ENHANCING CYBERSECURITY BY ELIMINATING INCONSISTENT REGULATIONS

HEARING

BEFORE THE

SUBCOMMITTEE ON CYBERSECURITY, INFORMATION TECHNOLOGY, AND GOVERNMENT INNOVATION

OF THE

COMMITTEE ON OVERSIGHT AND ACCOUNTABILITY

HOUSE OF REPRESENTATIVES

ONE HUNDRED EIGHTEENTH CONGRESS

SECOND SESSION

JULY 25, 2024

Serial No. 118–126

Printed for the use of the Committee on Oversight and Accountability

Available on: *govinfo.gov*
oversight.house.gov or
docs.house.gov

U.S. GOVERNMENT PUBLISHING OFFICE
56–568 PDF WASHINGTON : 2024

COMMITTEE ON OVERSIGHT AND ACCOUNTABILITY

JAMES COMER, Kentucky, Chairman

Jim Jordan, Ohio
Mike Turner, Ohio
Paul Gosar, Arizona
Virginia Foxx, North Carolina
Glenn Grothman, Wisconsin
Michael Cloud, Texas
Gary Palmer, Alabama
Clay Higgins, Louisiana
Pete Sessions, Texas
Andy Biggs, Arizona
Nancy Mace, South Carolina
Jake LaTurner, Kansas
Pat Fallon, Texas
Byron Donalds, Florida
Scott Perry, Pennsylvania
William Timmons, South Carolina
Tim Burchett, Tennessee
Marjorie Taylor Greene, Georgia
Lisa McClain, Michigan
Lauren Boebert, Colorado
Russell Fry, South Carolina
Anna Paulina Luna, Florida
Nick Langworthy, New York
Eric Burlison, Missouri
Mike Waltz, Florida

Jamie Raskin, Maryland, *Ranking Minority Member*
Eleanor Holmes Norton, District of Columbia
Stephen F. Lynch, Massachusetts
Gerald E. Connolly, Virginia
Raja Krishnamoorthi, Illinois
Ro Khanna, California
Kweisi Mfume, Maryland
Alexandria Ocasio-Cortez, New York
Katie Porter, California
Cori Bush, Missouri
Shontel Brown, Ohio
Melanie Stansbury, New Mexico
Robert Garcia, California
Maxwell Frost, Florida
Summer Lee, Pennsylvania
Greg Casar, Texas
Jasmine Crockett, Texas
Dan Goldman, New York
Jared Moskowitz, Florida
Rashida Tlaib, Michigan
Ayanna Pressley, Massachesetts

Mark Marin, Staff Director
Jessica Donlon, Deputy Staff Director and General Counsel
Peter Warren, Senior Advisor
Raj Bharwani, Senior Professional Staff Member
Lauren Lombardo, Senior Policy Analyst
Ellie McGowan, Staff Assistant and Administrative Clerk

Contact Number: 202-225-5074

Julie Tagen, Minority Staff Director
Contact Number: 202-225-5051

Subcommittee on Cybersecurity, Information Technology, and Government Innovation

Nancy Mace, South Carolina, Chairwoman

William Timmons, South Carolina
Tim Burchett, Tennessee
Marjorie Taylor Greene, Georgia
Anna Paulina Luna, Florida
Nick Langworthy, New York
Eric Burlison, Missouri
Vacancy
Vacancy

Gerald E. Connolly, Virginia *Ranking Minority Member*
Ro Khanna, California
Stephen F. Lynch, Massachusetts
Kweisi Mfume, Maryland
Jared Moskowitz, Florida
Ayanna Pressley, Massachesetts
Vacancy

C O N T E N T S

	Page
Hearing held on July 25, 2024	1

Witnesses

Mr. John Miller, Senior Vice President of Policy, Trust, Data, and Technology, Information Technology Industry Council	
Oral Statement	5
Ms. Maggie O'Connell, Director of Security, Reliability, and Resilience, Interstate Natural Gas Association of America	
Oral Statement	7
Mr. Patrick Warren, Vice President of Regulatory Technology, Bank Policy Institute	
Oral Statement	8
Dr. Charles Clancy, Chief Technology Officer, MITRE	
Oral Statement	10

Written opening statements and statements for the witnesses are available on the U.S. House of Representatives Document Repository at: docs.house.gov.

Index of Documents

* Statement for the Record; submitted by Rep. Connolly.

* Letter, July 31, 2024, from BSA to the Subcommittee; submitted by Rep. Mace.

* Statement, July 25, 2024, from Jason Healy to HCOA; submitted by Rep. Connolly.

* Statement, July 25, 2024; submitted by Rep. Mace.

* Statement, July 25, 2024, Airlines for America; submitted by Rep. Mace.

Documents are available at: docs.house.gov.

ENHANCING CYBERSECURITY BY ELIMINATING INCONSISTENT REGULATIONS INCONSISTENT REGULATIONS

Thursday, July 25, 2024

HOUSE OF REPRESENTATIVES
COMMITTEE ON OVERSIGHT AND ACCOUNTABILITY
SUBCOMMITTEE ON CYBERSECURITY, INFORMATION TECHNOLOGY,
AND GOVERNMENT INNOVATION
Washington, D.C.

The Subcommittee met, pursuant to notice, at 9:06 a.m., in room 2154, Rayburn House Office Building, Hon. Nancy Mace [Chairwoman of the Subcommittee] presiding.

Present: Representatives Mace, Burchett, Burlison, and Connolly.

Ms. MACE. Good Thursday morning. The Subcommittee on Cybersecurity, Information Technology, and Government Innovation will now come to order. And welcome everyone.

Without objection, the Chair may declare a recess at any time. And I recognize myself for the purpose of making an opening statement.

Good morning, and welcome to this hearing. Malicious cyberattacks on our Nation's critical infrastructure are increasing in frequency and scale. These attacks can create damaging disruptions and compromise highly sensitive data.

Much of our critical infrastructure is owned and operated by private sector companies. That includes transportation networks, energy production and distribution facilities, and the defense industrial base. Cyberattacks targeting such operations threaten our homeland security and our national security. That is why we need a strong partnership between the government and private operators of critical infrastructure.

Unfortunately, Federal regulations intended to mitigate cybersecurity risk often subject key industry participants to overlapping and inconsistent requirements. This creates an inefficient regulatory regime. The cost and burden of compliance is high. Companies are forced to divert resources away from cybersecurity enhancements to check various unnecessary compliance boxes. The unnecessary drain on resources also reduces the competitiveness of these businesses.

Regulations can proliferate out of control when multiple agencies are issuing rules on the same topic. A single company operating across critical sectors might need to comply with overlapping, inconsistent cybersecurity rules issued by a half dozen different agencies. Good luck with that.

So, it is not surprising that companies are feeling besieged by the growing barrage of cybersecurity requirements.

In March of last year, the then-acting White House Cyber Director appeared before this Subcommittee to discuss the Administration's National Cybersecurity Strategy. She testified that day that under the strategy, her office and the Office of Management and Budget were jointly responsible for addressing this issue of cybersecurity regulatory harmonization.

A few months later, her office issued a request for information asking critical sector operators to identify conflicting and mutually exclusive or inconsistent regulations and describe the burden that they impose.

The RFI describes the goal of harmonization, reciprocity in the regulation. An illustration of harmonization would be multiple Federal agencies agreeing on allowable forms of multifactor authentication to access IT systems. Reciprocity would mean that if one regulator found a company's multifactor authentication was being appropriately used on an IT system, another regulator could accept that find instead of doing its own independent assessment.

Unfortunately, judging from the response to the RFI, we have a long way to go to achieve harmonization and reciprocity.

The more than 100 respondents—a few of whom we will hear from today—describe a highly inefficient regulatory regime that detracts from cybersecurity outcomes by unnecessarily consuming scarce resources. Some of the respondents noted that state-level and international cybersecurity regulations contribute further to the regulatory morass they must investigate.

The upshot, according to the Financial Services Sector Coordinating Council, is that many company Chief Information Security Officers spend as much as half their time on regulatory compliance instead of upgrading their cybersecurity's posture.

In all, the administration received more than 2,000 pages of comments to its RFI.

I appreciate the Administration took the trouble to seek out the views of the affected parties, but the responses, thousands of them, show how challenging it will be to address the problem.

One thing seems clear: strong, centralized leadership from the Executive Office of the President will be required to harmonize cybersecurity regulations. That is the only way to put a check on regulators within the bureaucracy who may be blind to the broader impact of rules they issue.

I look forward to hearing from our witnesses today who will provide valuable insight on this problem from the perspective of different critical sectors. But before I introduce them, I am going to yield to the Ranking Member Connolly for 5 minutes.

Mr. CONNOLLY. Thank you.

And Madam Chairwoman, I would ask unanimous consent to enter into the record, at the appropriate time, a statement from—a thoughtful statement from Professor Jason Healey of Columbia School of International and Public Affairs.

Ms. MACE. Without objection.

Mr. CONNOLLY. I thank the Chair.

Cyberattacks on government agencies, businesses critical infrastructure, and private citizens have become alarmingly frequent and sophisticated. The cost of these attacks financially and in terms of national security is staggering.

According to data from the Federal Bureau of Investigation and the International Monetary Fund, the average annual cost of cybercrime worldwide is expected to reach $23 trillion by 2027, that is with a T.

Ransomware attacks against these sectors, for example, increased by more than 50 percent in 2023 alone. Federal agencies reported more than 32,000 cybersecurity incidents in Fiscal Year 2023. That is an increase of nearly 10 percent compared to the previous year.

In addition, the FBI's Internet Crime Complaint Center received more than 880,000 phishing, personal data breach, and other complaints in 2023.

As I stated in previous hearings held by this Subcommittee, data breaches and cyberattacks are no longer novel. That is why securing the systems that are the backbone of the U.S. economy is essential and fundamental both to the public and private sectors. To this end, the Federal Government has a responsibility to improve its cybersecurity outcomes.

To combat cyber threats, Federal agencies conduct comprehensive and multilayered processes to set and enforce cybersecurity requirements across components of our critical infrastructure, such as banks, water treatment plants, and telecommunication infrastructure. For example, the Federal Information Security Management Act and executive orders like Executive Order 14028 on Improving the Nation's Cybersecurity enacted after the Russian foreign intelligence service perpetrated the SolarWinds cybersecurity attack, they mandate specific cybersecurity practices. Among those are agencywide cybersecurity programs and risk assessments, incident response protocols, multifactor authentication, and improved event logging.

As National Cyber Director Harry Coker testified in January, there is a clear need for mandatory cybersecurity requirements for critical infrastructure. No fooling. However, Congress and the Administration must not lose sight of our responsibility to improve cybersecurity outcomes, and input from GAO, industry, civil society, and state and local partners indicate that existing regulations vary widely across many sectors and, at times, conflicting parameters.

This patchwork approach often leaves private, state, and local entities charged with securing critical infrastructure investing less in our collective goal of improving cybersecurity outcomes and more in compliance checking activities, putting national security and economic stability at some risk.

The Biden-Harris Administration recognized the need to address the overlapping nature of much needed cybersecurity regulations by launching efforts to deconflict and clarify cybersecurity requirements. In March 2023, the National Cyber Director released the National Cybersecurity Strategy, which listed harmonizing regulations to reduce the burden of compliance as one of the stated policy goals.

In August 2023, the ONCD issued a request for information from industry and other partners on the challenges with regulatory overlap and to explore framework for baseline cybersecurity requirements.

All our witnesses here today provided comments and feedback to the ONCD underscoring the Biden-Harris Administration's collaborative efforts with industry experts to get this right.

In May of this year, the Office of National Cyber Director also released the first-of-its-kind report on the cybersecurity posture of the United States. The report assesses the cybersecurity posture, the effectiveness of cyber policy and strategy, and the status of the implementation of national cyber policy and strategy by Federal departments and agencies.

Among the highlights of that report are actions taken by the Federal Government during the previous year. Establishing and using cyber requirements to protect critical infrastructure, including through the development and harmonization of regulatory requirements, is the first action listed in the report, which just goes to show how important the priority has been for this Administration.

I look forward to hearing today especially from Dr. Charles Clancy, a Senior Vice President and CTO at MITRE Corporation, about how Congress can support the efforts underway to achieve regulatory harmonization.

The goal is to maintain clear and consistent guidance when it comes to cybersecurity requirements. That will improve outcomes by bolstering incident response, enhancing resilience, reducing costs, and, ultimately, benefiting the American people.

Thank you, and I yield back.

Ms. MACE. Thank you, Mr. Connolly.

I am pleased to introduce our witnesses for today's hearing. Our first witness is Mr. John Miller, Vice President of Policy, Trust, Data, and Technology and General Counsel at the Information Technology Industry Council. Our second witness is Ms. Maggie O'Connell, Director of Security, Reliability, and Resilience at the Interstate Natural Gas Association of America. Our third witness is Mr. Patrick Warren, Vice President of Regulatory Technology with the Banking Policy Institute. And our fourth and final witness today is Dr. Charles Clancy, Chief Technology Officer at MITRE.

Welcome, everyone. We are pleased to have you this morning.

Pursuant to Committee Rule 9(g), the witnesses will please stand and raise your right hand.

Do you solemnly swear or affirm that the testimony that you are about to give is the truth, the whole truth, and nothing but the truth, so help you God?

Let the record show that the witnesses all answered in the affirmative.

We appreciate you being here today and look forward to your testimony. Let me remind the witnesses we have read your written statements, and they will appear in full in the hearing record. Please limit your oral statements to 5 minutes this morning.

As a reminder, please press the button on the microphone in front of you so that it is on and that the members up here can hear you. When you begin to speak, the light in front of you will turn green. After 4 minutes, it will turn yellow. When the light comes on and it turns red, your 5 minutes have expired. I use the gavel. I bang it hard. Let us not do that today. We would ask you to please wrap up.

All right. So, now I would like to recognize each of you individually for your opening statements. I will first recognize Mr. Miller. If you will please begin.

STATEMENT OF MR. JOHN MILLER
SENIOR VICE PRESIDENT OF POLICY, TRUST, DATA, AND TECHNOLOGY
INFORMATION TECHNOLOGY INDUSTRY COUNCIL

Mr. MILLER. Chairwoman Mace, Ranking Member Connolly, and distinguished members of the Subcommittee, on behalf of the Information Technology Industry Council, or ITI, thank you for the opportunity to testify today on the need to harmonize cybersecurity regulations.

ITI is a global policy and advocacy organization representing 80 of the world's leading tech companies, and I lead ITI's Trust, Data, and Technology policy team, including our work on cybersecurity in the U.S. and globally.

I have worked on cyber policy issues for over 15 years and have extensive experience partnering with CISA and other Federal Government stakeholders on efforts to improve cyber, supply chain, and critical infrastructure security, including currently serving in leadership positions on the ICT Supply Chain Risk Management Task Force and the IT Sector Coordinating Council.

For as long as I can remember, there has been strong, longstanding, widely agreed-upon bipartisan consensus on the need to harmonize inconsistent, duplicative, or conflicting cyber regulations. The past three administrations have prioritized the issue. Multiple Congresses have agreed it is a priority. And yet I do not recall a single conflicting, inconsistent, or duplicative cyber regulation ever being eliminated or streamlined after all these years.

So, I welcome this Subcommittee's interest and, again, shining a light on this important topic, and sincerely hope this hearing can help catalyze long overdue harmonization of cyber regulations.

The reasons why inconsistent, duplicative, or conflicting cyber regulations are costly to industry and government are obvious. The Office of the National Cyber Director has acknowledged that cyber overregulation leads to companies focusing more on compliance than security, resulting in higher costs to customers and working families, and negatively impacts national security.

This makes sense. The more resources organizations spend on compliance, auditing, and tracking across multiple regulatory regimes, the less resources are available to devote to obtaining better cyber outcomes at lower costs.

There are real costs on government too. Surely it is inefficient to use scarce government resources and regulatory capacity to create and enforce duplicative, inconsistent, or conflicting cyber regulatory requirements, particularly in light of the persistent Federal cyber workforce shortage.

Congress, to its credit, remains focused on the issue. Your colleagues at Senate HSGAC recently introduced the cyber regulatory streamlining bill, and Congress previously flagged this problem as part of the Cyber Incident Reporting for Critical Infrastructure Act, which established the Cyber Incident Reporting Council, or CIRC, to study and make recommendations to address conflicting and duplicative Federal incident reporting requirements.

Last September, CIRC report tallied over 50 such requirements that were in effect or pending, representing just one small slice of the overall cyber regulatory landscape.

When we consider that most companies are also encountering duplicative, inconsistent, or conflicting cyber regulations at the U.S. state level and internationally, it reveals the status quo as simply untenable.

The deluge of cyber incident reporting regulations perfectly illustrates the scope of the overregulation problem and also serves as a reminder that, to date, while we have studied the issue and offered recommendations, there has been no discernible harmonization. Instead, the problem is getting worse.

It is time that we stop admiring this problem and commit to addressing it. I encourage the subcommittee to consider all of the recommendations to drive better cyber harmonization in my written testimony, but I highlight five here.

First, ONCD must follow through on its ongoing work implementing the National Cyber Strategy to implement an actionable plan to harmonize existing cyber regulations and hold Federal agencies accountable for following through, including DHS for implementing the CIRC recommendations, and all agencies for actualizing harmonization efforts.

Second, we should align existing and future cyber regulations around a common taxonomy, including definitions and risk management controls grounded in international standards. The NIST Cybersecurity Framework provides a common language for doing so and can serve as an orientation point for Federal harmonization efforts.

Third, we should define a standardized clearing process for new cyber regulatory activity to prevent future fragmentation. For instance, by expanding OIRA's role to review sector-specific regulations for inconsistencies or by requiring Federal agencies to demonstrate that any new regulations must fill identified regulatory gaps.

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

Finally, Congress should seize the opportunity to drive actionable cyber harmonization solutions and use its oversight authorities to make sure that the current and future administrations follow through.

Given the Supreme Court's recent decision in Loper Bright to overturn Chevron deference, going forward, it is more important than ever that Congress provide precise cyber authorities and clear direction to the Federal agencies who will implement and enforce future rules.

Thank you again for the opportunity to testify today. I look forward to your questions.

Ms. MACE. Thank you.

I would like to recognize Mr. O'Connell for 5 minutes—Ms. O'Connell for 5 minutes.

STATEMENT OF MS. MAGGIE O'CONNELL DIRECTOR OF SECURITY, RELIABILITY, AND RESILIENCE INTERSTATE NATURAL GAS ASSOCIATION OF AMERICA

Ms. O'CONNELL. Good morning, Chairwoman Mace, Ranking Member Connolly, members of the Subcommittee. I am Maggie O'Connell, Director of Security, Reliability, and Resilience at the Interstate Natural Gas Association of America. I currently lead INGAA's cybersecurity, physical security, and emergency response policy. Thank you for inviting me to share our perspectives on cybersecurity regulatory harmonization.

INGAA is the national trade association that advocates to Federal policymakers the priorities of the interstate natural gas pipeline industry. Our members represent the majority of interstate natural gas transmission pipeline companies in the U.S. and are leaders in the reliable transportation of gas throughout the country. Many of our members also operate other forms of critical energy infrastructure, making our members some of the most regulated entities in the Nation.

The oil and natural gas subsector understands the importance of regulations to ensure the safe, secure, and reliable delivery of goods and services. Our primary purpose is to keep energy moving, which is precisely why our operators apply a risk-based "defense-in-depth" approach to cybersecurity.

Defense-in-depth is a strategy that protects the entire enterprise rather than each individual business unit from various threats. It entails robust governance, systematic risk-based management, and multidimensional programs based on industry recognized standards and frameworks.

To that end, security regulations should not be promulgated simply for the sake of doing so. They must be based on risk, outcome-focused, and threat-informed, with the goal of safeguarding those elements that enable the provision of energy services, protection of personal data, and of the essential functions that support the country's economy and national security.

The oil and natural gas industry believes there are three main considerations for determining how to harmonize cybersecurity regulations. First, regulators should engage in robust consultation processes with a regulated community, other agencies with authorities in that sector, and with regulators of sectors with direct dependencies to the sector for which the cybersecurity requirements are underdeveloped.

Second, if efforts cannot be made to harmonize proposed cybersecurity regulatory requirements, agencies should take action to retroactively ensure that requirements are harmonized in a reciprocating manner.

Third, Congress and the White House should consider whether a single entity, such as CISA, could facilitate the harmonizing role. A single entity to provide management and oversight of the multitude of cybersecurity regulations would enhance overall cybersecurity and ease compliance efforts.

I would like to briefly discuss two key principles that we believe are imperative to understanding: harmonization and reciprocity.

Harmonization is best understood as alignment across agencies and related regulations on a common set of requirements to achieve a desired security outcome. Harmonization achieves efficiency for compliance and the circumvention of duplicative or conflicting requirements. However, when undertaking this effort, the Federal Government should understand the risk within each critical infrastructure sector, the agencies with existing cybersecurity requirements, and the varying purposes of each of those regulations.

The other piece to harmonization is reciprocity, wherein the findings of one regulator satisfy the requirements of another. Reciprocity is particularly pertinent given the number of Federal regulations impacting the oil and natural gas sector emanating from a single Federal department. For example, TSA and the U.S. Coast Guard each have cybersecurity regulatory authority over segments of the oil and natural gas sector. While CISA does not currently have authority to enforce CFATS, most CFATS-regulated facilities implement the program's requirements on a voluntary basis.

These three agencies alone, existing under DHS, have made little effort to harmonize these efforts, leading to increased administrative burdens for coordinating with and meeting the requirements of these respective agencies. Indeed, a significant challenge for regulatory reciprocity is the silos in which each of these agencies exist. Each agency sees its mission as unique and independent from others despite the common goal of strong cybersecurity for critical infrastructure systems.

To that end, a single agency, such as CISA, could serve as an arbiter and facilitator for cybersecurity regulatory harmonization.

In closing, I would like to reiterate that INGAA and our members appreciate the role that smartly constructed risk-and outcome-based cybersecurity regulations play in securing our Nation's critical infrastructure. As additional agencies seek to expand their oversight and authorities to include cybersecurity, harmonization and reciprocity will be essential to ensure operators can continue to mature their security programs without overly burdensome compliance obligations.

Thank you for your time, and I look forward to your questions.

Ms. MACE. Thank you, Ms. O'Connell.

Mr. Warren, you may begin your opening statement.

STATEMENT OF MR. PATRICK WARREN VICE PRESIDENT OF REGULATORY TECHNOLOGY BANK POLICY INSTITUTE

Mr. WARREN. Chairwoman Mace, Ranking Member Connolly, and honorable members of the Subcommittee, thank you for inviting me to testify. I am Pat Warren, Vice President for Regulatory Technology for BITS, the technology division of the Bank Policy Institute.

BPI is a nonpartisan policy, research, and advocacy organization representing the Nation's leading banks. Through our technology division, we work with our members on cyber risk management, critical infrastructure protection, fraud reduction, regulation, and innovation.

As illustrated by CrowdStrike's software update last week, the security and resilience of the network systems and software that we rely on as a Nation is vitally important. Cybersecurity regulations can play a role in fostering the necessary programs and policies that protect our critical infrastructure. At the same time, we must be mindful that if not properly harmonized and aligned, such requirements can place unnecessary strain on the critical cybersecurity resources we rely on to prepare for emerging threats and address incidents when they occur.

On behalf of BPI members, we greatly appreciate the Committee's leadership and the opportunity to provide input on the need to harmonize cybersecurity regulations and streamline existing requirements.

Financial institutions are subject to numerous regulations and rigorous supervision from their prudential banking regulators: the Office of the Comptroller of the Currency, the Federal Reserve Board, and the Federal Deposit Insurance Corporation. This includes onsite examiners who regularly evaluate whether a financial institution operates in a safe and sound manner.

Firms also comply with cyber incident reporting and disclosure, consumer breach notification, data security and data privacy requirements enforced by agencies like the CFPB, the FCC, and the CFTC, among others.

Based on our experience navigating a complex regulatory environment, we believe congressional action and a focus on three areas could have meaningful impact. We encourage Congress to, one, require coordination among regulators to avoid duplication, overlap, or conflict in requirements placed on industry; two, encourage regulatory reciprocity; and three, leverage common frameworks.

First, it is imperative that all regulators consider existing requirements and do not duplicate or create variations of what already exists. We have seen this coordination does not always occur, particularly with independent regulatory agencies like the SEC.

Within the financial sector, there are several examples where the prudential banking regulators issue joint rules and guidance which helps provide clarity and consistency for firms and supports the efficient use of resources. However, the collective effect of supervision and oversight by multiple regulators can cause significant strain on personnel and the resources necessary to implement security solutions that keep pace with evolving threats.

According to a recent survey of large financial institutions, several firms reported their cyber teams now spend more than 70 percent of their time on regulatory compliance activities. Those same firms reported their Chief Information Security Officers or comparable senior cyber leaders spend between 30 to 50 percent of their time on those same regulatory compliance matters. Diverting finite cyber resources in this way leaves less time for risk mitigation activities and strategic security initiatives to fortify firm defenses moving forward.

Second, implementing a regulatory reciprocity model where one regulator accepts the work and results of another would be particularly valuable for sectors with multiple regulators and would alleviate the need for entities to demonstrate compliance with the same or similar requirements multiple times.

Based on our survey, financial institutions reported that only 30 percent of exam documentation can be reused due to slight differences in exam scope and cadence between regulators. By better leveraging each other's documentation, testing, evaluations, and findings, regulators would receive the information they need to conduct rigorous oversight while preserving the ability of cybersecurity teams to adjust to rapid technological change.

Finally, existing standards and frameworks, like NIST's Cybersecurity Framework, can be helpful tools for aligning regulatory requirements. The Cyber Risk Institute developed a financial sector profile, which is based on NIST's Cybersecurity Framework, and integrates regulatory requirements unique to the financial sector. This provides financial institutions with a single scalable resource for managing cyber risk and compliance requirements.

Regulators can also leverage common frameworks to tailor oversight priorities and more efficiently assess a company's baseline security posture.

As regulatory requirements continue to proliferate, congressional action is needed to ensure new and existing requirements accomplish the goals of better security and resilience while balancing the collective impact of these requirements on regulated entities.

We are committed to working with this Committee as it explores potential legislative solutions for achieving broader harmonization.

Thank you for the opportunity to testify today, and I am happy to answer any questions.

Ms. MACE. Thank you.

I would now like to recognize Dr. Clancy for your opening statement.

STATEMENT OF DR. CHARLES CLANCY
CHIEF TECHNOLOGY OFFICER
MITRE

Mr. CLANCY. Chairwoman Mace, Ranking Member Connolly, and members of the Subcommittee, good morning, and thank you for inviting me to testify before you today. And it is my pleasure to address the Subcommittee on this topic of critical national importance.

The practice of cybersecurity has grown organically, driven by need.

The first wave of standards, spurred by FISMA, was compliance-driven and focused on checklists of security controls. The second wave was threat-informed and motivated information sharing. The third wave was risk-based, prioritizing continuous assessment and adaptive security controls. The fourth wave that we are experiencing now is that of zero trust and architecture-driven, recognition that our greater reliance on devices and networks and cloud infrastructure that may be untrusted.

Umbrella frameworks like the NIST Cybersecurity Framework and ISO 27001 take a holistic approach from across business processes, technical controls, risk, and threat. These frameworks can be used as an organizing structure and common taxonomy to talk about regulations, but they do not really get down to the implementation level.

This leaves a patchwork of requirements for regulated organizations that have mandatory implementation obligations. It leaves them dealing with a jumble of not necessarily contradictory but often fragmented, overlapping, and inconsistent obligations.

First starting with security controls. A positive step would be to commission NIST to document the differing security controls required across different security standards. Such an enumeration would help harmonization as various standards organizations update their requirements over time and help regulators identify consensus controls that would minimize burden on their stakeholders. Again, this is not a call for new standards but, rather, illuminating the complexity of today's environment so we can build roadmaps that over time would lead to harmonization and potentially even consolidation of technically controlled standards.

Next is auditing processes. If a standard is mandatory to implement, then someone actually needs to check that it has been implemented. There is a range of everything from self-attestation of compliance to rigorous annual inspections by third-party auditors.

One concerning trend is efforts to make the NIST Cybersecurity Framework mandatory. And while this is an admiral goal, the framework was explicitly designed to be voluntary, and lacks the necessary metrology to even define compliance, making such attestations meaningless.

If you want to make something mandatory, then you need a standard that defines and provides the tools to measure compliance.

Additionally, reciprocity must be harmonized. No security standard is strictly more rigorous than any other. They all have industry-specific or domain-specific attributes, but there is a common core set of requirements across most, and the job of an auditor or regulator can be greatly simplified if there is reciprocity across that common core.

Last is incident reporting, which is probably the biggest headache for regulated organizations. Implement a single clearinghouse for reporting a cyber incident, either operated within a Federal agency, such as CISA, or by an independent third-party on behalf of the Federal Government.

Such a clearinghouse can identify a lead agency to engage with the affected party, coordinate with others across the interagency, and really serve as a touch point for major vendors that support that industry, like CrowdStrike or Microsoft that have equities that cross many different sectors.

A clearinghouse would serve a number of important other purposes as well, including energizing a Federal cyber action team that could help impacted organizations with incident response, if appropriate and necessary; serve as a focal point for major vendors and cloud providers who may be stakeholders, particularly in wide-scale cyber incidents; and be an important repository for cross-sector data on adversary cyber operations so we can actually keep track of what our adversaries are doing in an integrated way across the entire ecosystem.

Another important point is that reporting should be viewed as iterative. As reporting timelines get shorter and shorter, the amount of high-confidence, reportable information collected by affected organizations get smaller and smaller. We must balance reporting timelines with practical detail on incidents from the impacted organization and the actual utility of that data to a regulator.

Reporting "we might have been hacked but we are not sure, and we have no idea what might have been impacted" within 8 hours to a regulator does not provide anything actionable. If that regulator's typical response time for assigning a case agent and soliciting additional information is 2 weeks, then what was the point of the 8-hour reporting timeline in the first place?

A clearinghouse could also help with state, local, Tribal, and territorial government reporting and coordination. These governments have a growing set of cyber reporting obligations, and a Federal clearinghouse could ease the burden on impacted organizations.

In conclusion, I encourage the Committee to move from study to action. The National Cybersecurity Strategy identified the need to establish an initiative on harmonization. The Peters-Lankford bill currently in the Senate involves years of pilots. NSM 22 calls on DHS to develop a plan for harmonization and critical infrastructure by April 2025. Last fall's ONCD request for information gathered broad industry input from a variety of stakeholders. I think we have a good handle on the issues, and we need to move out on solutions.

Thank you, and I look forward to your questions.

Ms. MACE. Thank you.

I ask unanimous consent to submit the following statements for the record: a statement from the American Gas Association and a statement from Airlines for America. And without objection.

Ms. MACE. First of all, I want to thank you all for being here. We have a broad section of industry, from IT to natural gas, banking, and then, of course, MITRE company. You know, listening to your testimony, it is very clear that the government is way too big, way too overregulated because of all the duplicative efforts.

I would like to ask everyone a question this morning. For your member companies, or for MITRE specifically, would you be able and willing to invest more in cybersecurity enhancements like IT upgrades if the compliance burden of inconsistent, duplicative regulations was reduced? Would you have the resources to be able to invest more than what you are today if that burden was reduced?

Mr. MILLER. Yes. I mean, I think, based on everything that we have heard from our companies, they would definitely have more resources to invest in cybersecurity and producing better cybersecurity outcomes if they did not have to spend as much resources on complying with conflicting or duplicative regulatory regimes.

Ms. MACE. And I am sure you guys are all going to probably say yes, but I do want to focus on something Mr. Warren said in your testimony today, the 70 percent figure.

You are in the banking sector, so it might be slightly different. Is it the same in natural gas and IT? Are you seeing the 70 percent? What is the rough, the figure, roughly, of percentage of cybersecurity workers, generally within industry, that you guys represent that are focused on compliance? Do you have a handle on that?

Ms. O'CONNELL. I do not have exact numbers in front of me, but based on the information that I have heard from our members, that sounds about accurate, yes.

Ms. MACE. Even in natural gas, Mr. Miller?

Mr. MILLER. I mean, I think it—I do not have exact numbers either, but I do think it varies by companies, right. I mean, certainly larger multinational tech companies have more resources, so they are, you know, able to devote more resources to both compliance and better security outcomes.

I think that there are a lot of small and medium-sized companies in the tech sector, and I think that these types of conflicting requirements that we are talking about today really disproportionately hit those companies who it is much more of a zero-sum game for them.

Ms. MACE. Much more expensive, the cost of legal fees.

Mr. MILLER. Yes. If you are a smaller company, and you may not even be able to figure out what regulations you have to comply with, it creates, I think, a bad situation.

Ms. MACE. Yes. So, in terms of that—and I only have 2 1/2 minutes left, roughly, and I would like to hear from all members on the panel. I will start with—Ms. O'Connell, I will start with you. It is almost like where do you start? But if you could just do one thing, one bill, one policy, one regulation, one piece of legislation, what is that one thing?

Because we are so big. We are so bureaucratic. I mean, a comprehensive policy, it just is not going to happen, right. And it is not going to happen in the next decade because we are not nimble anymore. We do not move that fast, unfortunately.

But if you could do one thing today or tomorrow, what would that—what would that be to make it better for industry?

Ms. O'CONNELL. I would say specific to our sector, reciprocity would probably move the needle the quickest. Given we have multiple security regulators across our industry, any efforts to sort of streamline and, you know, have one set of requirements be applicable to another set of regulations would really be, I think, an efficient way to move that needle quickly.

Ms. MACE. Thank you.

Mr. Warren?

Mr. WARREN. Sure. I think an area that has been a particular challenge for financial institutions is cyber incident reporting. These requirements often have slightly different definitions, timeframes for reporting, and information requirements.

And so, hypothetically, if a financial institution were to experience a reportable incident, they would first have to report to the Federal Housing Administration within 12 hours of detection. They would have to notify their primary banking regulator within 36 hours. Another notification to Ginnie Mae within 48 hours. Once CIRCIA is finalized, they would have to provide a very detailed report to CISA within 72 hours, and then, finally, publicly disclose that incident to the SEC within 4 business days.

So, compiling all of those reports, similar but distinct reports, takes a lot of time from frontline cyber personnel, which leaves less time for day-to-day security——

Ms. MACE. Would it be better if it just went to CISA and then CISA distributed it accordingly?

Mr. WARREN. Sure. And I think that CISA has been tasked with harmonizing cybersecurity regulations under CIRCIA. Unfortunately, with a recent proposed rule to implement that legislation, it seems they have taken an expansive approach to implementing that law. We provided comment with a number of other financial trades, encouraging them to better leverage existing requirements, and leaders in the House Homeland Security Committee and Senate HSGAC provided similar feedback as well.

Ms. MACE. Dr. Clancy? We have 15 seconds.

Mr. CLANCY. I would just amplify that. I think you can build on CIRCIA in making that clearinghouse for reporting that coordinates across interagency.

Ms. MACE. OK. Thank you all. I appreciate your time this morning.

And I will now yield to Mr. Connolly for 5 minutes.

Mr. CONNOLLY. Thank you.

Just to clarify, Mr. Warren, what was that 70 percent referring to?

Mr. WARREN. That refers to the amount of time a number of our firms reported their frontline cyber personnel are spending on regulatory compliance matters.

Mr. CONNOLLY. Those personnel assigned to cyber?

Mr. WARREN. Correct.

Mr. CONNOLLY. Right. And how many people is that?

Mr. WARREN. It varies depending on firm. I am not sure I am able to give you an exact number across our member institutions.

Mr. CONNOLLY. Banks are often a target of cyberattacks or attempted attacks. Is that not correct?

Mr. WARREN. That is correct as a critical infrastructure statement.

Mr. CONNOLLY. Right. And how many—collectively, how many Americans are customers of banks?

Mr. WARREN. I am not sure I have the exact number of how many.

Mr. CONNOLLY. Kind of most of us, right?

Mr. WARREN. Yes.

Mr. CONNOLLY. So, the government has some interest in protecting those people, working with the banking community, in making sure that data is not disclosed, misused, assets diverted, deposits corrupted, just like banks do, presumably, because you do not want to lose customers. You would concede that point?

Mr. WARREN. Yes.

Mr. CONNOLLY. So, the issue is how best to do that, right. What is the balance between, you know, the need of banks to do their business or the gas industry or anybody else while the government tries to get its arms around the cyber problem and hopefully working with industry to protect American consumers? And, you know, it is going to be natural that we may have disagreements about how far we go.

Industry is always going to have an eye on what it costs and, you know, kind of cost-benefit analysis of how far do we go in that cyber thing. And government may have a different point of view about the value of that cost-benefit analysis. And so therein lies potential for conflict.

Let me ask you this: do you think if we got government entirely out of the business, the banking industry could handle this all by itself, thank you very much? We can—we can—we, the banking industry, could come up with our own set of standards, our own cyber protection policies that would be fairly standard and would voluntarily comply with them and there would be no problem.

Mr. WARREN. I think the financial sector is supportive of a number—has been supportive of a number of confidential reporting requirements, like CIRCIA and the banking 36-hour notification rule. Those regulators worked very collaboratively with industry to develop that requirement.

I think, really, it is about striking the right balance here. We recognize the importance of these requirements for the enhanced visibility they provide for the cyber threat environment and to warn potential downstream victims. I think it is less an issue of cost and more one of time.

Mr. CONNOLLY. OK. Got it.

Mr. WARREN. Institutes want to spend more time on cyber.

Mr. CONNOLLY. So, Dr. Clancy, my concern—I am not unsympathetic with the bureaucratic burden, and I think we could tolerate the bureaucratic burden if it led to efficacy. We talk about harmony and reciprocity. I am going to add a third one. Efficacy.

How effective is it? Because if it is effective, then I am going to leave it alone. But if we are doing all of this and it is not effective, then we have got to fix it. We have got to do something else.

Comment on that. Do these requirements, do these burdens on reporting and creating systems and so forth, how efficacious are they?

Mr. CLANCY. I think when we talk about this, we need to look at it through the lens of the adversary as well.

So, China and Russia have made it clear that they are coming after our critical infrastructure from a cybersecurity perspective. I think what we are seeing is lots of different regulators all layering slightly different versions of the same obligations on top of the critical infrastructure sectors. None of it is really new, and I do not know that any of it necessarily rises to the nature of the threat that we are seeing from Russia and China.

So, it is just sort of creating a compounding set of the same. And I think what we really need is new thinking and if you want to get after efficacy.

Mr. CONNOLLY. So, in my last few minutes, I wrote a bill to codify and set a new standard or—for FedRAMP, which is the process at GSA for certifying companies that want to do business with the Federal Government for cloud computing. And we had the same problem. Like, every Federal agency had its own standards, and you could go to one window but then go to another one, you had to start all over again and they had their own.

So, we built into the law that when you are certified by a Federal agency, there is a presumption of adequacy. And so, you are good to go in the other Federal windows as well. You do not have to start all over again. And we are trying to eliminate duplication and redundancy and overburden in regulations.

And it seems to me taking that concept here so that we can try to—you are calling it harmonization. OK. But the presumption of adequacy, if you have met a cyber standard by agency X, you ought to be good to go and not have to have a whole new set of regulations by agency Y. So, that is something I hope we can explore.

Thank you.

Ms. MACE. All right. I would now like to recognize Mr. Burlison for 5 minutes.

Mr. BURLISON. Thank you.

If we could go to Mr. Miller, Ms. O'Connell, and Mr. Warren, just to get an idea from your particular industry. What is the—if you had to put a dollar figure on it, what is the cost of complying—of the conflicts in the regulatory burdens that you are facing?

Mr. MILLER. Thank you for the question.

I do not know that I have a, you know, an actual aggregate number of the amount of, you know, of the compliance burden that we are talking about here. I mean, I guess I would just say that by all accounts, it is significant and, you know, I do think it is probably even more significant for heavily regulated industries, such as my, you know, colleagues here up on the panel.

But it is—it seems to be a problem. The compliance burdens are growing every day. And, again, I think they are disproportionately hitting the smaller companies in the sector even more harshly.

Ms. O'CONNELL. I would sort of echo that. The compliance costs, I think, vary greatly based on your company size, the complexity of your operations, your staffing. INGAA generally as a trade association tries to stay out of conversations around cost for antitrust reasons, so it is difficult for me to kind of quantify that.

But to your point, I mean, I think, you know, it does disproportionately affect smaller entities across all critical infrastructure, not just oil and natural gas.

Mr. WARREN. Similar to my fellow panelists, I am not sure I am able to provide a ballpark estimate. There will be some variance across our member financial institutions. The bottom line is firms are going to spend whatever they have to in order to secure their environments.

But what I will say is we have heard from firms that staff have had to work exceedingly long hours to balance the burden of regulatory compliance with their day-to-day security obligations, and there are scenarios where that has led to decreased morale and staff burnout.

Mr. BURLISON. I can totally relate with what you all are referring to. I used to conduct cybersecurity audits in healthcare and used to have to comply with meaningful use requirements and HIPAA, and knew firsthand real-world scenarios where the well intentions of this place, of this town did nothing to benefit patients and did nothing to benefit the patient-provider experience.

So, I would like to hear directly—because I can think of those laws in particular—what specifically—are we talking about rules that have been implemented that you are struggling with? And if it is possible to, because I want to put pen to paper here and actually take, you know, some tasks out of this hearing.

What specifically—what policies specifically are affecting your industry that we might be able to address? And are they laws? Are they rules? What are they? And if you could go down the line.

Mr. MILLER. Sure. I mean, I think, you know, the example that I cited earlier and that others have talked about here is I think top of mind for many folks, and that is cyber incident reporting, regulations, and requirements.

You know, on the one hand, we have Congress recently passing, you know, a couple years ago, CIRCIA, a Federal bill, with an idea of streamlining requirements and, you know, also setting up CIRC, Cyber Incident Reporting Council, to issue a report and streamline requirements.

You know, the requirements do vary. I mean, obviously, CIRCIA is an underlying legislative regulation, but there are different requirements that vary over those. I think it was 52 in total, different types of requirements and regulations on incident reporting.

And, again, the problem is that, even though we have identified the problem and Congress has identified the problem, we have set up, you know, a group, the council to fix it, even after that report has come out, we have had more divergent requirements being proposed.

An example is there was a FAR regulation that was proposed just a couple months after that that varied from the recommendations in that report. So, I mean, that is the example that I would use for the IT industry is incident reporting.

Mr. BURLISON. Ms. O'Connell?

Ms. O'CONNELL. I would echo the incident reporting requirements. I mean, we currently are required to report incidents to CISA within 24 hours under the first TSA security directive. We also have CIRCIA. There are also state and local reporting requirements.

But I would also, on the more kind of, you know, risk-based kind of regulatory side, I would say hastily promulgated regulations are also a real challenge for compliance. For example, when TSA first issued its first iteration of the second security directive, they required some very prescriptive mitigation measures that were either impossible to achieve in the pipeline environment or with existing technologies, or they had, you know, perhaps reactive and, you know, inconsequent, like, downstream impacts to pipeline reliability and safety. And those were not considered when TSA first promulgated that security directive.

They have since undertaken a very robust consultative process with industry and with the other regulators in the pipeline and oil and natural gas industry to make it more risk-based and outcome-focused.

And I think as long as regulations are promulgated with that risk-based, outcome-focused, threat-informed mentality, then they can be successful. But when they are overly prescriptive and they are reactive, that is where the challenge can be within compliance.

Mr. BURLISON. Mr. Warren?

Mr. WARREN. Incident reporting is a challenge for our sector as well. But another place where sometimes they overlap and duplication occurs is in the supervisory environment, where one financial regulator will examine a firm on a given topic, say, identity and access management, and shortly after that exam concludes, another regulator will come in and examine the exact or similar topic. That pulls on the same cyber personnel and is sort of a consistent exam regulatory obligation for them rather than their day-to-day security responsibilities.

Mr. BURLISON. Because it is—if I may? Can I continue?

It is a lot of work to pull all of those reports. When you are talking about identity and access management alone, to pull all of those reports and who has specific role access for any software, it can be a daunting task. And then to have to do it repeatedly and based on whatever the demand is for the different agency, I can absolutely see why that would be problematic.

Let me ask this, if it is OK. Are there—you know, if we did not have these in place, if the Federal Government was not doing it, you have an innate desire to want to have your data secure. And when there are events, they become high profile. You know, it is all over the news. Your stock goes down. That in and of itself is a deterrent.

But you have got industry standards as well, right. So, you have got the industry who is creating these certification levels and these standards that are not necessarily connected to the government. Which is more important to meet? I mean, which would you prefer: to try to meet the industry standard, the certification levels, or to try to comply with these regulators?

Mr. MILLER. I mean, I think—you are raising a really good point, Congressman. You know, I think there are a lot of different—it is an important reminder that, you know, regulations are not the answer to everything, right. It is not going to solve all of our problems. You know, we have got regulations. We have got frameworks, such as the Cybersecurity Framework. We have got international standards. We have got guidance, then there are administrative requirements.

So, there is a lot going on there, but, you know, in terms—I think they are all important and they all have a role, but what is really most important from a company standpoint is that, you know, everything is hopefully oriented toward common consensus-based standards and that those standards are risk management standards, right.

I mean, we are talking about risk management, which, you know, is not only just about defending—I do not want to minimize the importance of that—but also, response and recovery efforts as well. I mean, all of this is important.

You know, cybersecurity has a lot of dimensions, and from an industry standpoint, we need to do it all. We need to do it all well. We just need to align and not be operating at cross purposes.

Mr. BURLISON. Ms. O'Connell——

Ms. O'CONNELL. Sure. I would say the golden ticket is when regulations are aligned with industry standards. Of course, that cannot always happen, but, you know, when it does, when regulations are, again, promulgated in a way that is consulted with the industry, that is when you can get the best result of the regulation.

Mr. WARREN. And I think this is a place where industry can leverage common frameworks that sort of reference regulatory requirements and common standards to sort of validate that they are where they need to be from a cybersecurity standpoint and hopefully streamline some of these compliance requirements.

Mr. BURLISON. I am well beyond my time.

Ms. MACE. Thank you, Mr. Burlison. You did great.

OK. In closing today, I want to thank our panelists once again for their testimony.

And with that, and without objection, all members will have 5 legislative days within which to submit materials and to submit additional written questions for the witnesses which we will then forward to the witnesses for their response.

If there is no further business, then, without objection, we stand adjourned.

[Whereupon, at 9:59 a.m., the Subcommittee was adjourned.]

○