[177] AAR urged ONCD to "explicitly discourage new regulations when current voluntary standards, frameworks, or best practices are driving effective cybersecurity risk management activities."[178]

Reciprocity

As the transportation sector operates across states and countries, reciprocity at both the international and state level is particularly important.[179] A4A suggested the Federal Government "focus international engagement on reciprocity instead of harmonization" while also pursuing collaborative efforts to "develop common standards internationally."[180] Domestically, AAR noted that the current Federal regulatory environment is "further exacerbated by state laws attempting to address the same or similar issues," complicating compliance and increasing costs for a sector that operators across multiple jurisdictions.[181] Therefore, AAR argued for Federal legislation to "ensure an organized and unified national approach to cybersecurity." Federal preemption of state requirements "could help conserve resources through streamlining efforts across multiple Federal agencies and create a more effective response to cyber threats and incidents." Moreover, a Federal law "could put an end to the confusing and often conflicting individual state approaches […] cybersecurity regulation."[182]

★ ★ ★ ★ ★ ★

Additional Respondents

Cross-Sector Trade Organizations

The four cross-sector trade association respondents articulated a pressing need to streamline and harmonize cybersecurity regulations to support economic activity and protect national security. The U.S. Chamber of Commerce (Chamber), Business Roundtable (BRT), the Professional Services Council (PSC), and the Internet Security Alliance (ISA) shared their perspectives about the challenges of the current regulatory environment and the opportunity for harmonization to reduce compliance costs and improve cybersecurity posture. ISA wrote that "by recognizing the need for cybersecurity harmonization as Initiative 1.1.1 in the National Cybersecurity Strategy Implementation Plan, the Administration is properly prioritizing this initiative because addressing it will, comparatively quickly and effectively, enhance our nation's cybersecurity."[183]

BRT reported that "companies are subject to an ever-expanding web of cybersecurity regulations imposed at the state and Federal level, as well as internationally. As the National Cybersecurity Strategy acknowledges, it is important to address these concerns."[184] BRT maintained that "duplicative, conflicting or unnecessary regulations require companies to devote more resources to fulfilling technical compliance requirements without improving cybersecurity outcomes or customer protection."[185] ISA concurred, noting there is "wide consensus in the cybersecurity field […] that our collective efforts to enhance our cybersecurity is seriously undermined by an enormous lack of adequate cybersecurity resources."[186]

ISA warned that "the uncoordinated, wasteful, and redundant nature of cybersecurity regulation is not simply an administrative problem," but poses "one of the most persistent impediments to enhancing our nation's security," and "resolving the overlapping regulatory morass is one of the most efficient ways to enhance cybersecurity."[187] BRT added that the current environment also "incentivize[s] 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."[188] The Chamber stressed the importance of Federal leadership in driving regulatory harmonization, especially as "competing laws, regulations, and frameworks at the state and international level threaten to fragment the digital economy, confuse cybersecurity compliance efforts, and imperil the ability of American companies to compete globally."[189]

Alignment

Respondents underscored the importance of incorporating flexibility for sector-specific risk management in any cybersecurity regulatory regime, particularly in the face of a dynamic threat environment. BRT said that "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."[190]

Respondents referenced the value of a risk-based framework to inform the creation of minimum baseline cybersecurity requirements and enable reciprocity. PSC argued that the effectiveness of such frameworks "outweigh any burdens or cost in the following ways: frameworks are designed to align with other regulations and standards with which Federal contractors must comply; frameworks build in flexibility so Federal contractors can tailor to their specific needs; education and documentation resources help organizations understand implementation; and frameworks are continuously improving."[191]

Respondents noted the value of the NIST CSF, with PSC signaling its support for frameworks that "incorporate a wide array of controls and functions that align with other NIST standards and frameworks."[192] The Chamber wrote that the NIST CSF "is a reference point for organizations seeking to harmonize their cybersecurity practices domestically and internationally," and "there is broad consensus that the CSF is a sound baseline for cybersecurity practices and risk management." Furthermore, "the CSF has been translated into multiple languages, and the U.S. Chamber actively promotes its use internationally to comply with foreign cybersecurity rules."[193] The Chamber cited the Financial Services Sector Cybersecurity Profile (CRI Profile) as a prime example of leveraging the NIST CSF to create "efficiencies and flexibility for cybersecurity risk management" and provide "adequate assurance to Government supervisors."[194]

BRT echoed the Chamber's view, saying that the NIST CSF "has become a market baseline for cyber risk management" and suggesting that ONCD "emphasize regulatory approaches built around the NIST Cybersecurity Framework, broadly adopted international standards and other widely accepted, risk-based approaches to cybersecurity."[195]

Harmonization

Respondents voiced concern about the current practice of oversight and enforcement and cautioned against the addition of new regulations without unified efforts at harmonization. BRT said that "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."[196] BRT recommended that ONCD "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."[197]

A harmonized regulatory environment could also drive significant cybersecurity improvements for small- and medium-sized businesses. PSC suggested there is "tremendous opportunity to the Federal Government to work with managed service providers (MSPs) to assist in harmonizing regulations. In many cases, if an organization does not have in-house IT staff, it will employ the services of an MSP to build, maintain, and monitor a network infrastructure based on one of these CSP's cloud offerings. MSPs are integral to small business organizations. Many small businesses do not have the resources to support a full-time IT staff. MSPs often serve as IT and

cybersecurity support, as well as the translator to a small business leadership to understanding regulations and risks."[198]

Reciprocity

The Chamber identified opportunities for the United States to lead the international community on this issue, writing that "building off the U.S. Government's foreign policy and international engagement with non-U.S. cyber agencies, standards development organizations, and Government bodies, we urge the U.S. Government to take the lead on harmonizing regulations."[199] The Chamber recommended the use of "regulator-to-regulator Memoranda of Understanding or Bilateral Cybersecurity Mutual Recognition or Reciprocity Agreements," arguing that benefits included facilitation of cross-border trade, improved market access, assurance of stable and predictable regulatory environments, cost reduction, efficient compliance, enhanced cybersecurity, global interoperability, international cooperation, and improved consumer trust.[200]

Recommendations

The Chamber offered two recommendations to advance cybersecurity regulatory harmonization. First, the Chamber proposed that "the Administration and Congress should work with industry to pass legislation that carefully balances regulatory compliance with consensus standards and incentives," ensuring a "coordinated and cohesive Federal approach to national cybersecurity" that would "increase U.S. security and resilience." The Chamber stipulated that such legislation "should establish a common high-level standard for cybersecurity in the U.S. and provide a legal framework (1) to establish security measures routed in technical, international, consensus standards; (2) to protect covered entities from frivolous lawsuits and provide an affirmative defense; (3) to preempt substantially similar state-level cybersecurity rules; and (4) to create a White House office to drive state, Federal, and international harmonization."[201]

Second, the Chamber "urge[d] Congress to consider legislation" to sufficiently empower the White House with authority to convene independent regulatory agencies. Warning that "efforts at creating a cohesive and comprehensive cybersecurity framework would fall short should independent agencies not be included," the Chamber suggested that "narrowly scoped legislation authorizing the President's designee to convene independent regulatory agencies to exchange best practices on cybersecurity regulations would be a meaningful first step" to create "a cohesive and comprehensive cybersecurity framework."[202]

International Organizations

Two respondents offered international perspectives on cybersecurity regulatory harmonization – DIGITALEUROPE and the World Economic Forum (WEF). As cyberspace transcends borders, cybersecurity is inherently a global issue, requiring a regulatory approach that enables interoperability and mutual recognition. DIGITALEUROPE contends that "since every part of the world already is or has the potential to be connected, this shared risk is now a global risk. As a result, it is of great importance that cybersecurity policies, standards and the compliance or certification against them be globally interoperable across jurisdictions, with a baseline level of trust that extends across international boundaries."[203] WEF echoed the DIGITALEUROPE

position and stressed the negative impact to cybersecurity, stating that "regulatory hurdles hinder the achievement of global interoperability, leading to heightened costs, inefficiencies and missed opportunities as resources are redirected to tackle regulatory issues rather than enhancing sector-specific and organizational cybersecurity postures."[204] Consequently, WEF noted, "organizations have had to take hard, risk-based approaches ranging from managing regulatory complexities to exiting certain markets."[205]

Both respondents described the growing fragmentation of the global cybersecurity policy landscape, highlighting the complexities and inconsistencies resulting from disparate regulatory approaches and warning that diverging standards increase compliance costs and hinder sound cyber risk management. WEF observed that Government agencies worldwide "frequently adopt distinct approaches to address identical or similar cybersecurity challenges due to the absence of a global consensus. This leads to complex, industry and sector agnostic, fragmented, inconsistent, and sometimes conflicting regulations, which lack and prevent mutual interoperability."[206] Furthermore, "the evolution of the cybersecurity threat landscape and regulators' reflexive response to tighten regulations exacerbates the problem."[207] Both DIGITALEUROPE and WEF thus emphasized the importance of aligning cybersecurity regulations with internationally recognized frameworks to foster convergence, lower costs, and ensure interoperability across regulatory regimes.

Alignment

Respondents highlighted the important role that internationally accepted standards play in driving cybersecurity regulatory harmonization. DIGITALEUROPE recognized that "nuances in different jurisdictions understandably create different priorities for policymakers to manage and legislate," but cautioned that "jurisdiction-specific cybersecurity standards without cross-border interoperability and mutual recognition present challenges."[208] WEF wrote that the global digital economy requires "robust and unified international cybersecurity standards to ensure that multinational companies are best equipped to respond to new threats by malicious actors as they arise. As such, businesses around the world look to standards set by non-Government bodies such as the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) for guidance on a broad range of cybersecurity issues and as benchmarks for global best practices."[209]

WEF added that "when different regulators use widely recognized international technical standards – such as the ISO/IEC 27000 series of information security controls and the IEC 62443 series of industrial control system controls — to inform their policies, it not only sets a high standard of security for companies to adhere to but also lowers costs and assures interoperability with other regulatory regimes. Conversely, when different regulators and policy-makers use their own local standards and laws as a reference for establishing cybersecurity requirements, it contributes to the growing fragmentation of the global digital policy landscape, in turn unduly raising compliance costs for multi-jurisdictional companies and diverting resources from sound cyber-risk management activities."[210] Therefore, DIGITALEUROPE suggested that "likeminded partners should leverage every avenue of dialogue and cooperation to align their policies more closely to widely recognized international consensus-based technical standards,"[211] such as ISO and IEC, to "facilitate convergence" between nations.[212]

Reciprocity

WEF cited multiple examples of international reciprocity, including the European Union (EU)-US Data Privacy Framework, which removes regulatory hurdles to better facilitate data transfers between EU and U.S. companies, and the US-Israel Memorandum of Understanding on cybersecurity cooperation, which establishes a bilateral partnership focused on protecting critical infrastructure and includes mutual recognition of cybersecurity regulations.[213] Additionally, DIGITALEUROPE identified several existing programs that may serve as a model for international regulatory reciprocity, including FedRAMP for assessment and authorization of cloud services and Singapore's Cybersecurity Labelling Scheme for consumer information and communication technologies (ICT) products.[214]

Non-Profit and Professional Organizations

Ten non-profit and professional organizations, including certification bodies and research corporations, provided responses, and they were broadly supportive of Federal efforts to harmonize cybersecurity regulations. ISC2 wrote that "harmonization should be at the heart of any future cybersecurity regulations,"[215] while the Electronic Privacy Information Center (EPIC) and Consumer Reports, in a joint submission, supported ONCD's initiative "to ensure that strong and consistent cybersecurity rules apply across all critical infrastructure sectors and to create a harmonized regulatory environment that ensures baseline cybersecurity protections can be implemented and be effective."[216]

Several respondents noted the difficulties caused by the current array of cybersecurity regulations and the ensuing impact on managing cybersecurity risk. Aspen Digital wrote that its Aspen Global Cybersecurity Group members voiced concern over "the growing costs of operating in an international environment. One member observed that their organization is beholden to over 100 different countries' security baselines across their operating structure, in addition to over 500 customer-instantiated standards."[217] ISC2 observed that "organizations faced with overlapping, redundant, and/or conflicting cybersecurity requirements look to the 'highest watermark,' or said another way, the most restrictive requirements under each applicable law or regulation."[218] This complex regulatory environment puts significant strain on organizations, diverting limited cybersecurity resources as "cyber professionals are being forced to focus on legal compliance, rather than managing the cybersecurity behaviors and outcomes that lead to true risk mitigation for our nation, its businesses, and its citizens."[219]

As a result, organizations are increasingly vulnerable to cyber attacks. ISC2 explained that as "fear of non-compliance and penalties draws the focus of cybersecurity professionals from operational risk to compliance risk,"[220] cybersecurity professionals are "spending inordinate amounts of time complying with nuanced requirements rather than preventing and responding to cyber incidents."[221] Consequently, "tasks such as identifying internal and external threats, impact risk assessment, vulnerability assessment, and professional development are pushed to the backburner, which ultimately results in an increased risk of cyber breach and less efficient practices among cyber teams."[222]

The impact is particularly acute for small and medium businesses, which typically lack the compliance infrastructure and subject matter expertise to effectively manage multiple regulatory

regimes. ISC2 noted that "while larger organizations may have the resources to develop complex matrix systems to adhere to the numerous regulations and entities they report to, smaller companies are forced to decide whether to spend their time on compliance or protecting their organization from potential threats."[223] Aspen Digital remarked that this is especially challenging for small enterprises that operate internationally, as "the associated compliance work may make it impossible for them to compete in international markets" and therefore, "it is an equity imperative to streamline regulations and open the market to smaller competitors."[224]

Alignment

Respondents stressed the importance of developing requirements that shift the regulatory process from one that prioritizes compliance practices to instead inducing better cybersecurity posture. ISC2 warned that a reliance on "regulatory checklists" can leave organizations "vulnerable to breaches that could result in loss of profit and public trust — or an interruption to critical national infrastructure."[225] MITRE suggested that regulators provide "additional direction on how to shift the focus from compliance checking to strengthening the mechanisms" used by regulated entities "to produce meaningful improvements and more consistent outcomes."[226]

A "checklist" of rigid requirements is especially ineffective for critical infrastructure, where sector-specific risks, operational processes, and sensitive systems influence cybersecurity posture in unique ways for each sector. MITRE suggested that newly issued or revised regulations "not specify technical requirements or implementation details for critical infrastructure owners/operators or the industry vendors/providers that support them. Specifying such details would further complicate continuous regulation harmonization, and updates would likely not keep up with the rapidly evolving cybersecurity landscape."[227] Rather, critical infrastructure (CI) "owners/operators and industry vendors/providers need specific guidance, tailored to their CI sector, to be able to understand and implement the requirements. […] Without explicit guidance on how to prioritize risks and mitigation actions, many CI stakeholders are unable to appropriately calibrate their resources to address the requirements."[228]

Respondents highlighted the value of leveraging proven frameworks for sector-specific and cross-sector risk management. MITRE argued that "there is a need for frameworks that enable each CI sector to self-evaluate its specific risks, identify specific improvements in vulnerability and threat data and information sharing, and provide CI sector-specific technical assistance. At the same time, as vulnerabilities and threats can cut across individual sectors, it is also important for this support to enable cross-sector sharing and understanding."[229] In this regard, respondents cited the NIST CSF for its widespread implementation across sectors. ISC2 acknowledged the NIST CSF "as one of the foremost frameworks when it comes to mitigating cybersecurity risk," saying the CSF "has become a key to success and an industry standard for many organizations, both domestically and internationally, because of its adaptability and flexibility to evolve as the cyber landscape changes. […] The NIST Framework is particularly helpful as it complements security standards without supplanting the same, is flexible and easily adaptable, and provides for long-term cybersecurity risk management."[230]

To accommodate the varying risk levels of different critical infrastructure sectors, EPIC and Consumer Reports proposed adoption of "a risk-based, two-tiered framework" in which "the first tier would set the baseline that would apply to all critical infrastructure organizations," while

"the second tier would impose different requirements dependent upon the types of data and processing contexts in which the risks are greater (thereby implicating the second tier rather than the first tier), but would still constitute a uniform baseline within each respective data and processing situation."[231]

Harmonization

Respondents reacted favorably to cross-sector harmonization, and advocated for a more holistic approach that recognizes how states and other nations are driving regulatory action and often faster than the Federal Government. ISC2 advised that harmonization efforts should "focus not only on Federal requirements, but also global, state, local, and tribal requirements."[232] Calling for "immediate action on the global harmonization of cybersecurity regulations," ISC2 said "there is an opportunity to develop a common approach and taxonomy with collaboration among Governments, industry, and professional associations […] that will foster the strongest cyber resilience and posture globally."[233]

The Center for Internet Security (CIS) suggested that the United States is in "the pre-regulatory period of cybersecurity," as "there are few expressly relevant Federal statutes, and Federal regulation of cyber is mostly sector-based, inconsistent, and incomplete in coverage." In the absence of overarching Federal legislation, CIS observed that "states are passing cybersecurity laws, initially in the area of insurance law and, more recently, in the area of data privacy statutes, all of which have a cybersecurity requirement. […] The significance of this from the cyber perspective is that even though these laws were not advertised as such, they are all cybersecurity laws, as they each require the organization that controls the private information to protect that data on their computer networks using reasonable security. […] Accordingly, the lack of a national, cross-sector, statutory minimum standard of information security in the U.S. has resulted in a plethora of authorities that attempt to create greater cyber defenses but result in a hodgepodge of good intentions that are difficult to translate into action."[234]

State and Local Government Associations

Three state Government associations submitted responses – the National Association of Regulatory Utility Commissioners (NARUC), the National Association of State Chief Information Officers (NASCIO), and StateRAMP. Respondents shared their experiences with the lack of regulatory harmonization between Federal and SLTT entities and the impact on SLTT resources. NASCIO said that "compliance with duplicative requirements of Federal cybersecurity regulations has grown significantly in cost, both financial and in personnel time," presenting challenges for its members "who are actively seeking savings for taxpayers through IT initiatives like consolidation/optimization. Further, when state data centers are audited for compliance, states receive inconsistent findings from Federal auditors despite reviewing the same IT environment."[235] NARUC and NASCIO supported the Federal Government assuming a leadership role in cybersecurity regulatory harmonization, and StateRAMP offered "to serve as a conduit and collaborator with the Federal Government in advancing the pillars of the National Cybersecurity Strategy to all levels of Government."[236]

Alignment

Respondents agreed that the Federal Government should prioritize the establishment of minimum cybersecurity requirements while also allowing for sector-specific solutions. NASCIO observed that "Federal cybersecurity regulations largely address the same controls and outcomes but differ in their specific requirements"[237] and referenced a Government Accountability Office study which found "between 49 and 79 percent of Federal agency cybersecurity requirements had conflicting parameters."[238] NASCIO proposed that ONCD and Federal agencies collaborate with state chief information officers to simplify Federal cybersecurity regulations, asserting that "addressing duplicative regulations and inconsistent audit practices will not only save taxpayer funds but will also improve our nation's cybersecurity posture."[239]

NARUC identified a number of frameworks and standards that its members use for cybersecurity, writing that "Public Utility Commissions (PUCs) rely on the NIST Cybersecurity Framework" and similar best practices, alongside guidance from NARUC. NARUC noted "as cybersecurity threats against critical infrastructure grow and evolve," more of its members "are now considering specifying mandatory cybersecurity requirements for their jurisdictional utilities."[240] NARUC is working with PUCs, DOE, and CISA "to establish a set of baseline cybersecurity requirements specific to electric distribution utilities and connected distributed energy resources. This initiative is relying on the existing body of cybersecurity frameworks, standards, and practices as the basic building blocks of requirements tailored explicitly for the operational and cybersecurity risk environments of electric distribution utilities."[241]

Harmonization

While NARUC wrote that it considers "harmonization of regulations and requirements related to cybersecurity an important goal," it emphasized that "harmonization must include flexibility to address the unique operating and risk environments of critical infrastructure sectors."[242] NARUC added that "any Federal action to achieve effective, aligned cybersecurity requirements also must be mindful of existing Federal and State regulatory authority," particularly with respect to sectors, such as electricity, where there are clear jurisdictional divisions of responsibility between the Federal Government and states.[243]

StateRAMP also spoke to the importance of harmonization, explaining that "an important strategic initiative for StateRAMP is to harmonize frameworks to identify common standards that can apply a majority of the time for SLTTs. For example, if the StateRAMP standards can satisfy 90% of the requirements for a jurisdiction, that is a significant value-add for both the SLTT and provider communities."[244] StateRAMP encouraged "Federal harmonization of application of Federal frameworks" to facilitate SLTT compliance with requirements for Federal programs, including grants and law enforcement services.[245]

Reciprocity

NARUC recognized the importance of reciprocity and noted that "because existing standards are the foundation of NARUC's baselining initiative, reciprocity with those standards is built in. Mapping these standards to the baselines will be a key output of the initiative, which will demonstrate the inherent reciprocity."[246]

StateRAMP highlighted its work with FedRAMP to establish reciprocity, and noted that it is pursuing comparable arrangements with the Federal Bureau of Investigation's Criminal Justice Information Services and HITRUST "to further reduce provider costs and resource drains around meeting different compliance frameworks."[247] StateRAMP also recommended the creation of a "fast track process from StateRAMP to FedRAMP (for products with a StateRAMP authorization, allow them to leverage their StateRAMP work to achieve a FedRAMP (for products with a StateRAMP authorization, allow them to leverage their StateRAMP work to achieve a FedRAMP status)."[248]

★ ★ ★ ★ ★ ★

Appendix A: Cyber Regulatory Harmonization RFI Responses Received

Sector	Respondents	Total Comments
Academic Institutions	Georgia Tech Columbia University School of International and Public Affairs Cyber Florida	3
Chemical Sector	American Chemistry Council	1
Communications Sector	CTIA National Cable & Telecommunications Association USTelecom Verizon	4
Consulting	Deloitte Boston Consulting Group Accenture	3
Critical Manufacturing Sector	Aerospace Industries Association National Electrical Manufacturers Association	2
Cross-sector Trade Organizations	Business Roundtable Internet Security Alliance Professional Services Council United States Chamber of Commerce	4
Defense Industrial Base Sector	National Defense Industry Association National Defense Information Sharing & Analysis Center	2
Energy Sector	American Public Power Association Edison Electric Institute Exelon North American Electric Reliability Corporation North America Transmission Forum The Associations American Fuel & Petrochemical Manufacturers American Gas Association Petroleum Institute Interstate Natural Gas Association of America Western Area Power Association Southwestern Power Administration	8
Federal Government	United States Department of Interior Bureau of Reclamation	1
Financial Services Sector	Bank Policy Institute and American Bankers Association Credit Union National Association Fintech Open Source Foundation	10

	Fidelity National Information Services, Inc. Financial Services Sector Coordinating Council The Insurance Coalition Marsh McLennan Mortgage Bankers Association National Association of Federally-Insured Credit Unions SAFE Credit Union	
Government Services and Facilities Sector	New York State	1
Healthcare and Public Health Sector	AdvaMed American Hospital Association College of Healthcare Information Management Executives and Association for Executives in Healthcare Information Security Cooperative Exchange HITRUST Kaiser Permanente MITA Premier	8
Individual Contributors	Jerry Perullo Pamela Gupta Richard Halliger Sharpe Management Consulting Anonymous Fusion3 Consulting	6
Information Technology Sector	ACT The App Association Amazon Web Services BSA | The Software Alliance CyberSaint Security Cybersecurity Coalition Dragos Google HP Information Technology Industry Council Information Technology Sector Coordinating Council Microsoft Red Alert Labs SAP SecurityScorecard Team8 Workday	16
International Organizations	DigitalEurope World Economic Forum	2

Non-Profit and Professional Organizations	A2LA Aspen Digital Center for Internet Security Electronic Privacy Information Center International Society of Automation Global Cybersecurity Alliance ISACA (Information Systems Audit and Control Association) ISC2 MITRE Secure Controls Framework	9
Nuclear Reactors, Materials, and Waste Sector	Nuclear Energy Institute	1
State and Local Associations	National Association of Regulatory Utility Commissioners StateRAMP National Association of State Chief Information Officers	3
Transportation Systems Sector	Airlines for America Association of American Railroads	2
Total		**86**

★ ★ ★ ★ ★ ★

Appendix B: Request for Information on Cyber Regulatory Harmonization

ONCD noticed the "Request for Information on Cyber Regulatory Harmonization; Request for Information: Opportunities for and Obstacles to Harmonizing Cybersecurity Regulations" in the Federal Register on August 16, 2023. It is reprinted below and available online, here: https://www.Federalregister.gov/documents/2023/08/16/2023-17424/request-for-information-on-cyber-regulatory-harmonization-request-for-information-opportunities-for.

AGENCY:

Office of the National Cyber Director, Executive Office of the President.

ACTION:

Request for information (RFI).

SUMMARY:

The Office of the National Cyber Director (ONCD) invites public comments on opportunities for and obstacles to harmonizing cybersecurity regulations, per Strategic Objective 1.1 of the National Cybersecurity Strategy. ONCD seeks input from stakeholders to understand existing challenges with regulatory overlap, and explore a framework for reciprocity (the recognition or acceptance by one regulatory agency of another agency's assessment, determination, finding, or conclusion with respect to the extent of a regulated entity's compliance with certain cybersecurity requirements) in regulator acceptance of other regulators' recognition of compliance with baseline requirements.

DATES:

The original comment deadline for this RFI was 5 p.m. EDT September 15, 2023. ONCD has extended the deadline for comments to be received to 5 p.m. EDT October 31, 2023.

ADDRESSES:

Interested parties may submit comments through *www.regulations.gov*. For detailed instructions on submitting comments and additional information on this process, see the **SUPPLEMENTARY INFORMATION** section of this document.

FOR FURTHER INFORMATION CONTACT:

Requests for additional information may be sent to: Elizabeth Irwin, 202-881-6791, *regharmonization@ncd.eop.gov*.

★ ★ ★ ★ ★ ★

SUPPLEMENTARY INFORMATION:

In this RFI, ONCD invites public comments on cybersecurity regulatory conflicts, inconsistencies, redundancies, challenges, and priorities, in response to the questions below. Strategic Objective 1.1 of the National Cybersecurity Strategy [1] recognizes that while voluntary approaches to critical infrastructure cybersecurity have produced meaningful improvements, the lack of mandatory requirements has resulted in inadequate and inconsistent outcomes. The Strategy calls for establishing cybersecurity regulations to secure critical infrastructure where existing measures are insufficient, harmonizing and streamlining new and existing regulations, and enabling regulated entities to afford to achieve security. ONCD, in coordination with the Office of Management and Budget (OMB), has been tasked with leading the Administration's efforts on cybersecurity regulatory harmonization. [2] We will work with independent and executive branch regulators to identify opportunities to harmonize baseline cybersecurity requirements for critical infrastructure. [3]

ONCD is particularly interested in regulatory harmonization as it may apply to critical infrastructure sectors and sub-sectors identified in Presidential Policy Directive 21 and the National Infrastructure Protection Plan, and providers of communications, IT, and cybersecurity services to owners and operators of critical infrastructure. “Harmonization” as used in this RFI refers to a common set of updated baseline regulatory requirements that would apply across sectors. Sector regulators could go beyond the harmonized baseline to address cybersecurity risks specific to their sectors. ONCD is also interested in newer technologies, such as cloud services, or other “Critical and Emerging Technologies” identified by the National Science and Technology Council, [4] that are being introduced into critical infrastructure.

ONCD strongly encourages academics, non-profit entities, industry associations, regulated entities, and others with expertise in cybersecurity regulation, risk management, operations, compliance, and economics to respond to this RFI. We also welcome state, local, Tribal, and territorial (SLTT) entities to submit responses in their capacity as regulators and as critical infrastructure entities, specifying the sector(s) in which they are regulated or regulate.

Guidance for submitting comments:

- Please limit your narrative response to twenty-five (25) pages total. Additional analysis and/or contextual information specific to a question(s) may be submitted in a supplemental appendix.
- Respondents are encouraged to comment on any issues or concerns you believe are relevant or appropriate for our consideration and to submit written data, facts, and views addressing this subject, including but not limited to the questions below.
- Respondents do not need to answer all questions listed — only the question(s) for which you have relevant information. The written RFI response should address ONLY the topics for which the respondent has knowledge or expertise.
- Wherever possible, please provide credible data and specific examples to support your views. If you cite academic or other studies, they should be publicly available to be considered.

- Please provide the name of the critical infrastructure sector(s) to which you are aligned or support.
- Do not submit comment(s) in this RFI regarding harmonization of cyber incident reporting requirements. Such requirements are being analyzed through a separate effort led by the Cyber Incident Reporting Council established by the Secretary of Homeland Security as required by the Cyber Incident Reporting for Critical Infrastructure Act of 2022.
- All submissions are public records and may be published on *www.regulations.gov*. Do NOT submit sensitive, confidential, or personally identifiable information.

Questions for respondents:

1. Conflicting, mutually exclusive, or inconsistent regulations — If applicable, please provide examples of any conflicting, mutually exclusive, or inconsistent Federal and SLTT regulations affecting cybersecurity — including broad enterprise-wide requirements or specific, targeted requirements — that apply to the same information technology (IT) or operational technology (OT) infrastructure of the same regulated entity. Be as clear, specific, and detailed as possible.
   a. Please include specific examples with legal citations or hyperlinks to the particular Federal or SLTT cybersecurity rules or enforceable guidance that impose conflicting, mutually exclusive, or inconsistent requirements, and explain the specific conflicts or inconsistencies you identify.
   b. Have these conflicting, mutually exclusive, or inconsistent rules or guidance been updated to meet new cybersecurity risks, vulnerabilities, or threats (e.g., supply chain risk)? If so, were those separate rules or guidance updated at close to the same time?
   c. How do regulated entities comply with these conflicting mutually exclusive, or inconsistent requirements (e.g., follow the most demanding standard)? Please describe your experiences managing such compliance requirements.
   d. For entities subject to conflicting, mutually exclusive, or inconsistent regulations, what monetary, executive or cyber defense team work hours, or other resource costs do they incur as a result of managing compliance with the different requirements that apply to them from different regulators?
   e. Please identify cybersecurity requirements imposed by industry bodies, Federal or SLTT agencies that you believe may be redundant. [5] Please explain in detail how the requirements in question are redundant.
   f. As to the above questions, please provide the estimated annual cost over the past three years in terms of expenses or additional staff to comply with the conflicting, mutually exclusive, inconsistent, or redundant cybersecurity regulatory requirements you cite, and describe your methodology for developing those estimates.
   g. Currently, how resource intensive is it for regulated entities to achieve cybersecurity compliance?
   h. How often do prohibitive costs of compliance lead to meaningful security gaps?
   i. How can future regulations address any prohibitive costs which lead to meaningful security gaps?
   j. How can future regulations be implemented in ways which allow regulated entities to achieve security improvements at an acceptable cost?

2. Use of Common Guidelines — Through the Federal Financial Institutions Examination Council (FFIEC), regulators of certain financial institutions have issued common Interagency Guidelines Establishing Information Security Standards and have developed a Common Self-Assessment Tool and an Information Security Booklet to guide examinations of entities in the financial sector.

a. Is such a model effective at providing harmonized requirements and why?
b. What challenges are associated with such a model?
c. Are there opportunities to adapt such a model to other sectors — or across multiple sectors — and if so, how?
d. Are there sectors or subsectors for which such a model would not be appropriate, and if so, why?
e. How does or could such a model apply outside the context of examination-based compliance regimes?
f. Are there opportunities to improve on such a model through common oversight approaches, and, if so, how?
g. Does your organization voluntarily apply a self-assessment tool regularly? What are good examples of helpful tools?
h. Would a common self-assessment tool improve the ability of entities to meet regulatory requirements?

3. Use of Existing Standards or Frameworks — The practice of using existing standards or frameworks in setting regulatory requirements can reduce burdens on regulated entities and help to achieve the goals of regulatory harmonization. Under existing law, [6] Federal executive agencies use voluntary consensus standards for regulatory activities unless use of such standards is inconsistent with law or otherwise impractical. In a recent report [7] from the President's National Security Telecommunications Advisory Council (NSTAC) that addressed cybersecurity regulatory harmonization, the NSTAC noted that "even though most regulations cite consensus standards as the basis for their requirements, variations in implementations across regulators often result in divergent requirements."

a. To what extent are cybersecurity requirements applicable to your industry or sector based on, consistent with, or aligned with existing standards or frameworks?
    i. Which standards or frameworks have been applied to your industry or sector?
    ii. Have these standards or frameworks been adopted in whole, either through the same requirements or incorporation by reference, or have they been modified by regulators?
    iii. If modified, how were they modified by particular regulators? Has your entity or have others in your sector provided input that the regulator used to develop or adapt existing standards for your sector? If so, what are the mechanisms, frequency, and nature of the inputs?
b. Is demonstrating conformity with existing standards or frameworks that your industry is required by regulation to use readily auditable or verifiable and why?
c. What, if any, additional opportunities exist to align requirements to existing standards or frameworks and, if there are such opportunities, what are they?

4. Third-Party Frameworks — Both the Government (for example, through the NIST Cybersecurity Framework) and non-Government third parties have developed frameworks and

related resources that map cybersecurity standards and controls to cybersecurity outcomes. These frameworks and related resources have also been applied to map controls to regulatory requirements, including where requirements are leveled by multiple agencies.

a. Please identify such frameworks and related resources, both Governmental and non-Governmental, currently in use with respect to mitigating cybersecurity risk.
b. How well do such frameworks and related resources work in practice to address disparate cybersecurity requirements?

5. Tiered Regulation — Different levels of risk across and within sectors may in part be addressed through a tiered model (e.g., low, moderate, or high risk),[8] potentially assisting in tailoring baseline requirements for each regulatory purpose. Tiering may also help smaller businesses meet requirements commensurate with their risk. For example, while these are not regulations, tiering into several baselines is a feature of Federal Information Processing Standard 199 and the NIST Risk Management Framework.

a. Could such a model be adapted to apply to multiple regulated sectors? If so, how would tiers be structured?
b. How could this tiered approach be defined across disparate operational environments and what might be some of the opportunities and challenges associated with doing so?

6. Oversight — Please provide examples of cybersecurity oversight by multiple regulators of the same entity, and describe whether the oversight involved IT or OT infrastructure. Some of these questions reference a potential "regulatory reciprocity" model, under which cybersecurity oversight and enforcement as to cross-sector baseline cybersecurity requirements would be divided among regulators, with the "primary" or "principal" regulator for an entity having authority to oversee and enforce compliance with that baseline.

a. Please identify the Federal, state or local agencies that are engaged in cybersecurity oversight of the same IT or OT systems, components, or data ("infrastructure") at the same regulated entity. This may be multiple Federal regulatory schema or multiple intergovernmental bodies (e.g., Federal, state, local, Tribal, territorial).
b. Please describe the method(s) of cybersecurity oversight utilized by the agencies identified in your response to the question above.
c. To what extent, if any, are you aware that the agencies engaged in cybersecurity oversight of the same IT or OT infrastructure coordinate their oversight activities? Please describe.
d. Where multiple agencies are engaged in cybersecurity oversight of the same IT or OT infrastructure:
    i. Is the role of a "primary" or "principal" agency recognized? If so, please describe how.
    ii. To what extent do one or more of these agencies rely on or accept the findings, assessments or conclusions of another agency with respect to compliance with regard to certain cybersecurity requirements ("regulatory reciprocity")? Please provide specific examples.
    iii. What are the barriers to regulatory reciprocity (legal, cultural, sector-specific technical expertise, or other)?
e. Are there situations in which regulations related to physical security, safety, or other matters are intertwined with cybersecurity in such a way that baseline cybersecurity

regulatory requirements from a separate Federal entity might have unintended consequences on physical security, safety, or another matter? If so, please provide specific examples.

f. If you are a regulated entity, what is the estimated annual cost over the past five years in terms of expenses or additional staff to address overlapping cybersecurity oversight of the same IT or OT infrastructure? Please describe the methodology used to develop the cost estimate.
g. Do multiple public sector agencies examine or audit your cybersecurity compliance for the same IT or OT infrastructure? If so, how many entities examine or audit the infrastructure and how often do these audits occur?
h. What, if any, obstacles or inefficiencies have you experienced with regard to cybersecurity oversight, examination or enforcement related to OT components, systems, or data?
i. Please provide examples of regulatory reciprocity between two or more Federal agencies with respect to cybersecurity, including the recognition or acceptance by one regulatory agency of another agency's assessment, determination, finding, or conclusion with respect to the extent of a regulated entity's compliance with certain IT or OT cybersecurity requirements.
j. Are you aware of examples of regulatory reciprocity in contexts other than cybersecurity? If so, please describe briefly the agencies and the context.
k. Please provide examples of self-attestation in cybersecurity regulation. What are the strengths and weaknesses of this model?
l. Please comment on models of third-party assessments of cybersecurity compliance that may be effective at reducing burdens and harmonizing processes. For example, FedRAMP relies on Third Party Assessment Organizations (3PAOs) to perform initial assessments to inform decisions on FedRAMP eligibility. 3PAOs are accredited by an independent accreditation body.
    i. Are there circumstances under which use of third-party assessors would be most appropriate?
    ii. Are there circumstances under which use of third-party assessors would not be appropriate?

7. Cloud and Other Service Providers — Information technology, as a sector, is not regulated directly by the Federal Government. However, regulated entities' use of cloud and other service provider infrastructure is often regulated. To date, regulators have typically not directly regulated cloud providers operating in their sector. Rather, regulatory agencies have imposed obligations on their regulated entities that are passed along by contract to the cloud provider/service provider.

a. Please provide specific examples of conflicting, mutually exclusive, or inconsistent cybersecurity regulatory requirements that are passed along by contract to third-party service providers.
b. Please provide examples of direct cybersecurity regulation of third-party service providers.
c. Please provide information regarding the costs to third-party service providers of conflicting, mutually exclusive, or inconsistent cybersecurity regulatory requirements that are passed on to them through their contracts with regulated customers. Please also

provide estimated costs to a regulated customer of using a third-party service provider when conflicting, mutually exclusive, or inconsistent cybersecurity regulatory requirements are passed to the customer through contracts. In either case, please detail the methodology for developing the cost estimate.

d. Describe any two or more conflicting, mutually exclusive, or inconsistent regulation, one of which permits the use of cloud, while another does not. How does this impact your sector? Explain if these requirements also restrict the use of Managed Security Service Providers (MSSPs) and security tools that utilize the cloud.
e. Have any non-U.S. Governments instituted effective models for regulating the use of cloud services by regulated entities in a harmonized and consistent manner? Please provide examples and explain why these models are effective.
f. The Department of Defense allows defense industrial base contractors to meet security requirements for the use of the cloud by using FedRAMP-approved infrastructure. Please provide examples of how the FedRAMP process differs, positively or negatively, from other requirements. What, if anything, would need to change about the FedRAMP certification process and requirements for it to be usable to meet other cybersecurity regulatory requirements?
g. To the extent not included in response to any other question, please identify any specific Critical or Emerging Technologies that are subject to conflicting, mutually exclusive, or inconsistent regulation related to cybersecurity.

8. State, Local, Tribal, and Territorial Regulation. State, local, Tribal and territorial entities often impose regulatory requirements that affect critical infrastructure owners and operators across state lines, as well as entities that do not neatly fall into a defined critical infrastructure sector. The New York Department of Financial Services, for example, established cybersecurity requirements for financial services companies. [9] California similarly passed a cybersecurity law requiring manufacturers of the internet-of-things (IoT) devices to take certain measures. [10] Dozens of states have followed suit to date. Companies that operate in multiple states are often required to comply with a variety of overlapping state and Federal cybersecurity requirements.

a. Please provide examples where SLTT cybersecurity regulations are effectively harmonized or aligned with Federal regulations.
b. Please provide examples of regulatory reciprocity between Federal and SLTT regulatory agencies.
c. Please highlight any examples or models for harmonizing regulations across multiple SLTT jurisdictions, to include Federal support for such efforts.
d. Please provide examples, if any, where regulatory requirements related to cybersecurity are conflicting, mutually exclusive or inconsistent within one jurisdiction (for example, state regulatory requirements that conflict with regulations at the local level).

9. International — Many regulated entities within the United States operate internationally. A recent report from the NSTAC noted that foreign Governments have been implementing regulatory regimes with “overlapping, redundant or inconsistent requirements. . .”.

a. Identify specific instances in which U.S. Federal cybersecurity requirements conflict with foreign Government cybersecurity requirements.
b. Are there specific countries or sectors that should be prioritized in considering harmonizing cybersecurity requirements internationally?

c. Which international dialogues are engaged in work on harmonizing or aligning cybersecurity requirements? Which would be the most promising venues to pursue such alignment?
d. Please identify any ongoing initiatives by international standards organizations, trade groups, or non-Governmental organizations that are engaged in international cybersecurity standardization activities relevant to regulatory purposes. Describe the nature of those activities. Please identify any examples of regulatory reciprocity within a foreign country.
e. Please identify any examples of regulatory reciprocity between foreign countries or between a foreign country and the United States.

10. Additional Matters— Please provide any additional comments or raise additional matters you feel relevant that are not in response to the above questions.

Comments must be received no later than 5 p.m. EDT, October 31, 2023.

By October 31, 2023, all interested respondents should submit a written RFI response, in MS Word or PDF format, with their answers to questions on which they have expertise and insights for the Government through *regulations.gov*.

Inputs that meet most of the following criteria will be considered most valuable:

- *Concise:* Please limit your narrative response to 25 pages total. Additional analysis and/or contextual information specific to a question may be submitted in a supplemental appendix.
- *Easy to review and understand:* Content that is modularly organized in the order of the questions in the RFI and presented in such a fashion that it can be readily lifted (by topic area) and shared with relevant stakeholders in an easily consumable format.
- *Expert:* The Government, through this effort, is seeking insights to understand current best practices and approaches applicable to the above topics, as well as new and emerging solutions.
- *Clearly worded/not vague*: Clear, descriptive, and concise language is appreciated. Please avoid generalities and vague statements.
- *Actionable:* Please provide enough detail so that we can understand how to apply the information you provide.
- *Cost effective & impactful:* If applicable, respondents should consider whether their suggestions have a clear return on investment that can be articulated to secure funding and support.
- *Strategic shifts:* Challenges that seem to be intractable and overwhelmingly complex can often be resolved with a change in perspective that unlocks hidden opportunities and aligns stakeholder interests. We welcome these ideas as well.

Kemba Walden

Acting National Cyber Director

RFI Footnotes

1. *https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf*. Back to Citation
2. Pursuant to the National Cybersecurity Strategy: "ONCD, in coordination with the Office of Management and Budget (OMB), will lead the Administration's efforts on cybersecurity regulatory harmonization." Back to Citation
3. Pursuant to the National Cybersecurity Strategy, the Cyber Incident Reporting Council will coordinate, deconflict, and harmonize Federal incident reporting requirements. ONCD is not requesting views from respondents on incident reporting regulations. Back to Citation
4. *https://www.whitehouse.gov/wp-content/uploads/2022/02/02-2022-Critical-and-Emerging-Technologies-List-Update.pdf*. Back to Citation
5. For the purpose of this RFI, "redundant" would mean that (1) the same regulated entity must comply with more than one Federal or SLTT cybersecurity requirements covering the same systems and (2) one or more of those regulations could be eliminated while the regulating agencies that issued the regulations are still able to fulfill the purpose of the regulation. Back to Citation
6. Public Law 104-113. Back to Citation
7. *https://www.cisa.gov/sites/default/files/2023-04/NSTAC_Strategy_for_Increasing_Trust_Report_%282-21-23%29_508_0.pdf*. Back to Citation
8. FIPS 199, Standards for Security Categorization of Federal Information and Information Systems (*nist.gov*). Back to Citation
9. See 23 NYCRR Part 500. Back to Citation
10. See Senate Bill No. 327. Back to Citation

[FR Doc. 2023-17424 Filed 8-15-23; 8:45 am]

BILLING CODE 3340-D3-P

ENDNOTES

[1] American Chemistry Council (ACC), page 1. https://www.regulations.gov/comment/ONCD-2023-0001-0084.
[2] ACC, page 2. https://www.regulations.gov/comment/ONCD-2023-0001-0084.
[3] ACC, page 1. https://www.regulations.gov/comment/ONCD-2023-0001-0084.
[4] ACC, page 2. https://www.regulations.gov/comment/ONCD-2023-0001-0084.
[5] ACC, page 2. https://www.regulations.gov/comment/ONCD-2023-0001-0084.
[6] ACC, page 2. https://www.regulations.gov/comment/ONCD-2023-0001-0084.
[7] ACC, page 2. https://www.regulations.gov/comment/ONCD-2023-0001-0084.
[8] ACC, page 2. https://www.regulations.gov/comment/ONCD-2023-0001-0084.
[9] ACC, page 2. https://www.regulations.gov/comment/ONCD-2023-0001-0084.
[10] USTelecom, page 3. https://www.regulations.gov/comment/ONCD-2023-0001-0068.
[11] CTIA – The Wireless Association (CTIA), page 1. https://www.regulations.gov/comment/ONCD-2023-0001-0030.
[12] CTIA, page 4. https://www.regulations.gov/comment/ONCD-2023-0001-0030.
[13] CTIA, pages 4-5. https://www.regulations.gov/comment/ONCD-2023-0001-0030.
[14] CTIA, page 1. https://www.regulations.gov/comment/ONCD-2023-0001-0030.
[15] CTIA, page 21. https://www.regulations.gov/comment/ONCD-2023-0001-0030.
[16] NCTA – The Internet & Television Association (NCTA), page 2. https://www.regulations.gov/comment/ONCD-2023-0001-0082.
[17] NCTA, page 2. https://www.regulations.gov/comment/ONCD-2023-0001-0082.
[18] CTIA, pages 1-2. https://www.regulations.gov/comment/ONCD-2023-0001-0030.
[19] CTIA, page 15. https://www.regulations.gov/comment/ONCD-2023-0001-0030.
[20] NCTA, page 2. https://www.regulations.gov/comment/ONCD-2023-0001-0082.
[21] Verizon, pages 2-3. https://www.regulations.gov/comment/ONCD-2023-0001-0051.
[22] Verizon, pages 1-2. https://www.regulations.gov/comment/ONCD-2023-0001-0051.
[23] Verizon, page 7. https://www.regulations.gov/comment/ONCD-2023-0001-0051.
[24] CTIA, page 21. https://www.regulations.gov/comment/ONCD-2023-0001-0030.
[25] Aerospace Industries Association (AIA), page 1. https://www.regulations.gov/comment/ONCD-2023-0001-0073.
[26] National Electrical Manufacturers Association (NEMA), page 7. https://www.regulations.gov/comment/ONCD-2023-0001-0018.
[27] NEMA, pages 6-7. https://www.regulations.gov/comment/ONCD-2023-0001-0018.
[28] AIA, page 1. https://www.regulations.gov/comment/ONCD-2023-0001-0073.
[29] NEMA, page 7. https://www.regulations.gov/comment/ONCD-2023-0001-0018.
[30] NEMA, pages 7-8. https://www.regulations.gov/comment/ONCD-2023-0001-0018.
[31] NEMA, page 7. https://www.regulations.gov/comment/ONCD-2023-0001-0018.
[32] AIA, page 9 https://www.regulations.gov/comment/ONCD-2023-0001-0073.
[33] AIA, page 3. https://www.regulations.gov/comment/ONCD-2023-0001-0073.
[34] AIA, page 2. https://www.regulations.gov/comment/ONCD-2023-0001-0073.
[35] AIA, page 5. https://www.regulations.gov/comment/ONCD-2023-0001-0073.
[36] NEMA, pages 7-8. https://www.regulations.gov/comment/ONCD-2023-0001-0018.
[37] AIA, page 2. https://www.regulations.gov/comment/ONCD-2023-0001-0073.
[38] AIA, page 9. https://www.regulations.gov/comment/ONCD-2023-0001-0073.
[39] AIA, page 7. https://www.regulations.gov/comment/ONCD-2023-0001-0073.
[40] NEMA, page 2. https://www.regulations.gov/comment/ONCD-2023-0001-0018.
[41] NEMA, page 2. https://www.regulations.gov/comment/ONCD-2023-0001-0018.
[42] National Defense Industry Association (NDIA), page 1. https://www.regulations.gov/comment/ONCD-2023-0001-0085.
[43] National Defense Information Sharing and Analysis Center – Policy, Standards and Regulations Working Group (ND-ISAC WG), page 6. https://www.regulations.gov/comment/ONCD-2023-0001-0071.
[44] ND-ISAC WG, pages 3-4. https://www.regulations.gov/comment/ONCD-2023-0001-0071.
[45] NDIA, page 6. https://www.regulations.gov/comment/ONCD-2023-0001-0085.
[46] ND-ISAC WG, page 25. https://www.regulations.gov/comment/ONCD-2023-0001-0071.

[47] NDIA, page 4. https://www.regulations.gov/comment/ONCD-2023-0001-0085.
[48] NDIA, page 7. https://www.regulations.gov/comment/ONCD-2023-0001-0085.
[49] ND-ISAC WG, page 15. https://www.regulations.gov/comment/ONCD-2023-0001-0071.
[50] ND-ISAC WG, page 4. https://www.regulations.gov/comment/ONCD-2023-0001-0071.
[51] ND-ISAC WG, page 2. https://www.regulations.gov/comment/ONCD-2023-0001-0071.
[52] NDIA, page 7. https://www.regulations.gov/comment/ONCD-2023-0001-0085.
[53] NDIA, page 4. https://www.regulations.gov/comment/ONCD-2023-0001-0085; ND-ISAC WG, page 14. https://www.regulations.gov/comment/ONCD-2023-0001-0071.
[54] NDIA, page 6. https://www.regulations.gov/comment/ONCD-2023-0001-0085; ND-ISAC WG, page 19. https://www.regulations.gov/comment/ONCD-2023-0001-0071.
[55] ND-ISAC WG, pages 1-2. https://www.regulations.gov/comment/ONCD-2023-0001-0071.
[56] ND-ISAC WG, page 1. https://www.regulations.gov/comment/ONCD-2023-0001-0071.
[57] ND-ISAC WG, page 22. https://www.regulations.gov/comment/ONCD-2023-0001-0071.
[58] ND-ISAC WG, page 22. https://www.regulations.gov/comment/ONCD-2023-0001-0071.
[59] ND-ISAC WG, page 22. https://www.regulations.gov/comment/ONCD-2023-0001-0071.
[60] ND-ISAC WG, page 1. https://www.regulations.gov/comment/ONCD-2023-0001-0071.
[61] NDIA, page 3. https://www.regulations.gov/comment/ONCD-2023-0001-0085.
[62] ND-ISAC WG, page 16. https://www.regulations.gov/comment/ONCD-2023-0001-0071.
[63] NDIA, page 3. https://www.regulations.gov/comment/ONCD-2023-0001-0085.
[64] NDIA, page 3. https://www.regulations.gov/comment/ONCD-2023-0001-0085.
[65] Exelon, page 1. https://www.regulations.gov/comment/ONCD-2023-0001-0033.
[66] American Fuel & Petrochemical Manufacturers (AFPM), the American Gas Association (AGA), the American Petroleum Institute (API), and the Interstate Natural Gas Association of America (INGAA), page 2. https://www.regulations.gov/comment/ONCD-2023-0001-0021.
[67] Edison Electric Institute (EEI), page 3. https://www.regulations.gov/comment/ONCD-2023-0001-0039.
[68] EEI, page 1. https://www.regulations.gov/comment/ONCD-2023-0001-0039.
[69] AFPM, AGA, API, and INGAA, page 2. https://www.regulations.gov/comment/ONCD-2023-0001-0021.
[70] AFPM, AGA, API, and INGAA, page 1. https://www.regulations.gov/comment/ONCD-2023-0001-0021.
[71] American Public Power Association (APPA) and Large Public Power Association (LPPC), pages 1-2. https://www.regulations.gov/comment/ONCD-2023-0001-0067.
[72] APPA and LPPC, page 4. https://www.regulations.gov/comment/ONCD-2023-0001-0067.
[73] North American Transmission Forum (NATF), page 2. https://www.regulations.gov/comment/ONCD-2023-0001-0049.
[74] Western Area Power Administration (WAPA), page 11. https://www.regulations.gov/comment/ONCD-2023-0001-0087.
[75] Exelon, page 1. https://www.regulations.gov/comment/ONCD-2023-0001-0033.
[76] Exelon, page 2. https://www.regulations.gov/comment/ONCD-2023-0001-0033.
[77] Exelon, pages 2-3. https://www.regulations.gov/comment/ONCD-2023-0001-0033.
[78] AFPM, AGA, API, and INGAA, page 3. https://www.regulations.gov/comment/ONCD-2023-0001-0021.
[79] AFPM, AGA, API, and INGAA, page 5. https://www.regulations.gov/comment/ONCD-2023-0001-0021.
[80] North American Electric Reliability Corporation (NERC), page 5. https://www.regulations.gov/comment/ONCD-2023-0001-0077.
[81] NATF, page 2. https://www.regulations.gov/comment/ONCD-2023-0001-0049.
[82] WAPA, page 3. https://www.regulations.gov/comment/ONCD-2023-0001-0087.
[83] Southwestern Power Administration (Southwestern), page 11. https://www.regulations.gov/comment/ONCD-2023-0001-0088.
[84] AFPM, AGA, API, and INGAA, page 3. https://www.regulations.gov/comment/ONCD-2023-0001-0021.
[85] AFPM, AGA, API, and INGAA, page 2. https://www.regulations.gov/comment/ONCD-2023-0001-0021.
[86] AFPM, AGA, API, and INGAA, page 4. https://www.regulations.gov/comment/ONCD-2023-0001-0021.
[87] EEI, pages 4-5. https://www.regulations.gov/comment/ONCD-2023-0001-0039.
[88] APPA and LPPC, page 3. https://www.regulations.gov/comment/ONCD-2023-0001-0067.
[89] APPA and LPPC, page 3. https://www.regulations.gov/comment/ONCD-2023-0001-0067.
[90] Exelon, page 5. https://www.regulations.gov/comment/ONCD-2023-0001-0033.

[91] Financial Services Sector Coordinating Council (FSSCC), pages 1-2. https://www.regulations.gov/comment/ONCD-2023-0001-0052.
[92] Marsh McLennan, page 1. https://www.regulations.gov/comment/ONCD-2023-0001-0010.
[93] FSSCC, pages 1-2. https://www.regulations.gov/comment/ONCD-2023-0001-0052.
[94] Mortgage Bankers Association (MBA), page 2. https://www.regulations.gov/comment/ONCD-2023-0001-0029.
[95] MBA, page 4. https://www.regulations.gov/comment/ONCD-2023-0001-0029.
[96] The Insurance Coalition, page 2. https://www.regulations.gov/comment/ONCD-2023-0001-0020.
[97] The Insurance Coalition, page 2. https://www.regulations.gov/comment/ONCD-2023-0001-0020.
[98] Bank Policy Institute (BPI) and American Bankers Association (ABA), page 2. https://www.regulations.gov/comment/ONCD-2023-0001-0069.
[99] Marsh McLennan, page 4. https://www.regulations.gov/comment/ONCD-2023-0001-0010.
[100] Marsh McLennan, page 4. https://www.regulations.gov/comment/ONCD-2023-0001-0010.
[101] The Insurance Coalition, page 1. https://www.regulations.gov/comment/ONCD-2023-0001-0020.
[102] Credit Union National Association (CUNA), page 2. https://www.regulations.gov/comment/ONCD-2023-0001-0035.
[103] BPI and ABA, page 11. https://www.regulations.gov/comment/ONCD-2023-0001-0069.
[104] CUNA, page 3. https://www.regulations.gov/comment/ONCD-2023-0001-0035.
[105] CUNA, page 3. https://www.regulations.gov/comment/ONCD-2023-0001-0035.
[106] BPI and ABA, page 1. https://www.regulations.gov/comment/ONCD-2023-0001-0069.
[107] FSSCC, pages 2-3. https://www.regulations.gov/comment/ONCD-2023-0001-0052.
[108] Marsh McLennan, page 8. https://www.regulations.gov/comment/ONCD-2023-0001-0010.
[109] MBA, page 5. https://www.regulations.gov/comment/ONCD-2023-0001-0029.
[110] MBA, page 1. https://www.regulations.gov/comment/ONCD-2023-0001-0029.
[111] BPI and ABA, page 13. https://www.regulations.gov/comment/ONCD-2023-0001-0069.
[112] BPI and ABA, page 13. https://www.regulations.gov/comment/ONCD-2023-0001-0069.
[113] BPI and ABA, page 14. https://www.regulations.gov/comment/ONCD-2023-0001-0069.
[114] Marsh McLennan, page 9. https://www.regulations.gov/comment/ONCD-2023-0001-0010.
[115] BPI and ABA, page 13. https://www.regulations.gov/comment/ONCD-2023-0001-0069.
[116] New York State, page 3. https://www.regulations.gov/comment/ONCD-2023-0001-0057.
[117] New York State, page 3. https://www.regulations.gov/comment/ONCD-2023-0001-0057.
[118] New York State, page 3. https://www.regulations.gov/comment/ONCD-2023-0001-0057.
[119] New York State, page 3. https://www.regulations.gov/comment/ONCD-2023-0001-0057.
[120] New York State, page 3. https://www.regulations.gov/comment/ONCD-2023-0001-0057.
[121] New York State, page 2. https://www.regulations.gov/comment/ONCD-2023-0001-0057.
[122] New York State, page 1. https://www.regulations.gov/comment/ONCD-2023-0001-0057.
[123] New York State, page 1. https://www.regulations.gov/comment/ONCD-2023-0001-0057.
[124] New York State, page 2. https://www.regulations.gov/comment/ONCD-2023-0001-0057.
[125] New York State, page 2. https://www.regulations.gov/comment/ONCD-2023-0001-0057.
[126] New York State, page 1. https://www.regulations.gov/comment/ONCD-2023-0001-0057.
[127] New York State, pages 1-2. https://www.regulations.gov/comment/ONCD-2023-0001-0057.
[128] New York State, page 1. https://www.regulations.gov/comment/ONCD-2023-0001-0057.
[129] Cooperative Exchange, page 2. https://www.regulations.gov/comment/ONCD-2023-0001-0075.
[130] HITRUST, page 4. https://www.regulations.gov/comment/ONCD-2023-0001-0012.
[131] HITRUST, page 4. https://www.regulations.gov/comment/ONCD-2023-0001-0012.
[132] College of Healthcare Information Management Executives (CHIME) and Association for Executives in Healthcare Information Security (AEHIS), page 2. https://www.regulations.gov/comment/ONCD-2023-0001-0044.
[133] Cooperative Exchange, page 2. https://www.regulations.gov/comment/ONCD-2023-0001-0075.
[134] Kaiser Permanente, page 4. https://www.regulations.gov/comment/ONCD-2023-0001-0050.
[135] CHIME and AEHIS, page 6. https://www.regulations.gov/comment/ONCD-2023-0001-0044.
[136] Cooperative Exchange, page 17. https://www.regulations.gov/comment/ONCD-2023-0001-0075.
[137] HITRUST, page 9. https://www.regulations.gov/comment/ONCD-2023-0001-0012.
[138] Kaiser Permanente, page 2. https://www.regulations.gov/comment/ONCD-2023-0001-0050.

[139] Medical Imaging and Technology Alliance (MITA), pages 1-2. https://www.regulations.gov/comment/ONCD-2023-0001-0008.
[140] MITA, page 2. https://www.regulations.gov/comment/ONCD-2023-0001-0008.
[141] MITA, page 2. https://www.regulations.gov/comment/ONCD-2023-0001-0008.
[142] Kaiser Permanente, page 3. https://www.regulations.gov/comment/ONCD-2023-0001-0050.
[143] Kaiser Permanente, page 3. https://www.regulations.gov/comment/ONCD-2023-0001-0050.
[144] Kaiser Permanente, page 3. https://www.regulations.gov/comment/ONCD-2023-0001-0050.
[145] HITRUST, page 22. https://www.regulations.gov/comment/ONCD-2023-0001-0012.
[146] Cooperative Exchange, page 6. https://www.regulations.gov/comment/ONCD-2023-0001-0075.
[147] Cooperative Exchange, page 6. https://www.regulations.gov/comment/ONCD-2023-0001-0075.
[148] Cooperative Exchange, page 5. https://www.regulations.gov/comment/ONCD-2023-0001-0075.
[149]Cooperative Exchange, pages 6–7. https://www.regulations.gov/comment/ONCD-2023-0001-0075.
[150] The Information Technology Sector Coordinating Council (IT SCC), page 1. https://www.regulations.gov/comment/ONCD-2023-0001-0046.
[151] Red Alert Labs, page 3. https://www.regulations.gov/comment/ONCD-2023-0001-0005.
[152] Dragos, page 2. https://www.regulations.gov/comment/ONCD-2023-0001-0081.
[153] BSA|The Software Alliance (BSA), page 2. https://www.regulations.gov/comment/ONCD-2023-0001-0047.
[154] The App Association, page 2. https://www.regulations.gov/comment/ONCD-2023-0001-0062.
[155] Microsoft, page 3. https://www.regulations.gov/comment/ONCD-2023-0001-0080.
[156] Microsoft, pages 1-2. https://www.regulations.gov/comment/ONCD-2023-0001-0080.
[157] Google, 3. https://www.regulations.gov/comment/ONCD-2023-0001-0058..
[158] SAP, page 3. https://www.regulations.gov/comment/ONCD-2023-0001-0036.
[159] The Information Technology Industry Council (ITI), page 8. https://www.regulations.gov/comment/ONCD-2023-0001-0048. he Information Technology Industry Council (ITI), page 8.
[160] Cybersecurity Coalition, page 5. https://www.regulations.gov/comment/ONCD-2023-0001-0065.
[161] BSA, page 3. https://www.regulations.gov/comment/ONCD-2023-0001-0047.
[162] Workday, page 3. https://www.regulations.gov/comment/ONCD-2023-0001-0014.
[163] BSA, page 2. https://www.regulations.gov/comment/ONCD-2023-0001-0047.
[164] Microsoft, page 3. https://www.regulations.gov/comment/ONCD-2023-0001-0080.
[165] Microsoft, page 3. https://www.regulations.gov/comment/ONCD-2023-0001-0080.
[166] Dragos, page 6. https://www.regulations.gov/comment/ONCD-2023-0001-0081.
[167] Workday, page 1. https://www.regulations.gov/comment/ONCD-2023-0001-0014.
[168] BSA, page 3. https://www.regulations.gov/comment/ONCD-2023-0001-0047.
[169] Nuclear Energy Institute (NEI), page 3. https://www.regulations.gov/comment/ONCD-2023-0001-0017.
[170] NEI, page 2. https://www.regulations.gov/comment/ONCD-2023-0001-0017.
[171] NEI, page 3. https://www.regulations.gov/comment/ONCD-2023-0001-0017.
[172] Airlines for America (A4A), page 3. https://www.regulations.gov/comment/ONCD-2023-0001-0086.
[173] Association of American Railroads (AAR), page 2. https://www.regulations.gov/comment/ONCD-2023-0001-0023.
[174] AAR, page 9. https://www.regulations.gov/comment/ONCD-2023-0001-0023.
[175] A4A, page 1. https://www.regulations.gov/comment/ONCD-2023-0001-0086.
[176] AAR, page 5. https://www.regulations.gov/comment/ONCD-2023-0001-0023.
[177] AAR, pages 8-9. https://www.regulations.gov/comment/ONCD-2023-0001-0023.
[178] AAR, pages 8-9. https://www.regulations.gov/comment/ONCD-2023-0001-0023.
[179] A4A, page 3. https://www.regulations.gov/comment/ONCD-2023-0001-0086.
[180] A4A, page 3. https://www.regulations.gov/comment/ONCD-2023-0001-0086.
[181] AAR, page 10. https://www.regulations.gov/comment/ONCD-2023-0001-0023.
[182] AAR, page 11. https://www.regulations.gov/comment/ONCD-2023-0001-0023.
[183] Internet Security Alliance (ISA), page 1. https://www.regulations.gov/comment/ONCD-2023-0001-0019.
[184] Business Roundtable (BRT), page 2. https://www.regulations.gov/comment/ONCD-2023-0001-0009.
[185] BRT, page 2. https://www.regulations.gov/comment/ONCD-2023-0001-0009.
[186] ISA, pages 1-2. https://www.regulations.gov/comment/ONCD-2023-0001-0019.
[187] ISA, page 1. https://www.regulations.gov/comment/ONCD-2023-0001-0019.

[188] BRT, page 2. https://www.regulations.gov/comment/ONCD-2023-0001-0009.
[189] U.S. Chamber of Commerce (Chamber), page 3. https://www.regulations.gov/comment/ONCD-2023-0001-0034.
[190] BRT, page 2. https://www.regulations.gov/comment/ONCD-2023-0001-0009.
[191] Professional Services Council (PSC), page 7. https://www.regulations.gov/comment/ONCD-2023-0001-0032.
[192] PSC, page 7. https://www.regulations.gov/comment/ONCD-2023-0001-0032.
[193] Chamber, page 4. https://www.regulations.gov/comment/ONCD-2023-0001-0034.
[194] Chamber, page 4. https://www.regulations.gov/comment/ONCD-2023-0001-0034.
[195] BRT, page 2. https://www.regulations.gov/comment/ONCD-2023-0001-0009.
[196] BRT, page 3. https://www.regulations.gov/comment/ONCD-2023-0001-0009.
[197] BRT, page 4. https://www.regulations.gov/comment/ONCD-2023-0001-0009.
[198] PSC, page 9. https://www.regulations.gov/comment/ONCD-2023-0001-0032.
[199] Chamber, page 5. https://www.regulations.gov/comment/ONCD-2023-0001-0034.
[200] Chamber, pages 8-9. https://www.regulations.gov/comment/ONCD-2023-0001-0034.
[201] Chamber, page 3. https://www.regulations.gov/comment/ONCD-2023-0001-0034.
[202] Chamber, page 12. https://www.regulations.gov/comment/ONCD-2023-0001-0034.
[203] DIGITALEUROPE, page 9. https://www.regulations.gov/comment/ONCD-2023-0001-0063.
[204] World Economic Forum (WEF), page 5. https://www.regulations.gov/comment/ONCD-2023-0001-0015.
[205] WEF, page 5. https://www.regulations.gov/comment/ONCD-2023-0001-0015.
[206] WEF, page 7. https://www.regulations.gov/comment/ONCD-2023-0001-0015.
[207] WEF, page 7. https://www.regulations.gov/comment/ONCD-2023-0001-0015.
[208] DIGITALEUROPE, pages 6-7. https://www.regulations.gov/comment/ONCD-2023-0001-0063.
[209] WEF, page 7. https://www.regulations.gov/comment/ONCD-2023-0001-0015.
[210] WEF, page 7. https://www.regulations.gov/comment/ONCD-2023-0001-0015.
[211] DIGITALEUROPE, page 6. https://www.regulations.gov/comment/ONCD-2023-0001-0063.
[212] DIGITALEUROPE, page 1. https://www.regulations.gov/comment/ONCD-2023-0001-0063.
[213] WEF, page 11. https://www.regulations.gov/comment/ONCD-2023-0001-0015.
[214] DIGITALEUROPE, pages 1-2. https://www.regulations.gov/comment/ONCD-2023-0001-0063.
[215] ISC2, page 8. https://www.regulations.gov/comment/ONCD-2023-0001-0056.
[216] Electronic Privacy Information Center (EPIC) and Consumer Reports, page ii. https://www.regulations.gov/comment/ONCD-2023-0001-0028.
[217] Aspen Digital, page 1. https://www.regulations.gov/comment/ONCD-2023-0001-0055.
[218] ISC2, page 5. https://www.regulations.gov/comment/ONCD-2023-0001-0056.
[219] ISC2, page 3. https://www.regulations.gov/comment/ONCD-2023-0001-0056.
[220] ISC2, page 5. https://www.regulations.gov/comment/ONCD-2023-0001-0056.
[221] ISC2, page 3. https://www.regulations.gov/comment/ONCD-2023-0001-0056.
[222] ISC2, page 5. https://www.regulations.gov/comment/ONCD-2023-0001-0056.
[223] ISC2, page 6. https://www.regulations.gov/comment/ONCD-2023-0001-0056.
[224] Aspen Digital, page 4. https://www.regulations.gov/comment/ONCD-2023-0001-0055.
[225] ISC2, pages 5-6. https://www.regulations.gov/comment/ONCD-2023-0001-0056.
[226] MITRE, pages 1-2. https://www.regulations.gov/comment/ONCD-2023-0001-0079.
[227] MITRE, page 1. https://www.regulations.gov/comment/ONCD-2023-0001-0079.
[228] MITRE, page 3. https://www.regulations.gov/comment/ONCD-2023-0001-0079.
[229] MITRE, pages 2-3. https://www.regulations.gov/comment/ONCD-2023-0001-0079.
[230] ISC2, page 8. https://www.regulations.gov/comment/ONCD-2023-0001-0056.
[231] EPIC and Consumer Reports, page 9. https://www.regulations.gov/comment/ONCD-2023-0001-0028.
[232] ISC2, page 9. https://www.regulations.gov/comment/ONCD-2023-0001-0056.
[233] ISC2, page 11. https://www.regulations.gov/comment/ONCD-2023-0001-0056.
[234] Center for Internet Security (CIS), pages 7–8. https://www.regulations.gov/comment/ONCD-2023-0001-0037.
[235] National Association of State Chief Information Officers (NASCIO), page 1. https://www.regulations.gov/comment/ONCD-2023-0001-0043.
[236] StateRAMP, page 1. https://www.regulations.gov/comment/ONCD-2023-0001-0038.
[237] NASCIO, page 1. https://www.regulations.gov/comment/ONCD-2023-0001-0043.
[238] NASCIO, page 1. https://www.regulations.gov/comment/ONCD-2023-0001-0043.

[239] NASCIO, page 2. https://www.regulations.gov/comment/ONCD-2023-0001-0043.
[240] National Association of Regulatory Utility Commissioners (NARUC), page 4. https://www.regulations.gov/comment/ONCD-2023-0001-0027.
[241] NARUC, page 4. https://www.regulations.gov/comment/ONCD-2023-0001-0027.
[242] NARUC, page 2. https://www.regulations.gov/comment/ONCD-2023-0001-0027.
[243] NARUC, pages 3-4. https://www.regulations.gov/comment/ONCD-2023-0001-0027.
[244] StateRAMP, page 10. https://www.regulations.gov/comment/ONCD-2023-0001-0038.
[245] StateRAMP, page 11. https://www.regulations.gov/comment/ONCD-2023-0001-0038.
[246] NARUC, page 4. https://www.regulations.gov/comment/ONCD-2023-0001-0027.
[247] StateRAMP, page 10. https://www.regulations.gov/comment/ONCD-2023-0001-0038.
[248] StateRAMP, page 11. https://www.regulations.gov/comment/ONCD-2023-0001-0038.