ITI Promoting Innovation Worldwide

Written Testimony of

John S. Miller
Senior Vice President of Policy and General Counsel
Information Technology Industry Council (ITI)

Before the

Committee on Oversight and Accountability
Subcommittee on Cybersecurity, Information Technology, and Government Innovation

United States House of Representatives

Enhancing Cybersecurity by Eliminating Inconsistent Regulations

July 25, 2024

Global Headquarters
700 K Street NW, Suite 600
Washington, D.C. 20001, USA
+1 202-737-8888

Europe Office
Rue de la Loi 227
Brussels - 1040, Belgium
+32 (0)2-321-10-90

info@itic.org
www.itic.org
@iti_techtweets

Written Testimony of
John S. Miller
Senior Vice President of Policy and General Counsel
The Information Technology Industry Council (ITI)

Before the

United States House of Representatives
Committee on Oversight and Accountability
Subcommittee on Cybersecurity, Information Technology, and Government Innovation

"Enhancing Cybersecurity by Eliminating Inconsistent Regulations"

July 25, 2024

Chairwoman Mace, Ranking Member Connolly, and Distinguished Members of the Subcommittee on Cybersecurity, Information Technology, and Government Innovation, thank you for the opportunity to testify today. My name is John Miller, Senior Vice President of Policy and General Counsel at the Information Technology Industry Council (ITI).[1]

I lead ITI's Trust, Data, and Technology policy team, including our work on cybersecurity, supply chain resiliency, privacy, artificial intelligence, data, and related policy issues in the United States (U.S.) and globally. I have deep experience working on public-private cyber, supply chain, and national security initiatives with the Cybersecurity and Infrastructure Security Agency (CISA) and other federal agencies in the United States. Currently, I serve as the Co-chair of the CISA-sponsored Information and Communications Technology Supply Chain Risk Management Task Force (ICT SCRM Task Force) and on the Executive Committee of the Information Technology Sector Coordinating Council (ITSCC), the principal IT sector partner to CISA on critical infrastructure protection and cybersecurity policy (after previously serving consecutive terms as ITSCC Chair). I have also previously served as a principal IT sector representative to the Enduring Security Framework, and on multiple National Security and Telecommunications Advisory Committee (NSTAC) subcommittees, most recently as an appointee to the Subcommittee on Addressing the Misuse of Domestic Infrastructure by Foreign Malicious Actors.

I am honored to testify this morning on "Enhancing Cybersecurity by Eliminating Inconsistent Regulations," a bipartisan issue which has been widely acknowledged by government and

[1] The Information Technology Industry Council (ITI) is the premier global advocate for technology, representing the world's most innovative companies. Founded in 1916, ITI is an international trade association with a team of professionals on four continents. We promote public policies and industry standards that advance competition and innovation worldwide. Our diverse membership and expert staff provide policymakers the broadest perspective and thought leadership from technology, hardware, software, services, manufacturing, and related industries. Visit https://www.itic.org/ to learn more.

industry stakeholders alike as deserving remedial action for well over a decade. ITI strongly supports efforts that seek to further regulatory harmonization and curtail the proliferation of divergent regulations.

ITI represents eighty of the world's leading information and communications technology (ICT) companies.[2] We promote innovation worldwide, serving as the ICT industry's premier advocate and thought leader in the United States and around the globe. ITI's membership comprises leading innovative companies from all corners of the technology sector, including hardware, software, digital services, semiconductor, network equipment, cloud, artificial intelligence (AI), cybersecurity and other internet and technology-enabled companies that rely on ICT to evolve their businesses. Our companies service and support the global ICT marketplace via complex supply chains in which products are developed, made, and assembled in multiple countries, and service customers across all levels of government and the full range of global industry sectors, including financial services, healthcare, and energy. We thus not only acutely understand the importance of cybersecurity as a global priority for governments, companies, and customers and critical to our collective security, but our members can also attest to the complexities of demonstrating compliance with diverging or duplicative regulations in the U.S. and around the world.

While ITI regularly engages on a full range of cybersecurity policy issues, of particular note for purposes of this hearing is our deep engagement on cybersecurity incident reporting in the U.S. and globally. ITI developed policy recommendations designed to help the U.S. Congress, CISA, and other government stakeholders develop an effective and efficient cybersecurity incident reporting regime, including to support the *Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA).* I had the privilege of testifying before the House Homeland Security Committee in support of that bill, and ITI has subsequently been deeply engaged in providing comments as part of CISA's ongoing rulemaking process to help make sure that important law is effectively implemented – and ideally, deconflicted with the over 50 existing or pending federal incident reporting requirements as well as similar requirements at the U.S. state level and internationally.

After briefly providing important context and background regarding the long history of and recent government efforts to address this problem, including in the area of security incident notification, the balance of my written testimony will focus on two areas that ITI believes are most worthy of the Committee's consideration of how it can best help harmonize federal cybersecurity regulations in the U.S.: 1) the costs of duplicative, contradictory and excessive regulations on both industry and government – and the benefits of regulatory streamlining; and (2) actionable recommendations that Congress and the broader U.S. Government, including

[2] Visit https://www.itic.org/about/membership/iti-members for a full list of ITI members.

independent regulatory agencies, can take to better streamline existing cybersecurity regulations and avoid a further worsening of the problem going forward.

There is a Strong, Longstanding, Widely Agreed-Upon Bipartisan Consensus on the Need to Harmonize Cybersecurity Regulations

The need to harmonize conflicting, divergent, duplicative, or excessive cybersecurity regulations has been recognized by a wide array of government and industry stakeholders as a priority issue in urgent need of attention over the past three U.S. presidential administrations.

Successive administrations have identified and prioritized the need for regulatory harmonization or streamlining. Section 10 of the Obama Administration's Executive Order 13636, *Improving Critical Infrastructure Cybersecurity,*[3] clearly contemplated regulatory harmonization, referencing opportunities that the *Cybersecurity Framework* (launched by that same EO) created for regulatory streamlining.[4] Though then White House cyber coordinator, Michael Daniel, indicated the Obama Administration was "beginning a process to identify federal regulations that are excessively burdensome, conflicting, or ineffective,"[5] we have found no evidence that any regulations were streamlined or otherwise eliminated as a result of those efforts or authorities.

Though not specific to cybersecurity, the Trump administration also took steps to examine and streamline regulations through two executive orders intended to 1) require elimination of two regulations for every new regulation and prudent cost management of planned regulations;[6] and 2) create regulatory reform officers within each agency to implement regulatory reform initiatives and policies, including reducing the number of regulations and controlling regulatory costs.[7] However, we have found no evidence that any excessive, duplicative, or conflicting cybersecurity regulations were eliminated or otherwise streamlined during the Trump administration either.

---

[3] Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*, February 12, 2013, https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.

[4] *Id.* EO 13636 requires that agencies "1) assess the sufficiency of existing regulatory authority to establish requirements based on the *Cybersecurity Framework* to address current and projected cyber risks; and 2) identify proposed changes in order to address insufficiencies identified."

[5] Michael Daniel, *Strengthening Cyber Risk Management,* February 2, 2015, *available at* https://obamawhitehouse.archives.gov/blog/2015/02/02/strengthening-cyber-risk-management.

[6] Executive Order 13771, *Reducing Regulation and Controlling Regulatory Costs*, January 30, 2017, https://trumpwhitehouse.archives.gov/presidential-actions/presidential-executive-order-reducing-regulation-controlling-regulatory-costs/

[7] Executive Order 13777, *Enforcing the Regulatory Reform Agenda*, February 24, 2017, https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/06/EO13777_EnforcingRegulatoryReformAgenda.pdf

The Biden administration, for its part, identified the need for regulatory harmonization as a priority in its National Cybersecurity Strategy[8] and Implementation Plan.[9] The Office of the National Cyber Director (ONCD) has taken initial steps to follow through, including to issue an RFI soliciting inputs on the need for cybersecurity regulatory harmonization, and a report summarizing those findings. Because ONCD's work is not yet done, it is premature to provide a "final" grade on the Biden administration's regulatory streamlining efforts. However, it is noteworthy that DoD introduced a Cybersecurity Reciprocity Playbook earlier this year[10] – a promising development that hopefully foreshadows additional efforts to make progress toward one of ITI's recommendations (*see* recommendation (d) at p. 11). Additionally, while the NCS addressed the need to harmonize cybersecurity regulations, it bears noting that the Biden administration has also issued executive actions such as Executive Order 14028 on *Improving the Nation's Cybersecurity* (EO 14028)[11] imposing additional cybersecurity requirements on companies, likely resulting in a net increase in cybersecurity regulations.

Congress has also long recognized the need to harmonize cybersecurity regulations. Congress has identified this issue as a priority dating back to at least 2017, when the Senate Committee on Homeland Security and Governmental Affairs held a hearing on "Cybersecurity Regulation Harmonization."[12] More recently, Congress anticipated the problem of potential cybersecurity over-regulation in the area of cyber incident reporting, calling for DHS to establish the Cyber Incident Reporting Council (CIRC) to study the issue and make actionable recommendations. Established as part of*CIRCIA*, the CIRC produced its first report last September assessing **over 50** in effect or pending federal cyber incident reporting requirements. Finally, just yesterday, HSGAC marked up a bill addressing the exact same topic that we are discussing here today – S. 4630, *The Streamlining Federal Cybersecurity Regulations Act*. The bill calls on the National Cyber Director (NCD) to establish an interagency committee to harmonize *all* cybersecurity regulatory regimes in the U.S. and, importantly, does not exempt the CIRC from its scope,

---

[8] ONCD, National Cybersecurity Strategy, March 1, 2023, https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

[9] ONCD, National Cybersecurity Strategy Implementation Plan, Version 2, May 2024 https://www.whitehouse.gov/wp-content/uploads/2024/05/National-Cybersecurity-Strategy-Implementation-Plan-Version-2.pdf

[10] DOD, Cybersecurity Reciprocity Playbook, Version 1, March 2024, https://dodcio.defense.gov/Portals/0/Documents/Library/(U)%202024-01-02%20DoD%20Cybersecurity%20Reciprocity%20Playbook.pdf

[11] Executive Order 14028 on Improving the Nation's Cybersecurity (May 12, 2021), https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

[12] U.S. Senate Committee on Homeland Security and Government Affairs, Full Committee Hearing, "Cybersecurity Regulation Harmonization," June 21, 2017. ITI testified at this hearing. *See* Testimony of Dean C. Garfield on Cybersecurity Regulation Harmonization, https://www.hsgac.senate.gov/wp-content/uploads/imo/media/doc/Testimony-Garfield-2017-06-21-REVISED.pdf

illustrating Congress' understanding that this problem cannot be addressed in a piecemeal fashion.

Regulatory Developments Around Cyber Incident Reporting Illustrate that the Problem is Getting Worse. To its credit, the CIRC report also included several actionable recommendations for streamlining these dozens of cyber incident reporting requirements, although it is not clear any of those recommendations has yet to be implemented, or that any existing duplicative or contradictory regulations have been streamlined or eliminated as result of the CIRC's work. While we strongly support the harmonization of incident reporting requirements and encourage ONCD to consult with the CIRC to coordinate a consistent interagency approach to regulatory harmonization, we note that regulatory harmonization can only succeed if regulators coordinate their actions. Unfortunately, the Federal Acquisition Regulatory (FAR) Council proposed and continues to pursue a rule[13] on federal incident reporting requirements that ignored several of the CIRC's positive recommendations, including that that agencies should use the report's model language and model reporting timeline, instead introducing its own unique requirements. This is not only problematic given the FAR council's control over federal agencies but is symptomatic of the Kafkaesque reality that regulations only seem to multiply over time and are never eliminated, making fragmentation worse and placing harmonization further out of reach.

The deluge of cybersecurity incident notification regulations perfectly illustrates the scope of the over-regulation problem and serves as a reminder that, to date, while we have studied the issue for years, not much has been done to drive actionable solutions – to actually harmonize cybersecurity regulatory requirements.

The Costs of Duplicative, Inconsistent, or Conflicting Cybersecurity Regulations are Widely Acknowledged and Real

Diverging regulations negatively impact private sector organizations and federal agencies alike. In contrast, the benefits of regulatory harmonization or streamlining are clear.

(a) Costs to Industry

The ONCD RFI referenced earlier appropriately captures well the negative impacts on industry:

> *When cybersecurity regulations of the same underlying technology are inconsistent or contradictory – or where they are duplicative but enforced differently by different regulators – consumers pay more, and our national security suffers. Duplicative regulation leads to companies focusing more on compliance than on security, which results in their passing higher costs on to customers, working families, and state, local,*

[13] DOD, GSA, and NASA, Federal Acquisition Regulation: Cyber Threat Incident Reporting and Information Sharing, October 3, 2023, https://www.federalregister.gov/documents/2023/10/03/2023-21328/federal-acquisition-regulation-cyber-threat-and-incident-reporting-and-information-sharing

Tribal, and territorial governments. Harmonizing baseline regulatory requirements can therefore produce better security outcomes at lower costs.[14]

ONCD correctly identifies the primary cost to business arising from unharmonized regulations as the increased compliance burden on companies. At the top line, these compliance costs take away companies' limited resources from cyber defense activities and technological innovation and instead require them to engage in a wide range of compliance-oriented activities. These costs include a wide range of administrative activities that range from keeping pace with a dynamic, mushrooming, and fragmented regulatory environment, including by identifying which new requirements apply to their specific business contexts, and determining how new requirements potentially conflict with or overlap with existing requirements; undertaking various recordkeeping activities to document their compliance with various regulatory requirements; monitoring the impact of new regulations on third-party relationships involving service providers and others in sometimes vast global supply chains, and modifying relevant contracts to keep pace; and potentially reengineering products or services to comply with new regulations, rather than innovating new technology solutions. While all of these compliance costs associated with unharmonized cybersecurity regulations are significant even for the largest global corporations, such costs disproportionately impact small and medium-sized businesses who typically lack the resources necessary even to do the bare minimum, such as monitoring which new regulations they must comply with. This is a significant disincentive for those innovative businesses to engage with heavily regulated sectors, including the government itself.

When we layer on the reality that most companies are also encountering conflicting or duplicative cybersecurity regulations – particularly in active areas such as cyber incident reporting – at the U.S. state level and internationally, it reveals why the status quo is untenable for companies large and small alike.

(b) Costs to Government

While not the principal focus of this hearing, we encourage subcommittee members to also take note of the impacts of unharmonized, fragmented, duplicative cybersecurity regulations and requirements on federal government stakeholders.

ONCD and other stakeholders have noted the cybersecurity workforce shortage globally, in the U.S., and across the federal government. By one accounting, the current number of vacant cybersecurity positions in the U.S. is currently approaching half a million.[15] In light of these persistent cybersecurity workforce challenges, it seems highly inefficient to devote scarce

[14] Request for Information on Cybersecurity Regulatory Harmonization, Office of the National Cyber Director, [Docket ID Number: ONCD-2023-0001], July 19, 2023, https://www.whitehouse.gov/wp-content/uploads/2023/07/ONCD-Reg-Harm-RFI-Final-July-19.2023.pdf

[15] Cybersecurity Supply/Demand Heat Map, Cyberseek, https://www.cyberseek.org/heatmap.html

government cybersecurity resources – including government regulatory capacity – to create and enforce duplicative regulatory requirements that address common underlying cybersecurity issues or technologies. To reiterate a point I made earlier – it seems like we perpetually add new cybersecurity regulations and requirements, but never streamline or eliminate duplicative or conflicting requirements. Doing directly impacts government resources, in addition to those in the private sector, not only with respect to the rulemaking process itself but also in the areas of enforcement, guidance and oversight.

Federal agencies, however, are additionally impacted by duplicative regulations in the same ways that private sector companies are – in terms of their own cybersecurity compliance activities. For example, the Federal Bureau of Investigation (FBI) has to comply with cybersecurity requirements for the Department of Justice and Federal Civilian Agencies, the Intelligence Community, and its own Criminal Justice standards for the sharing of law enforcement information with state and local agencies. This siphons resources away from security outcomes and towards compliance, auditing, and duplicative copy requirements. Other agencies have similar challenges.

(c) Benefits of Regulatory Harmonization

Regulatory harmonization can drive positive outcomes across stakeholder groups and create a win-win situation. Organizations, both public and private, may benefit from regulatory harmonization through the freeing up of resources that can be allocated towards driving security outcomes and innovation. By extension, this benefits consumers for whom harmonization will result in more consistent cyber protections. Federal agencies may also benefit from improved mission delivery and constituent services, while private sector organizations may find it easier to compete for business in regulated markets and engage in international trade. Streamlined and harmonized regulations across federal agencies would also yield cost savings to the government.

Recommendations to Support Regulatory Streamlining and Avoid Worsening Regulatory Fragmentation

ITI offers several recommendations designed to support regulatory harmonization, including streamlining existing regulations, and avoiding worsening regulatory fragmentation going forward.

(a) ONCD Should Follow Through on its Ongoing Study of the Cybersecurity Harmonization to Drive Actionable Solutions, including Coordination of Ongoing and Future Cybersecurity Regulatory Activity

ONCD's work thus far to implement the recommendations in the National Cybersecurity Strategy regarding cybersecurity regulatory harmonization can best be described as helpful, but preliminary. While careful study of the existing cybersecurity regulatory environment is a necessary precursor to driving meaningful change, including harmonizing existing contradictory

regulations or eliminating needlessly duplicative regulations, ONCD must follow up on this ongoing work to drive forward an actionable plan to harmonize existing cybersecurity regulations and hold federal agencies accountable for their own regulatory streamlining activities. ONCD fulfilling this mandate could include holding DHS/CIRC accountable for implementing the CIRC recommendations for harmonizing cyber incident notification regulations.

In fact, the CIRC report does contain several recommendations that could be useful to more broadly drive harmonization of cybersecurity regulations beyond the incident reporting context. We strongly support the harmonization of incident reporting requirements and encourage ONCD to consult with the CIRC to coordinate a consistent interagency approach to regulatory harmonization. The CIRC may additionally provide helpful lessons learned for building out a broader entity that is focused on streamlining federal cybersecurity requirements beyond incident reporting. For example, the CIRC's oversight authorities ought to be revised and harmonized vis-à-vis other government agencies' oversight roles for specific entities to avoid duplicative oversight.

At the same time, regulatory harmonization can only succeed if regulators coordinate their actions. As noted above, the fact that the FAR Council decided to issue a proposed rule on federal incident reporting requirements that ignored the CIRC report's recommendations illustrates the need for directive coordination. ONCD is well positioned to drive such improved coordination among regulators and to hold them accountable for following through.

(b) Orient Alignment of Current and Future Regulatory Efforts Around the Common Taxonomy Provided by the NIST Cybersecurity Framework 2.0

We should collectively work to align existing and future cybersecurity regulations around a common taxonomy including definitions and risk-management controls grounded in consensus-based international standards. NIST has recently revised its seminal Cybersecurity Framework, a voluntary, risk-based framework grounded in consensus international cybersecurity standards that has been widely adopted by industry and government organizations alike, issuing a version 2.0 earlier this year. The potential of the Framework to provide a common taxonomy for policymakers domestically and globally has yet to be fully realized. Amongst its many attributes, the Framework has long been regarded as providing a common language for cybersecurity risk management taxonomy that can be effectively used by not only by organizations seeking to better manage cybersecurity risks but policymakers globally and at all levels of U.S. government.

Any cybersecurity streamlining effort must foundationally recognize that it is counterproductive to create siloed, agency-specific, or country-specific approaches to cybersecurity, so the federal government should promote polices that help break down these and other artificial barriers that hinder cybersecurity efforts. Unfortunately, without a common lexicon for cybersecurity and risk

management efforts, federal, state, local, and international governments will continue to create separate approaches to cybersecurity that ultimately lead to greater insecurity for governments, consumers, and private industry. Thus, in our view the Cybersecurity Framework provides the surest substantive footing for streamlining cybersecurity regulations and so and can serve as a productive orientation point for federal harmonization efforts.

Additionally, to facilitate clear and consistent communications among stakeholders, we believe a common set of terms and definitions is needed when analyzing and describing relationships between standards and regulations. Definitions tend to be provided for each standard or regulation which complicates the harmonization process. To overcome this piecemeal approach, we recommend the development of a common set of baseline terms in partnership with industry.

In February 2024, NIST published IR 8477, which proposes a standardized approach for mapping the elements of documentary standards, regulations, frameworks, and guidelines to one another. The objective of this workstream is to establish a single concept system over time that links cybersecurity and privacy concepts from many sources into a cohesive, consistent set of relationship mappings within the NIST Cybersecurity and Privacy Reference Tool (CPRT). While this effort falls short of standardizing the definitions and terminology, it describes a potentially helpful taxonomy to describe the relationship styles between multiple standards, regulations, and frameworks that could be leveraged for the purposes of this RFI. For example, conducting a supportive relationship mapping between sector-specific regulations could help with the identification of supporting, identical, or equivalent concepts. These insights, in turn, could be leveraged to identify and prioritize areas for regulatory and standards harmonization.

(c) Define A Standardized Clearing Process for New Cybersecurity Regulations to Prevent Future Fragmentation

While it is important to structure and harmonize existing regulations, it is equally important to develop a review process that prevents future fragmentation. The federal government has existing processes in place that could be expanded for this purpose. According to its own website, the Office of Information and Regulatory Affairs within the White House (OIRA) is “the United States Government’s central authority for the review of Executive Branch regulations, approval of Government information collections, establishment of Government statistical practices, and coordination of Federal privacy policy.” One possibility is that OIRA’s role could be expanded to develop a clear and consistent model for assessing the cost of cyber regulations, and to review sector-specific regulations for inconsistencies. They should hire specialists in technology to ensure there is adequate in-house technical expertise present in the organization. This may require legislative action and/or the provision of sufficient funding to support the expansion in scope, to acquire the needed expertise and to avoid regulatory bottlenecks.

(d) Develop and Implement a Structured Reciprocity Process Anchored in Baseline Standards, Frameworks, and Risk-Management Controls Across Federal Government Regulations and Assessments

ONCD should develop and implement a structured reciprocity process anchored in baseline controls and standards across federal government regulations and assessments to reduce barriers and clarify obligations. Reciprocity among federal agency requirements is critical for reducing redundant compliance costs on industry and is particularly important in areas such as cloud security.

One strategy to consider to drive reciprocity is to create and maintain a centralized repository of risk profiles. Agency regulators will have different risk profiles and risk tolerances based on the sector over which they have authority or will otherwise identify that they are adding new requirements based on specific threats. Further, different industry sectors have different historical and current experiences with regulation. While this may be the case, ONCD can work with NIST and CISA to establish consistent definitions for risk. Overly prescriptive requirements will not keep pace with technological developments and will quickly become obsolete. Regulators should develop a common understanding of what constitutes "reasonable security" from a principles and risk-based perspective.

Once such government-wide definitions are available, work can begin to define security control baselines for each risk level. These control baselines should be based on NIST SP 800-53, which is a widely accepted standard and already serves as the basis for Federal Information Security Modernization Act (FISMA) compliance and the backbone of the Federal Risk and Authorization Management Program (FedRAMP). Public Law 113-283, "Federal Information Security Modernization Act of 2014" requires that agencies protect government information and assets from unauthorized access, use, disclosure, disruption, modification, or destruction. Subsequently, NIST 800-53, "Security and Privacy Controls for Information Systems and Organizations," is the standard that contains the individual security controls required for agencies to comply with FISMA. The control family is widely used and managed across some of the leading global technology companies due to their existing business with the U.S. Federal Government.

The exercise of defining risk-based security baselines could build on the work that NIST has been doing on NIST IR 8477 and making security controls accessible through the CPRT. Like the NIST Risk Management Framework (RMF) control overlay repository, agencies could submit risk profiles or overlays which in turn should be evaluated for consistency before being approved, possibly by conducting a mapping exercise as described in NIST IR 8477. The proposing agency should face the burden of proof to plausibly demonstrate what additional risk warrants the creation of a new overlay. Agency regulator participation should be mandatory. When an entity is subject to multiple regulators (e.g., a sectoral entity, such as a financial institution), there should be one designated primary regulator for that entity, and either a carve out in the

remaining applicable regulations and/or a deferral from the other applicable regulators. The creation and ingestion of artifacts should rely on automated and machine-readable tools. FedRAMP has already done a lot of good work on promoting the adoption of OSCAL (Open Security Controls Assessment Language), which could serve as inspiration of how to structure such a reciprocity framework. This could also help with the monitoring of a system's cybersecurity posture.

(e) Consider Regulatory Harmonization When Updating Existing Guidance

Technological developments will necessitate updates to existing guidance documents. As policymakers review these documents, they should think about the impact of changes on the regulatory landscape. Integrating regulatory harmonization considerations into the review process will minimize the risk of unintended consequences on downstream adoption. For example, as the Administration reviews and revises Presidential Policy Directive 21 (PPD-21), it should think about the relationship between critical infrastructure entities and their respective service providers and how that might translate into a revision.

While critical infrastructure entities may be directly regulated, it does not make sense to also regulate their service providers. Further, regulators should avoid regulating both entities and their service providers as this creates confusion in roles and responsibilities, and results in a lack of accountability. Regulators should directly regulate the entity, who can cascade requirements to its service providers via contract, as necessary. Relatedly, regulators should not require service providers to report on their clients. This can also result in redundant and conflicting reporting.

For instance, when a critical infrastructure entity is using a cloud service, the critical infrastructure entity, and not the cloud service provider, should be directly regulated. Cloud relies on a shared responsibility model for cybersecurity. Regulators should allow cloud clients and service providers to identify and delegate such responsibility, accordingly.

(f) Leverage Internationally Recognized, Voluntary Standards as the Basis for Cybersecurity Regulations

While harmonizing the domestic regulatory landscape is important, the effort cannot stop there. Adopting or otherwise seeking to align with international standards will be just as important as harmonizing regulations, helping to drive interoperability, ease compliance burdens, and improve market access. Companies benefit from adopting globally recognized, voluntary, consensus-based standards, such as ISA/IEC 62443 or the ISO 27000 series, as they provide a basis for interoperability and assurances for customers about expected levels of quality or service that jurisdictions around the world endorse. We are also pleased to see the NIST Cybersecurity Framework (CSF) develop additional crosswalks to other Frameworks while continuing to leverage international standards as the basis for implementing various outcomes.

We recommend the U.S. Government provide robust support to strengthen the private sector-led U.S. standardization system and promote U.S. stakeholders' leadership and participation in international standardization and conformity assessment systems. This type of engagement will also help to identify areas where there are gaps in or an otherwise identified need for standardization, for example on discrete elements of emerging technologies.

(g) Seek to Drive Harmonization of Cybersecurity Regulations Across Borders

Building on the above, it is important that in seeking to streamline regulatory requirements in the United States, the Administration also considers the existing cybersecurity requirements of other countries. The same applies to the supervisory compliance obligations for regulated industries. As noted, our members operate globally and are therefore subject to the requirements of other countries, in addition to those in the United States. Because cybersecurity is a global imperative and cyberspace is borderless, it is critical that the United States seeks to better align regulatory approaches across national borders. Globally recognized, voluntary, consensus-based standards that are already widely adopted by companies around the world should serve as the basis for international regulatory alignment.

(h) Promote Cultural Change by Enforcing Accountability to Drive Regulatory Harmonization

Today, the risk owners, be they sector regulating agencies responsible for individual sector cybersecurity risk, or federal CIOs responsible for federal agency risk, are individually responsible for making risk management decisions. They are therefore incentivized to make independent decisions about implementing security requirements and/or interpreting compliance with technical controls, instead of allowing for reciprocity or ensuring consistency. Instead, ONCD should hold regulators accountable to using the consistent standards and definitions proposed above. For instance, if FISMA is implemented via NIST 800-53, it would be useful for other entities to ensure that the same control family is referenced in their controls. Regulators and risk owners should only be able to adopt new and different control processes (including demonstrations of compliance) if they have demonstrated that the existing standards and processes are insufficient to meet their risks. And in those cases, they should still be required to minimize any new requirements and demonstrate the easiest way that entities can comply with new requirements by building on top of what already exists. Further, we believe if there are multiple applicable regulations and/or frameworks, adherence to one should constitute a good faith effort and provide liability exemption under the others. We recommend the inclusion of this discussion in the forthcoming software liability forum that was outlined in Strategic Initiative 3.3.1 of the National Cybersecurity Strategy Implementation Plan.

(i) Support a Unified Approach to Cybersecurity Regulation Across Federal, State, Local, Tribal, and Territorial Governments

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.

Federal regulations preempting state laws ensure a single, comprehensive set of rules that can be consistently applied across the country, providing industry and government with a clear and predictable regulatory landscape. ITI supports collaborative efforts between federal, state, and local entities in order to strike the right balance between a unified approach and the unique needs of local communities, which will ultimately enhance our nation's cybersecurity posture.

For instance, the Federal Bureau of Investigation's (FBI) Criminal Justice Information Services (CJIS) Security Policy is a key resource governing the storage, processing, and handling of Criminal Justice Information (CJI). However, states in particular have developed different expectations surrounding CJIS Security Policy compliance over time, leading to onerous compliance obligations for companies that operate nationally. A single standard or structured reciprocity process would reduce barriers, clarify obligations, enhance privacy, and generally speed the adoption of innovative technologies.

(j) Congress must help drive regulatory harmonization by legislating any needed incremental authorities and providing more precise regulatory authorities and direction to federal agencies in a post-*Chevron* world

Congress should seize the opportunity to drive actionable cybersecurity harmonization solutions and use its oversight authorities to make sure that the current and future administrations follow through. As I mentioned at the outset of my testimony, even though the Obama, Trump, and Biden administrations all set a policy direction to identify federal regulations that are excessively burdensome, conflicting, or ineffective, we as a community have yet to take meaningful action to realize that goal. We applaud this subcommittee for tackling this issue today and commend Senators Peters and Lankford for their work on the "Streamlining Federal Cybersecurity Regulations Act," which will take the important step of empowering the NCD to help us collectively stop admiring the problem and start taking action.

Beyond further empowering ONCD and providing authorization wherever else it is needed to support our harmonization recommendations, Congress should consider the potential impacts of the Supreme Court's recent decision in *Loper Bright Enterprises v. Raimondo (Loper Bright)* on its efforts to draft cybersecurity legislation going forward. *Loper Bright* overturned the longstanding doctrine known as *Chevron* deference, which required federal courts to defer to a federal agencies' reasonable interpretations of ambiguous statutory language. One clear impact

of *Loper Bright* is that Congress will be well advised to write clearer, more precise laws (in cybersecurity and other areas) and, where regulations are anticipated, to grant specific, directive, rulemaking authorities to the federal agencies who will be called on to enforce those regulations. We should be clear-eyed that Congress will likely have to obtain additional expertise and resources as it takes on a more expansive role in this regard.

Conclusion

Members of the Subcommittee, ITI once again commends you for your focus on the critical issue of enhancing cybersecurity by eliminating inconsistent regulations and is pleased you are considering our recommendations for driving harmonization of federal cybersecurity regulations and requirements.

This Congress and administration have an opportunity to complete what prior administrations and Congresses have not—to not only identify ineffective, duplicative, or unnecessarily burdensome cybersecurity regulations but also take tangible actions to eliminate them. It is past time that we stop admiring the problem and commit to doing something about it, and we stand ready to work with Congress and the administration to effect meaningful progress on this longstanding issue.

I again thank the Chairwoman, Ranking Member, and Members of the Committee for inviting me to testify today and for your interest in and examination of this important issue. I look forward to your questions.

Thank you.