

REGULATORY HARM OR HARMONIZATION? EXAM-
INING THE OPPORTUNITY TO IMPROVE THE
CYBER REGULATORY REGIME

HEARING
BEFORE THE
SUBCOMMITTEE ON
CYBERSECURITY AND INFRASTRUCTURE
PROTECTION
OF THE
COMMITTEE ON HOMELAND SECURITY
HOUSE OF REPRESENTATIVES
ONE HUNDRED NINETEENTH CONGRESS

FIRST SESSION

MARCH 11, 2025

Serial No. 119-7

Printed for the use of the Committee on Homeland Security



Available via the World Wide Web: <http://www.govinfo.gov>

U.S. GOVERNMENT PUBLISHING OFFICE

60-983 PDF

WASHINGTON : 2025

COMMITTEE ON HOMELAND SECURITY

MARK E. GREEN, MD, Tennessee, *Chairman*

MICHAEL T. MCCAUL, Texas, <i>Vice Chair</i>	BENNIE G. THOMPSON, Mississippi, <i>Ranking Member</i>
CLAY HIGGINS, Louisiana	ERIC SWALWELL, California
MICHAEL GUEST, Mississippi	J. LUIS CORREA, California
CARLOS A. GIMENEZ, Florida	SHRI THANEDAR, Michigan
AUGUST PFLUGER, Texas	SETH MAGAZINER, Rhode Island
ANDREW R. GARBARINO, New York	DANIEL S. GOLDMAN, New York
MARJORIE TAYLOR GREENE, Georgia	DELIA C. RAMIREZ, Illinois
TONY GONZALES, Texas	TIMOTHY M. KENNEDY, New York
MORGAN LUTTRELL, Texas	LAMONICA MCIVER, New Jersey
DALE W. STRONG, Alabama	JULIE JOHNSON, Texas, <i>Vice Ranking Member</i>
JOSH BRECHEEN, Oklahoma	PABLO JOSÉ HERNÁNDEZ, Puerto Rico
ELIJAH CRANE, Arizona	NELLIE POU, New Jersey
ANDREW OGLES, Tennessee	TROY A. CARTER, Louisiana
SHERI BIGGS, South Carolina	ROBERT GARCIA, California
GABE EVANS, Colorado	VACANT
RYAN MACKENZIE, Pennsylvania	
BRAD KNOTT, North Carolina	

ERIC HEIGHBERGER, *Staff Director*
HOPE GOINS, *Minority Staff Director*
SEAN CORCORAN, *Chief Clerk*

SUBCOMMITTEE ON CYBERSECURITY AND INFRASTRUCTURE PROTECTION

ANDREW R. GARBARINO, New York, *Chairman*

CLAY HIGGINS, Louisiana	ERIC SWALWELL, California, <i>Ranking Member</i>
CARLOS A. GIMENEZ, Florida	SETH MAGAZINER, Rhode Island
MORGAN LUTTRELL, Texas	LAMONICA MCIVER, New Jersey
ANDREW OGLES, Tennessee	VACANT
MARK E. GREEN, MD, Tennessee (<i>ex officio</i>)	BENNIE G. THOMPSON, Mississippi (<i>ex officio</i>)

ALEXANDRA SEYMOUR, *Subcommittee Staff Director*
MOIRA BERGIN, *Minority Subcommittee Staff Director*

CONTENTS

	Page
STATEMENTS	
The Honorable Andrew R. Garbarino, a Representative in Congress From the State of New York, and Chairman, Subcommittee on Cybersecurity and Infrastructure Protection:	
Oral Statement	1
Prepared Statement	2
The Honorable Eric Swalwell, a Representative in Congress From the State of California, and Ranking Member, Subcommittee on Cybersecurity and Infrastructure Protection:	
Oral Statement	3
Prepared Statement	5
The Honorable Mark E. Green, MD, a Representative in Congress From the State of Tennessee, and Chairman, Committee on Homeland Security ...	6
The Honorable Bennie G. Thompson, a Representative in Congress From the State of Mississippi, and Ranking Member, Committee on Homeland Security:	
Prepared Statement	7
WITNESSES	
Mr. Scott I. Aaronson, Senior Vice President, Energy Security & Industry Operations, Edison Electric Institute:	
Oral Statement	9
Prepared Statement	11
Ms. Heather Hogsett, Senior Vice President and Deputy Head of BITS, Bank Policy Institute:	
Oral Statement	14
Prepared Statement	16
Mr. Robert Mayer, Senior Vice President, Cybersecurity and Innovation, USTelecom, The Broadband Association:	
Oral Statement	20
Prepared Statement	21
Mr. Ari Schwartz, Coordinator, Cybersecurity Coalition:	
Oral Statement	23
Prepared Statement	25
APPENDIX I	
Statement of CTIA—The Wireless Association	49
APPENDIX II	
Questions From Chairman Andrew R. Garbarino for Scott I. Aaronson	55
Questions From Chairman Andrew R. Garbarino for Heather Hogsett	57
Questions From Chairman Andrew R. Garbarino for Robert Mayer	59
Questions From Chairman Andrew R. Garbarino for Ari Schwartz	62

REGULATORY HARM OR HARMONIZATION? EXAMINING THE OPPORTUNITY TO IM- PROVE THE CYBER REGULATORY REGIME

Tuesday, March 11, 2025

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
SUBCOMMITTEE ON CYBERSECURITY AND
INFRASTRUCTURE PROTECTION,
Washington, DC.

The subcommittee met, pursuant to notice, at 10:08 a.m., in room 310, Cannon House Office Building, Hon. Andrew R. Garbarino (Chairman of the subcommittee) presiding.

Present: Representatives Garbarino, Higgins, Gimenez, Ogles, Green (ex officio), Swalwell, Magaziner, McIver, Clarke, and Hernández.

Mr. GARBARINO. The Committee on Homeland Security will come to order.

Without objection, the Chair may declare the committee in recess at any point.

Without objection, the gentlewoman from New York, Ms. Clarke, and the gentleman from Puerto Rico, Mr. Hernandez, are permitted to sit on the dais and ask questions of the witnesses.

The purpose of this hearing is to evaluate the effectiveness of the Federal cyber regulatory regime and to identify opportunities to harmonize cyber regulations across the Federal Government. Specifically, we will examine the challenges that private-sector owners and operators of critical regulatory—of critical infrastructure face while navigating cyber regulatory regime, including the potential impact of the final CIRCIA rule if it does not meet Congressional intent.

I now recognize myself for an opening statement.

Good morning. I am honored to serve as Chairman of this subcommittee again in the 119th Congress.

Ranking Member Swalwell, it's great to serve alongside you for another term.

I'd also like to welcome all of our Members returning and the new ones that are here. I'm looking forward to working with all of you and to making this a productive Congress.

As cyber threats to information technology and operational technology increase, we must work hard to ensure cybersecurity is front and center on Congress' agenda. Until we change our cybersecurity posture, we'll continue to see rogue nation-state actors target our Nation's critical infrastructure. In that spirit, I am pleased to kick

off this Congress with a bipartisan priority that is vital to our Nation's security, regulatory harmonization.

For too long we have talked about the cumbersome nature of cyber regulatory regime without seeing the changes necessary to solve it. In fact, the Biden administration tried to add more regulations on this sector and sectors such as health care and water. While it is important for the Federal Government to work with those sectors that are not as cyber mature, more regulation is not the answer. With over 50 regulations at the Federal level alone, it is time to streamline requirements to ensure they promote useful, actionable, and reasonable information sharing within the time frame requested.

When organizations face their most vulnerable moment, they should only be thinking about one thing: Securing their networks. Hours of duplicative compliance tasks and hundreds of thousands of dollars invested to navigate the landscape must come to an end. With the beginning of the new administration, we have an opportunity to reset the regulatory regime once and for all.

In 2022, Congress passed landmark legislation to streamline cyber incident reporting. The Cyber Incident Reporting for Critical Infrastructure Act of 2022, or CIRCIA, has directed CISA to develop regulations to set an acceptable standard for cyber incident reporting across all 16 critical infrastructure sectors.

Unfortunately, as many of today's witnesses reinforced last year, the scope of the proposed CIRCIA rule went far beyond Congressional intent. Knowing that the deadline for the final rule is approaching, we will dig into the value of CIRCIA and what the future of the rule should look like. This new administration presents an opportunity to get cyber incident reporting right. We should seize it.

Beyond CIRCIA, different regulatory agencies have imposed rules that directly contradict Congressional intent with CIRCIA. Securities and Exchange Commission's rules on cybersecurity risk management, strategy, governance, and incidents disclosure are a perfect example of how rulemaking should not be done—that is without buy-in from their key stakeholders, industry, and Congress.

As we strive for regulatory harmonization, collaboration across the public and private sector is vital. We cannot allow malicious cyber actors to get ahead of us because paperwork holds us back from effective cyber risk management, mitigation, and response. I look forward to hearing from our witnesses about the steps we take to finally—we can take to finally achieve regulatory harmonization.

[The statement of Chairman Garbarino follows:]

STATEMENT OF CHAIRMAN ANDREW R. GARBARINO

MARCH 11, 2024

Good morning.

I am honored to serve as Chairman of this subcommittee again in the 119th Congress. Ranking Member Swalwell, it is great to serve alongside you for another term. I'd also like to welcome all our Members, returning and new. I'm looking forward to working with all of you, and to making this a productive Congress.

As cyber threats from nation-state and criminal actors to information technology (IT) and operational technology (OT) increase, we must work hard to ensure cybersecurity is front and center on Congress' agenda. Until we change our cybersecurity

posture, we will keep hearing about the Typhoons—including new ones that will inevitably emerge.

In that spirit, I am pleased to kick off the Congress with a bipartisan priority that is vital to our Nation's security: regulatory harmonization.

For too long, we have talked about the cumbersome nature of the cyber regulatory regime without seeing the changes necessary to solve it. In fact, the Biden administration tried to add more regulations on sectors such as health care and water. Some sectors admittedly have a more mature cybersecurity posture than others. While it is important for the Federal Government to work with those entities, more regulation is not the answer. With over 50 regulations at the Federal level alone, it is time to streamline requirements to ensure they provide information that is useful, actionable, and reasonable within the time frame requested.

When organizations face their most vulnerable moment, they should only be thinking about one thing: securing their networks. Hours of duplicative compliance tasks and hundreds of thousands of dollars invested to navigate the landscape must come to an end. With President Trump's mandate to increase Government efficiency and reduce regulatory burden, we have an opportunity to reset the regulatory regime once and for all.

In 2022, Congress passed landmark legislation to streamline cyber incident reporting. The Cyber Incident Reporting for Critical Infrastructure Act of 2022, or CIRCIA, directed CISA to develop regulations to set an acceptable standard for cyber incident reporting across all 16 critical infrastructure sectors.

Unfortunately, as many of today's witnesses reinforced last year, the scope of the proposed CIRCIA rule went far beyond Congressional intent. Knowing that the deadline for the final rule is approaching, we will dig into the value of CIRCIA and what the future of the rule should look like. This new administration presents an opportunity to get cyber incident reporting right. We should seize it.

Beyond CIRCIA, different regulatory agencies have imposed rules that directly contradict Congressional intent with CIRCIA. The SEC rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure are a perfect example of how rulemaking should not be done—that is, without buy-in from their key stakeholders: industry and Congress.

As we strive for regulatory harmonization, collaboration across the public and private sectors is vital. We cannot allow malicious cyber actors to get ahead of us because paperwork holds us back from effective cyber risk management, mitigation, and response.

I look forward to hearing from our witnesses about the steps we can take to finally achieve regulatory harmonization.

Mr. GARBARINO. I now recognize the Ranking Member for an opening statement.

Mr. SWALWELL. I thank the Chairman, and excited to begin this new Congress, again, with the Chairman. It's not a great place to be in the Minority, but if you have a Chairman like Mr. Garbarino on your subcommittee, it's a great place to get things done, and that's our mission here is to get things done for the good of our constituents and the security of the people and companies we represent.

This first hearing is focused on a bipartisan priority, identifying opportunities to improve implementation of the Cyber Incident Reporting for Critical Infrastructure Act, CIRCIA, and the need to harmonize cyber regulations.

Before I begin though, I did want to take a moment to recognize and express my condolences to the family, friends, and constituents of Congressman Sylvester Turner, who passed away last week. He was a Member of this subcommittee, and his passion for cybersecurity, whether it was as the mayor of one of America's largest cities in Houston, that was clear also as a Member of Congress serving on a committee that works on that, and it was clear during his first 2 full committee hearings last month. We'll miss his contributions that he made and would've made to this subcommittee.

Turning to the subject of today's hearing, I agree that compliance costs can outweigh the security benefit of regulations when compliance with duplicative regulations cuts into investment and security. We should not be imposing regulations for the sake of imposing regulations. Security should be designed to achieve outcomes that are proven to reduce risk and improve resilience and security.

Toward that end, I am pleased to support CIRCIA because it addressed a concrete security gap and will improve the Government's ability to detect and disrupt malicious cyber activity. It also put in place a framework that ensures covered entities would not need to report the same cyber incidents multiple times to multiple regulators. If a hacker gets into a bank or energy company, we want them to focus on eradicating the threat as quickly as possible, not huddling the lawyers and compliance experts. They should be fixing the problem and reestablishing their services.

I am troubled that the proposed rule does not incorporate the feedback that the private sector provided during the RFI process. Congress put CISA in charge of the cyber incident reporting rule because it has a record of working collaboratively with the private sector, and our intent was that CISA would engage the private sector to develop a workable rule.

Together with Ranking Member Thompson and my colleague Congresswoman Clarke, I submitted comments on the proposed rule urging CISA to more carefully scope the entities, incidents, and information that must be reported. I've also called on CISA to establish an ex parte process to facilitate on-going engagements with the prior—with the private sector.

With the fall 2025 deadline for issuing a final rule looming, I urge CISA to work quickly to reengage with the private sector and refine the scope of this rule. There are also 3 key pieces of cybersecurity legislation that I urge this committee to pass as quickly as possible. First, we must authorize the Joint Cyber Defense Collaborative, CISA's operational and collaboration hub. Formal authorization of the JCDC will provide much-needed transparency regarding who can be a member and the activities JCDC takes on. We passed this in a bipartisan manner last Congress with support of the Chairman of the whole committee, and I hope that authorization this Congress will restore trust among JCDC participants and focus JCDC on the activities most likely to drive security benefits.

Relatedly, the Cyber Information Sharing Act of 2015 is set to expire at the end of September. The bill is the foundational collaboration between the Government and the private sector, and it must be reauthorized.

As it relates to CISA and some of the firings that we've seen there, I want to make sure that we get rid of waste, fraud, and abuse. The Government should be efficient and not waste your money. That is a priority of mine; it's a priority of most of my colleagues. However, we must be especially careful when any cut goes to public safety, national security, or cybersecurity, because we know that we are more vulnerable than ever to a cyber attack, and we want to make sure that we have the best folks on guard working hand-in-hand with the private sector to make sure we're best protected.

Finally, State and local cybersecurity grant programs will expire on September 30. The grant program has helped State and local governments across the country improve their ability to defend against and become resilient to sophisticated cyber attacks from our adversaries and other criminals.

Again, I thank my colleagues for their commitment to moving the ball forward on cybersecurity, and I look forward to working with each of you and our witnesses to do that.

Mr. Chairman, again, I'm looking forward to this Congress and what we can do together, and this is an appropriate way to kick off this subcommittee, and I yield back.

[The statement of Ranking Member Swalwell follows:]

STATEMENT OF RANKING MEMBER ERIC SWALWELL

MARCH 11, 2025

I'm glad our subcommittee's first hearing of the Congress is focused on a bipartisan priority: identifying opportunities to improve implementation of the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) and the need to harmonize cyber regulations more broadly.

But before I begin, I would like to take a moment to express my condolences to the family, friends, and constituents of Congressman Sylvester Turner, who passed away last week. His passion for cybersecurity was clear during his participation in the first 2 full committee hearings last month, and we will miss the contributions he would have made to the subcommittee.

Turning to the subject of today's hearing, I agree that compliance costs can outweigh the security benefit of regulations when compliance with duplicative regulations cuts into investments in security. We should not be imposing regulations for regulation's sake. Cybersecurity regulations should be designed to achieve outcomes that are proven to reduce risk and improve security and resilience.

Toward that end, I was pleased to support CIRCIA because it addressed a concrete security gap and will improve the Government's ability to detect and disrupt malicious cyber campaigns faster. It also put in place a framework to ensure that covered entities would not need to report the same cyber incident multiple times to multiple regulators.

If a hacker gets into a bank or energy company, we want them to focus on eradicating the threat and getting back up and running. Their first step should not be bringing in a team of lawyers and compliance experts. It should be fixing the problem and re-establishing their services.

I share the concerns raised by our panelists today regarding the scope of the proposed rule that CISA issued last spring. Notably, I was troubled that the proposed rule did not incorporate the feedback that the private sector provided during the RFI process.

Congress put CISA in charge of the cyber incident reporting rule because it has a record of working collaboratively with the private sector, and our intent was that CISA would engage the private sector to develop a workable rule.

Together with Ranking Member Thompson and Congresswoman Clarke, I submitted comments on the proposed rule urging CISA to more carefully scope the entities, incidents, and information that must be reported.

I also called on CISA to establish an ex parte process to facilitate on-going engagement with the private sector. With the fall 2025 deadline for issuing a final rule looming, I urge CISA to work quickly to re-engage with the private sector and refine the scope of the rule.

The cyber threats we face are evolving too quickly for any unnecessary delay. I would like to thank Chairman Garbarino and Chairman Green for their focus on improving the Nation's cybersecurity posture.

Toward that end, there are at least 3 key pieces of cybersecurity legislation that I urge the committee to begin its work on as soon as possible.

First, we must authorize the Joint Cyber Defense Collaborative, CISA's operational collaboration hub. Formal authorization of the JCDC will provide much-needed transparency regarding who can be a member of JCDC and the activities JCDC takes on.

Authorization will help restore trust among JCDC participants, focus JCDC on the activities most likely to drive security benefits, and ensure that it is accountable

to both stakeholders and Congress for delivering a return on investment. I appreciated Chairman Green's support of the legislation last Congress and hope to work with my colleagues on a bipartisan basis to refine the bill and broaden support for it this Congress.

Relatedly, the Cybersecurity Information Sharing Act of 2015 is set to expire on September 30. The bill is the foundation of operational collaboration between the Government and the private sector and it must be reauthorized.

Finally, the State and Local Cybersecurity Grant program will also expire on September 30. The grant program has helped State and local governments across the country improve their ability to defend against and become resilient to sophisticated cyber attacks from our adversaries and other cyber criminals. For months, stakeholders have asked me to do everything in my power to reauthorize the program and I hope my Republican colleagues will support this effort.

Once again, I thank my colleagues for their commitment to moving the ball forward on cybersecurity, and I look forward to working with you to do just that.

Mr. GARBARINO. The gentleman yields back.

I thank—I now recognize the Chairman of the full committee, Mr. Green, for an opening statement.

Mr. GREEN. Thank you, Chairman Garbarino and Ranking Member. Good to see you guys today.

Today's hearing serves as a crucial opportunity to examine the effectiveness of Federal cyber bureaucracy. At a time when cyber attacks are growing more frequent and sophisticated, it's imperative that our regulatory process governing cyber space is strengthened and harmonized. This will promote security and cooperation while minimizing cost and confusion.

Last May, this subcommittee held a hearing focused on CIRCIA, Cyber Incident Reporting for Critical Infrastructure Act of 2022. CIRCIA, among other things, directed CISA to create and implement regulations for cyber incident reporting across 16 critical infrastructure sectors. Although Congress passed CIRCIA nearly 3 years ago, wide-spread regulatory disharmony persists throughout the cyber incident reporting and response regime.

There are now at least 50 cyber incident reporting requirements in effect across the Federal Government. These regulations are often duplicative and complex, requiring private-sector owners and operators to invest significant sums into regulatory compliance rather than security. This patchwork of conflicting and complex regulations place a significant burden on reporting entities.

Let's be clear, improving our Nation's cyber regulatory regime will bolster our Nation's security. Current cyber incident reporting regulations require too much of the private sector, drawing their attention away from actually securing their networks. Federal regulations, like the SEC's public cyber disclosure rule, clearly illustrate the urgent need for harmonization. This rule in particular is riddled with ambiguity and sets constrictive reporting time lines for organizations that experience cyber incidents.

Ambiguous and conflicting standards like the SEC rule are allowing compliance to take a priority over security, leaving our critical infrastructure more vulnerable to subsequent attacks. Injecting consistency and efficiency into the cyber regulatory regime is necessary to protect our Nation from digital threats to our critical infrastructure. The security of our homeland depends on effective cooperation between the private and public sectors, and it is our duty to help remove any unnecessary barriers to collaboration.

Since CIRCIA is still in the rule-making process until later this year, there is still time to ensure that regulatory effectiveness and

harmonization are core features of our national cyber incident reporting requirements. The final rule must not place an undue burden on private-sector entities that are critical to our national cyber defense.

I want to thank our witnesses, Scott Aaronson from Edison Electric, Heather Hogsett from Bank Policy Institute, Robert Mayer from USTelecom, and Ari Schwartz from the Cybersecurity Coalition, for being here today. Most of you have testified before during our hearings last May, and each provided invaluable insight to this subcommittee. Thank you for being here today.

With President Trump in office, we have a unique opportunity to create a common-sense cyber regulatory structure that ensures compliance serves its purpose to share actionable information with the Federal Government and with each other. As nation-state threats rise, we must do all we can to ensure that our cyber professionals can focus their precious time and attention and resources on securing networks and critical infrastructure and not on checking a box. I look forward to working with you as we pursue this shared objective. I yield.

Mr. GARBARINO. The Chairman yields back.

Other Members of the committee are reminded that opening statements may be submitted for the record.

[The statement of Ranking Member Thompson follows:]

STATEMENT OF RANKING MEMBER BENNIE G. THOMPSON

MARCH 11, 2025

Every day, we face efforts by adversaries like China and Russia to breach Government and critical infrastructure networks. To combat this risk, we need critical infrastructure entities to strategically increase their cyber defenses, and we need Government visibility into the threats we are facing.

Experience has demonstrated that a purely voluntary approach to cybersecurity is insufficient for today's threat landscape and that thoughtful regulations can improve security outcomes. With numerous Government agencies having regulatory authority over different critical infrastructure sectors, I understand the concerns from the private sector that regulations may be duplicative or inconsistent, resulting in unnecessarily burdensome compliance efforts.

Additionally, regulations risk being box-checking exercises rather than focusing on improved security outcomes. Therefore, efforts to improve cyber regulatory harmonization are important to ensuring regulations strengthen security and do not instead distract critical infrastructure from their security efforts.

The most meaningful step Congress has taken in recent years to address duplicative cybersecurity regulations was the enactment of the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) in 2022. Sponsored by Congresswoman Yvette Clarke, this legislation seeks to increase visibility into the current cyber threat landscape, by mandating critical infrastructure entities to report substantial cyber incidents to CISA. It also seeks to harmonize cyber incident reporting requirements by establishing CISA as a central reporting hub that can share cyber incident reports with other relevant agencies.

As I emphasized in comments I submitted to CISA, along with Ranking Member Swalwell and Representative Clarke, the proposed rule issued last year is overly broad and needs significant refinement in order to align with Congress's goals for the program. Additionally, I encourage increased engagement with stakeholders so that CISA can fully understand their concerns and can maximize the effectiveness of this new mandatory cyber incident reporting regime.

That being said, a final CIRCIA rule has tremendous potential to improve the Government's understanding of the cyber threats we face and to ultimately reduce the compliance burden on companies by harmonizing incident reporting requirements to a new CIRCIA standard.

By statute, CISA is required to issue a final rule by September of this year. It is essential that CISA work expeditiously to issue a final rule so that we can begin

to see the benefits of CIRCIA implementation and so that other agencies can begin work to align their incident reporting regimes to CIRCIA's.

Our adversaries are not pausing their efforts to breach our networks, and we cannot afford to pause our efforts to better defend them.

Relatedly, I am deeply concerned by the new administration's anti-regulatory attitude that risks undermining our security. While there is a need to streamline cybersecurity regulations, arbitrary policies that require eliminating regulations in order to issue any new ones would prevent agencies from responding to the evolving cyber threat landscape.

Instead, agencies must thoughtfully evaluate how to ensure critical infrastructure entities have the defenses in place to protect our networks and must coordinate efforts to create a more harmonized approach. We must avoid a simplistic discussion of more or less regulation and instead prioritize implementing policies that maximize security outcomes without unnecessary burdens.

I appreciate the support for CIRCIA from our witnesses, and I look forward to their testimony today on how to ensure proper implementation and improved regulatory harmonization.

Mr. GARBARINO. I am pleased to have a distinguished panel of witnesses before us today. I ask that our witnesses please rise and raise their right hand.

[Witnesses sworn.]

Mr. GARBARINO. Let the record reflect that all the witnesses have answered in the affirmative.

Thank you. Please be seated.

I would now like to formally introduce our witnesses. Mr. Scott Aaronson currently serves as senior vice president for energy security and industry operations for the Edison Electric Institute. In this role, he focuses on industry security and resilience initiatives establishing collaborative partnerships between Government and electric companies and across critical infrastructure sectors that enhance security for the energy sector. In addition to his role at EEI, Scott also serves as the Secretary for Electricity Subsector Coordinating Council, ESCC.

Ms. Heather Hogsett is the senior vice president and deputy head of BITS, the technology policy division of the Bank Policy Institute. In this position she develops and leads initiatives on emerging technology security resilience matters facing the Nation's largest financial firms. Ms. Hogsett also cochairs the policy committee of the Financial Services Sector Coordinating Council and is board member of fTLD Registry Services.

Mr. Robert Mayer is the senior vice president of cybersecurity innovation with the USTelecom Association. He is responsible for leading cyber and national security policy and strategic initiatives. In addition to this role, he serves as chairman of the Communications Sector Coordinating Council, which represents the broadcast, cable, satellite, wireless, and wire line industries in connection with DHS and public/private partnership activities across the U.S. Government. He also serves as cochair of the Council to Secure the Digital Economy.

Ari Schwartz currently serves as the coordinator for the Cybersecurity Coalition. In this role, he leads consortium of cybersecurity companies coordinating the Coalition's advocacy and education regarding cybersecurity policies. He also serves as the managing director of cybersecurity services for Venable where he helps organizations develop and implement cybersecurity risk management strategies. He was previously a member of the White House Na-

tional Security Council where he served as special assistant to the President and senior director for cybersecurity.

I thank the witnesses for being here today.

I now recognize Mr. Aaronson for 5 minutes to summarize his opening statement.

STATEMENT OF SCOTT I. AARONSON, SENIOR VICE PRESIDENT, ENERGY SECURITY & INDUSTRY OPERATIONS, EDISON ELECTRIC INSTITUTE

Mr. AARONSON. Thank you, Chairman Garbarino and Ranking Member Swalwell, Chairman Green, and to all the Members of the subcommittee. Appreciate the opportunity to testify today on cyber regulatory harmonization and specifically on implementation of the Cyber Incident Reporting for Critical Infrastructure Act of 2022, or more easily, CIRCIA.

My name is Scott Aaronson, and as noted, I am senior vice president for energy security and industry operations at the Edison Electric Institute. As you know, EEI is the trade association representing 250 million—companies that provide electricity to nearly 250 million Americans operating in all 50 States and the District of Columbia.

As I testified last May, EEI and its members wholly endorse the policy objectives underpinning CIRCIA. Incident reporting can help industry and our Government partners identify threats, see patterns, set policies, and prioritize risks to better protect critical infrastructure. CIRCIA is an important law with an important goal of identifying and mitigating cyber risks across all sectors of the economy, and I appreciate this committee's leadership in shepherding this effort these last several years.

When CIRCIA was enacted, Congress emphasized that the legislation sought to strike a balance between enabling CISA to receive information quickly and allowing the impacted entities to respond to an attack without imposing burdensome requirements that prioritize paperwork over cyber defense and response. Details matter when it comes to how CIRCIA or any new cybersecurity policy is implemented. Nearly a year after the subcommittee's hearing and my initial testimony on CIRCIA, we are in a period of transition with a new administration and a new Congress. Change brings opportunity, and I urge this subcommittee to leverage this opportunity to help ensure CISA is implementing CIRCIA effectively.

Both my written testimony and comments today focus on 2 main considerations for Congress when evaluating how best to proceed: First, the need to finalize the CIRCIA rule as mandated by statute so that electric companies and all critical infrastructure operators can benefit from this reporting to mitigate attacks and the disruptions they can cause; and, second, improving the existing proposal to better align with Congressional intent. CISA must do more to meaningfully incorporate industry feedback into the final rule to ensure reporting is not duplicative and that Government is a resource to ingest and protect this sensitive information.

Following the hearing last May, EEI has continued to engage with CISA on CIRCIA. In July 2024, EEI submitted 3 sets of comments on the proposed rule. In October 2024, EEI joined more than 20 organizations in requesting the establishment of an ex parte

process to enhance stakeholder engagement and facilitate on-going dialog for implementation.

As I once again testify before you alongside the financial services and telecommunications sectors representing some of the most sophisticated critical infrastructure operators, our collective concern remains that even the most mature sectors will be overburdened by the proposed rule if it were to be finalized as is. The committee should work with CISA to reduce this burden and focus on a few areas for improvement: First, conduct oversight regarding the current status of CIRCIA, including staffing levels, resource needs, projected time-line for final rule completion, and anticipated future engagement with industry stakeholders; second, facilitate coordination amongst Congressional committees of jurisdiction to align CISA, sector risk management agencies, and other regulators, and review concerns with existing Federal reporting requirements, including the national security concerns associated with the public disclosure of incidents as required by the U.S. Securities and Exchange Commission rule; third, further clarify CISA's role in cybersecurity regulatory harmonization in relation to other Federal entities; and, fourth, reauthorize the Cybersecurity Information Sharing Act of 2015. Mandatory incident reporting and voluntary information sharing both are valuable tools in ensuring the cybersecurity of critical infrastructure.

EEL and its members are committed to working with both public and private partners across all sectors to comply with incident reporting requirements, and cyber regulations more broadly, in a way that prioritizes and enhances critical infrastructure security. We look forward to working with you and CISA to finalize a rule that leverages existing regimes, provides meaningful insights to Government and industry, and protects sensitive information.

I'll also take a moment here to note, a little off script, that—the news this morning about the Critical Infrastructure Partnership Advisory Committee Act being rethought under this new leadership at the Department of Homeland Security. It's not our place to decide how Government organizes, but I want to highlight the value of industry-Government partnership, and CIPAC provides extraordinary protections for those partnerships and those partnership activities. Nearly 90 percent of critical infrastructure is owned by the private sector. It's critical because it's critical to national security, and it is critical to the life and safety of the communities that we serve. Industry and Government have to be working hand in glove, and, again, CIPAC provides a really valuable mechanism to do that.

We appreciate the bipartisan support of this committee in ensuring we get CIRCIA right and CIPAC right, and we look forward to continuing our collaboration to protect the safety, security, well-being of all Americans as we face evolving cyber risk. Thank you again for the opportunity to testify, and I look forward to your questions.

[The prepared statement of Mr. Aaronson follows:]

PREPARED STATEMENT OF SCOTT I. AARONSON

MARCH 11, 2025

INTRODUCTION

Chairman Garbarino, Ranking Member Swalwell, and Members of the subcommittee, thank you for the opportunity to testify. My name is Scott Aaronson, and I am senior vice president for energy security & industry operations at the Edison Electric Institute (EEI). EEI is the association that represents all U.S. investor-owned electric companies, which together are projected to invest more than \$200 billion this year to make the energy grid stronger, smarter, cleaner, more dynamic, and more secure against all hazards. That includes cyber threats. EEI's member companies provide electricity for nearly 250 million Americans and operate in all 50 States and the District of Columbia. The electric power industry supports more than 7 million jobs in communities across the United States. I appreciate your invitation to discuss this important topic on their behalf.

We rely on safe, reliable, affordable, and resilient energy to power our daily lives, run our Nation's economy, and support national security. Today, demand for electricity is growing at the fastest pace in decades, creating challenges for our Nation, as well as opportunities to ensure America is home to the industries, technologies, and jobs of tomorrow. America's investor-owned electric companies are uniquely positioned to meet growing demand and to address evolving risks, while working to keep customer bills as low as possible.

EEI'S COMMENTS ON CYBER REGULATORY HARMONIZATION

The electricity subsector is a part of the energy sector that is designated by National Security Memorandum/NSM-22 as one of the 16 critical infrastructure sectors whose assets, systems, and networks are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on national security, economic security, or public health and safety. The reliance of virtually all industries on electric power means that all critical infrastructure sectors have some dependence on the energy sector.

The electric subsector employs a risk-based, defense-in-depth approach to cybersecurity, including employing a variety of tools and strategies that support existing voluntary and mandatory cybersecurity standards and regulations, both of which are valuable tools in ensuring the cybersecurity of critical infrastructure.

Throughout the country, investor-owned electric companies are meeting and exceeding existing cybersecurity regulations and standards. As the Federal Government, States, and private sector work together to reduce risk holistically and continue to enhance cybersecurity protections of critical infrastructure, it is important that new cybersecurity requirements are not duplicative, conflicting, overlapping, or inefficient. Regulations that include flexibility and support for resilience, response, and recovery can help electric companies protect the electric grid. We also need to have strong partnerships in place across key sectors and with Government in order to maintain the robust cybersecurity posture needed to face the realities of potential cyber warfare.

In November 2023, EEI submitted comments on the Office of the National Cyber Director's (ONCD) Request for Information on Cybersecurity Regulatory Harmonization.¹ In summary, EEI's comments recognized that cybersecurity regulations must keep pace with the evolving threat landscape. Because industry owns, operates, and secures the majority of the energy grid, the Federal Government should incorporate industry's subject-matter expertise in developing and implementing new regulations and streamline processes from which new regulations may emerge. EEI's comments also provided examples of cybersecurity regulatory conflicts, inconsistencies, redundancies, challenges, and opportunities. Some of the key points that EEI made include:

- Effective communication between Government and industry is paramount to reconciling existing and future cybersecurity regulations;
- Harmonization is needed to address the high costs and inefficiencies caused by existing regulations or standards, or both;
- Harmonization efforts also must address third-party business partners;
- In addition to Federal regulations, EEI members also are subject to (and must comply with) many State, local, Tribal, and territorial cybersecurity requirements and standards; and,

¹ Comment from Edison Electric Institute, REGULATIONS.GOV, <https://www.regulations.gov/comment/ONCD-2023-0001-0039> (November 1, 2023).

- Additional matters to help harmonize cybersecurity regulations, such as:
 - Voluntary information sharing and protection;
 - Privacy laws and regulations;
 - Information handling;
 - Cloud security;
 - Contract terms; and,
 - Government coordination.

EEI'S ENGAGEMENT ON CIRCIA

While the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) is the first Federal cybersecurity reporting requirement focused specifically on reporting across all 16 critical infrastructure sectors, electric companies have been subject to similar Federal reporting for years pursuant to mandates imposed by the Federal Energy Regulatory Commission (FERC), the North American Electric Reliability Corporation (NERC), the Transportation Security Administration (TSA), and the Department of Energy (DOE). These existing reporting requirements should be considered by the Cybersecurity and Infrastructure Security Agency (CISA) as it determines how to implement its own cybersecurity and incident reporting regulations.

In May 2024, EEI had the opportunity to testify during this subcommittee's hearing entitled, "Surveying CIRCIA: Sector Perspectives on the Notice of Proposed Rulemaking."² EEI testified that one of our member electric companies estimated they could file roughly 65,000 reports through 2033 under the proposed rule—vastly exceeding CISA's estimate of more than 200,000 total reports during that period. In addition, our testimony highlighted that the Department of Homeland Security's (DHS) Cyber Incident Reporting Council (CIRC) report on harmonization identified that there currently are 45 different Federal cyber incident reporting requirements administered by 22 Federal agencies.³ We recommended that CISA thoroughly explore opportunities to limit duplicative reporting through the "substantially similar" exception of CIRCIA, and through the establishment of CIRCIA Agreements with Federal counterparts. EEI's testimony also identified several areas for enhancement of the proposed rule, including:

- Scope of substantial cyber incident definition;
- Volume of information requested;
- Workforce burden;
- Data preservation requirements; and
- Protection of information.

Following the hearing last May, EEI has continued to engage with CISA on CIRCIA. In July 2024, EEI submitted 3 sets of comments on the proposed rule. The first set of comments was sent on behalf of EEI's member electric companies and included feedback that was discussed in the May hearing, including:

- CISA's proposed definition of "substantial cyber incident" is too broad and therefore must be narrowed in scope;
- The amount of information required under the proposed rule is excessive, significantly increasing a covered entity's reporting burden while often contributing little analytical value;
- CISA must do all it can to protect reported information from threat actors and recognize its own limitations;
- The proposed rule's data-preservation requirements are unduly onerous;
- The proposed rule includes contrasting interpretations of the term "promptly" as it relates to the time frame within which covered entities must submit supplemental reports;
- CISA's proposed marking requirements need clarifying; and
- Harmonizing existing and proposed cybersecurity requirements is vital.⁴

The second set of comments was sent on behalf of the communications sector, electricity subsector, and financial services sector, encouraging CISA to limit the scope and raise the threshold for incident reporting by amending the definition of a substantial cyber incident in the final rule.⁵ Cosigners of these comments included

²Statement of Scott Aaronson, CONGRESS.GOV, <https://www.congress.gov/118/meeting/house/117105/witnesses/HHRG-118-HM08-WState-AaronsonS-20240501.pdf> (May 1, 2024).

³Harmonization of Cyber Incident Reporting to the Federal Government, DHS.GOV, <https://www.dhs.gov/sites/default/files/2023-09/Harmonization%20of%20Cyber%20Incident%20Reporting%20to%20the%20Federal%20Government.pdf> (September 19, 2023).

⁴Comment submitted by Edison Electric Institute, REGULATIONS.GOV, <https://www.regulations.gov/comment/CISA-2022-0010-0452> (July 5, 2024).

⁵Comment submitted by ABA, APPA, BPI, EEI, NRECA, NTCA, SIFMA, USTelecom, REGULATIONS.GOV, <https://www.regulations.gov/comment/CISA-2022-0010-0254> (June 28, 2024).

some of the most sophisticated critical infrastructure owners and operators across the United States, including the American Bankers Association, American Public Power Association, Bank Policy Institute, EEI, National Rural Electric Cooperative Association, NTCA—The Rural Broadband Association, Securities Industry and Financial Markets Association, and USTelecom—The Broadband Association.

The third set of comments was sent on behalf of more than 50 organizations seeking clarification on whether trade associations would be considered “covered entities” that are required to report cyber incidents to CISA under the proposed rule.⁶ The uncertainty around the inclusion of associations, which serve members within critical infrastructure sectors—but which do not own or operate critical infrastructure—in the definition of a covered entity is just one example of the ways in which CISA’s proposed rule is out of scope. These comments were intended to ensure CISA appropriately tailors reporting requirements to provide only the most relevant information necessary to protect homeland security.

Also in July 2024, subcommittee Chairman Andrew Garbarino,⁷ subcommittee Ranking Member Eric Swalwell, full committee Ranking Member Bennie Thompson, Rep. Yvette Clarke,⁸ (July 9, 2024), as well as then-Senate Homeland Security and Government Affairs Committee Chairman Gary Peters,⁹ submitted comments on the proposed rule. The feedback provided by Congress suggested that CISA mischaracterized or failed to meet the Congressional intent of CIRCIA. Universally, Congressional leaders have encouraged CISA to refine the scope of definitions and to meaningfully incorporate industry feedback in the final rule.

Finally, in October 2024, EEI, along with more than 20 organizations, sent a letter to CISA regarding the status of CIRCIA implementation, specifically requesting the establishment of an ex parte process to enhance stakeholder engagement and facilitate on-going dialog for its implementation.¹⁰ The letter urged CISA to:

- Adopt an ex parte process for on-going stakeholder engagement;
- Narrow the scope of CIRCIA to enable a positive cycle of information sharing and actionable insights;
- Proactively harmonize CIRCIA implementation with existing regulatory requirements to optimize operational response; and,
- Strengthen safeguards for information and protections against liability to support cyber attack victims and foster candor in reporting.

To date, CISA has not established an ex parte process and the status of the remaining recommendations remains unknown.

OPPORTUNITIES FOR CIRCIA AND RECOMMENDATIONS FOR CONGRESS

Nearly a year after this subcommittee’s hearing and EEI’s testimony on CIRCIA, we are in a period of transition with a new administration and a new Congress. Change brings opportunity—and I urge this subcommittee to leverage this opportunity to help CISA improve implementation of CIRCIA.

As we stated in our comments on the proposed rule, EEI and its members wholly endorse the policy objectives underpinning CIRCIA. CIRCIA is an important law with an important goal of identifying and mitigating cyber risks across all sectors of the economy, and I appreciate this committee’s leadership in shepherding this effort forward these last several years. When CIRCIA was enacted, Congress emphasized that the legislation sought to strike a balance between enabling CISA to receive information quickly and allowing the impacted entity to respond to an attack without imposing burdensome requirements. Details matter when it comes to how CIRCIA, or how any mandatory cyber incident reporting regime, is implemented. We need our most skilled cyber experts to be spending the majority of their time protecting America’s critical infrastructure, not filling out paperwork.

When evaluating how best to proceed, I encourage Congress to consider that:

- A final CIRCIA rule could help mitigate attacks and the disruptions they cause to American individuals and businesses. Therefore, improving the existing pro-

⁶Comment submitted by National Association of Manufacturers and 50 other trade associations, REGULATIONS.GOV, <https://www.regulations.gov/comment/CISA-2022-0010-0320> (July 3, 2024).

⁷Comment submitted by Congressman Andrew R. Garbarino, REGULATIONS.GOV, <https://www.regulations.gov/comment/CISA-2022-0010-0464> (July 9, 2024).

⁸Comment submitted by CHS—Ranking Member Bennie G. Thompson, Ranking Member Eric Swalwell, Rep. Yvette Clarke, REGULATIONS.GOV, <https://www.regulations.gov/comment/CISA-2022-0010-0463>.

⁹Comment submitted by Homeland Security and Government Affairs Committee, REGULATIONS.GOV, <https://www.regulations.gov/comment/CISA-2022-0010-0424> (July 3, 2024).

¹⁰Cross-sector Letter on CIRCIA Implementation, CYBERSCOOP.COM, <https://cyberscoop.com/wp-content/uploads/sites/3/2024/10/10.29.24-Cross-sector-Letter-on-CIRCIA-Implementation68.pdf> (October 29, 2024).

posal and finalizing the rule by the fall 2025 deadline, as mandated by statute, may be preferable to issuing a new proposed rule. A new proposal may cause confusion and unnecessary delays, as well as increase costly paperwork for both covered entities and the Federal Government.

- CISA faces several challenges in improving the existing proposal to better align with Congressional intent. These include difficulties in collaborating with industry stemming from the lack of an established ex parte process, as well as issues related to natural attrition and staff turnover following the change in administration. Additionally, uncertainty around Congressional appropriations may impact CISA's ability to effectively intake incident reports by the end of 2025.

RECOMMENDATIONS FOR CONGRESS

1. Conduct oversight regarding the current status of CIRCIA, including staffing levels, resource needs, the projected time line for final rule completion, and anticipated future engagement with industry stakeholders.
2. Facilitate coordination amongst Congressional committees of jurisdiction to:
 - a. Ensure alignment between CISA, Sector Risk Management Agencies, and other regulators, confirming that CIRCIA Agreements are developed in compliance with the law's substantially similar reporting exception; and
 - b. Review concerns with existing Federal reporting requirements, including the national security concerns associated with the public disclosure of incidents required by the U.S. Securities and Exchange Commission.
3. Further clarify CISA's role in cybersecurity regulatory harmonization in relation to other Federal entities, such as DHS and ONCD; and assess the next steps for the CIRC at DHS, as well as the legislative proposals recommended by CIRC in its harmonization report.
4. Reauthorize the Cybersecurity Information Sharing Act of 2015 (CISA 2015), a pivotal law that encourages and protects cyber threat information sharing between the Government and the private sector. While CISA 2015 is more about information sharing than incident reporting, both are essential to strengthening our collective cyber defenses to meet the evolving threat landscape.

CONCLUSION

Thank you again to this committee for holding today's hearing and for your ongoing efforts to strengthen America's energy security. EEI's member companies are committed to working with Federal partners and stakeholders across all sectors to achieve cyber regulatory harmonization that prioritizes and enhances U.S. critical infrastructure security. We appreciate the bipartisan support of this committee in ensuring we get CIRCIA right and we look forward to continuing our collaboration to protect the safety, security, and well-being of all Americans.

Mr. GARBARINO. Thank you, Mr. Aaronson.

I now recognize Ms. Hogsett for 5 minutes to summarize her opening statement.

STATEMENT OF HEATHER HOGSETT, SENIOR VICE PRESIDENT AND DEPUTY HEAD OF BITS, BANK POLICY INSTITUTE

Ms. HOGSETT. Thank you. Good morning Chairman Garbarino, Ranking Member Swalwell, Chairman Green, and honorable Members of the subcommittee. Thank you for inviting me to testify. I'm Heather Hogsett, senior vice president and deputy head of BITS, the technology division of the Bank Policy Institute.

BPI is a nonpartisan policy research and advocacy organization representing the Nation's leading banks. On behalf of BPI members, we greatly appreciate this committee's leadership and the opportunity to provide perspective on cybersecurity regulations.

As today's national security threats increasingly target vital infrastructure and our economy, it is imperative that industry and Government work together to have an awareness of cyber incidents and vulnerabilities while ensuring cyber teams can focus on day-to-day tasks, responding to incidents when they occur, and imple-

menting next-generation technologies. Unfortunately, the current state of cyber regulations detract from this vital work.

To support the Nation's security and resilience, we offer a few recommendations: First, streamline the reporting of cyber incidents to allow cyber teams to focus on response. I previously testified before this committee in support of the Cyber Incident Reporting for Critical Infrastructure Act, CIRCIA, and its goal to create a uniform incident reporting system. This would provide CISA with information it needs to have broader awareness of cyber threats and the tactics used by attackers. Armed with this information, CISA can better assess threats and provide early warning to help other entities protect themselves.

We continue to believe that CIRCIA, if properly implemented, will play an important role in our collective defense. However, as we noted in formal comments last June, it is critical that the final rule not extend beyond the authorities granted to it under the statute. Bipartisan Members of this committee, as well as Senator Peters, submitted comments emphasizing a similar view. Your comments were enormously helpful in reiterating Congressional intent, and we thank you for your continued leadership and engagement.

We, along with several other financial trade associations, recently asked that the current proposal be withdrawn and reissued. In particular, we encouraged CISA to significantly revise last year's proposed rule to reduce the scope of reporting to incidents affecting critical services, focus data collection on what companies need to know to prevent contagion, and reduce on-going reporting obligations.

At the same time, Congress and the administration should direct other agencies to cease issuance of bespoke reporting requirements. Some agencies, such as the Federal banking regulators, have incident notification requirements that are simple and serve a very specific operational or emergency response purpose. These requirements were developed in close collaboration with industry and work well in practice. Other agencies, however, continue to issue onerous reporting or disclosure requirements with different definitions, time-lines, and varying data elements that do not improve security outcomes.

One rule in particular is the SEC's requirement to disclose material cyber incidents within 4 business days, regardless of whether the incident has been contained or remediated. This rule should be rescinded as it undermines CIRCIA and confidential reporting and unnecessarily complicates incident response.

Second, we encourage Congress and the administration to consolidate industry-specific cyber regulations and regulatory oversight. This is a particularly acute challenge for financial institutions with multiple regulators. A survey of bank chief information security officers found that they spent 30 to 50 percent of their time on compliance and examiner management, and their teams can spend 70 percent of their time on those functions.

Firms receive on average 100 requests for information leading up to an exam, with anywhere from 75 to 100 supplemental requests during an exam that can take weeks if not months to complete. Once one exam is completed, another regulator often comes in to

examine the same or a similar topic. The current state risks undermining our security, and it is time for a reassessment.

Finally, we urge Congress to reauthorize cyber information sharing protections that expire this fall. The Cybersecurity Information Sharing Act of 2015 established important liability and antitrust protections for entities sharing cyber threat information, which were subsequently incorporated into CIRCIA. In the decades since their enactment, these protections have supported not only the sharing of cyber threat indicators but also broader awareness of vulnerabilities, knowledge of threat actors and their tactics, and effective defensive measures.

Recent attacks against public and private infrastructure underscore the importance of preserving these protections and the important information exchange they facilitate. We greatly appreciate this committee's thoughtful approach to these issues and stand ready to work with you to protect the security and resilience of our Nation's infrastructure. Thank you for the opportunity to speak today, and I'm happy to answer any questions.

[The prepared statement of Ms. Hogsett follows:]

PREPARED STATEMENT OF HEATHER HOGSETT

MARCH 11, 2025

Chairman Garbarino, Ranking Member Swalwell, and Honorable Members of the subcommittee, thank you for inviting me to testify. I am Heather Hogsett, senior vice president and deputy head of BITS, the technology policy division of the Bank Policy Institute.

BPI is a nonpartisan policy, research, and advocacy organization representing the Nation's leading banks. BPI members include universal banks, regional banks, and major foreign banks doing business in the United States. BITS, our technology policy division, works with our member banks as well as insurance, card companies, and market utilities on cyber risk management, critical infrastructure protection, fraud reduction, regulation, and innovation.

I also serve as co-chair of the Financial Services Sector Coordinating Council Policy Committee. The FSSCC coordinates across the financial sector to enhance security and resiliency and to collaborate with Government partners such as the U.S. Treasury and the Cybersecurity and Infrastructure Security Agency, as well as financial regulatory agencies.

On behalf of BPI member companies, I appreciate the opportunity to provide input on the status of the Cyber Incident Reporting for Critical Infrastructure Act, as well as the state of cybersecurity regulation, and ways to potentially harmonize existing requirements. There is an urgent need to reduce overlapping and duplicative regulatory requirements that present considerable challenges for many critical infrastructure entities. Financial institutions experience these challenges acutely when complying with a multitude of incident reporting requirements and during cyber-specific supervisory examinations conducted by numerous financial regulatory agencies.

As the Government surveys the current cyber regulatory landscape in search of increased efficiencies, it should prioritize: (1) Streamlining cyber incident reporting requirements to allow cyber personnel to focus on response efforts; and (2) consolidating cyber regulatory requirements and supervision.

CYBER INCIDENT REPORTING

To better align incident reporting requirements, Government agencies should consider: (1) substantial revisions to CISA's proposed rule to implement the Cyber Incident Reporting for Critical Infrastructure Act ("CIRCIA"); (2) rescinding the SEC's Cyber Incident Disclosure Rule; and (3) directing Federal agencies to stop issuing duplicative requirements and instead leverage CIRCIA as Congress intended.

Revise the CIRCIA Proposed Rule

Almost a year ago, I testified before this subcommittee shortly after CISA released its proposed rule.¹ During that hearing, I noted our members' concerns that CISA's proposal reflected an overly broad reading of the underlying statute and would add significant compliance obligations on front-line cyber personnel during the most critical incident response phase. As we move closer to the statutory deadline for CISA to issue its final rule, our members maintain those same concerns.

Financial institutions supported CIRCIA as it was being considered by Congress because it proposed a uniform incident reporting standard for critical infrastructure and sought to enhance CISA's ability to combat sophisticated cyber threats. Because CISA's proposal fell short of that aspiration, we—along with several other financial trade associations—recently reiterated this viewpoint in a letter to Department of Homeland Security Secretary Noem and Office of Management and Budget Director Vought requesting that they withdraw the current proposal and re-issue it more in line with Congressional intent.² While the current proposal is too broad in scope, we continue to believe that CIRCIA, if properly calibrated, can enhance our collective defenses and mitigate threats from foreign adversaries.

For that enhancement to be most effective, it is also important that Congress reauthorize the Cybersecurity Information Sharing Act of 2015 ("CISA 2015").³ The information, antitrust, and liability protections in CISA 2015 are imperative for public-private information sharing and provide the legal clarity companies need to share information not only with CISA but with other companies across critical infrastructure. The protections in CISA 2015 are also incorporated by reference in CIRCIA—making their reauthorization all the more critical. The expiration of the legal framework provided in the Act could substantially disrupt information sharing—leaving us all less prepared to confront emerging cyber risks.

As we noted in our joint financial trades response to CISA's proposal last June, it is critical that CISA's final rule not extend beyond the authorities granted to it under the statute.⁴ Bipartisan Members of this committee, along with Senator Peters, submitted comments emphasizing that same view.⁵ These responses were enormously helpful for reiterating Congressional intent, and we thank you for your leadership.

To adhere more closely to the CIRCIA statute, the final rule should limit reporting to information directly related to an actionable purpose—like detecting signs of a wide-spread vulnerability. Narrowing reporting data elements in this way would help give life to CIRCIA's "substantially similar" exception—something that would be unavailable to covered entities under the breadth of the current proposal. It would also lessen the burden of the supplemental reporting requirements which, as currently drafted, would likely require entities to file multiple additional reports during a single incident. Finally, CISA's rule should have reasonable thresholds for reporting above the standard proposed in the current substantial cyber incident definition that would likely cause a flood of reports on low-risk incidents.

Rescind the SEC Cyber Incident Disclosure Rule

Before the SEC finalized this rule in 2023, the financial sector raised significant concerns with its requirement to publicly disclose on-going cyber incidents.⁶ Chief

¹*Surveying CIRCIA: Sector Perspectives on the Notice of Proposed Rulemaking Before the Subcomm. on Cybersecurity and Infrastructure Protection of the H. Comm. on Homeland Security*, 118th Cong. (2024) (Statement of Heather Hogsett, Senior Vice President, Technology & Risk Strategy for BITS, Bank Policy Institute).

²Letter from the American Bankers Assoc., Bank Policy Inst., Inst. of Int'l Bankers, & Sec. Industry & Fin. Markets Assoc., to Kristi Noem, Secretary, Dep't of Homeland Sec. & Russell T. Vought, Director, Office of Mgmt. & Budget (Feb. 28, 2025), <https://bpi.com/wp-content/uploads/2025/02/CIRCIA-Letter-to-Noem-Vought-2.28.25.pdf>.

³Consolidated Appropriations Act, Pub. L. No. 114–113, Div. N, Title I—Cybersecurity Information Sharing Act, 129 Stat. 2935 (2015), 6 U.S.C. § 1501.

⁴American Bankers Assoc., Bank Policy Institute, Institute of International Bankers, & Sec. Industry & Financial Markets Assoc., Comment Letter on Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements (Jun. 28, 2024), <https://bpi.com/wp-content/uploads/2024/06/CIRCIA-Reporting-Requirements-Comment-Letter.pdf>.

⁵Representative Andrew Garbarino, Comment Letter on Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements (Jul. 3, 2024); Representatives Bennie G. Thompson, Yvette D. Clarke, & Eric M. Swalwell, Comment Letter on Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements (Jul. 3, 2024); Senator Gary Peters, Comment Letter on Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements (Jul. 2, 2024).

⁶Bank Policy Institute, American Bankers Assoc., Independent Community Bankers of America, & Mid-Size Banking Coalition of America, Comment Letter on Proposed Rules Regarding

among those concerns was that publicly disclosing on-going and unremediated cyber incidents could impair a victim company's ability to respond or otherwise exacerbate harm to the company, its shareholders, and customers. Unfortunately, those reservations were realized in November 2023 when ransomware group AlphV weaponized the public disclosure requirement as an additional ransom payment extortion method by reporting its own victim to the SEC.⁷ Given the pervasiveness of ransomware attacks, it is misguided to provide cyber criminals with an additional means to inflict financial harm on victim companies.

The public disclosure element of this rule is also problematic because it directly conflicts with the purpose of confidential incident reporting requirements. Although there are numerous confidential reporting rules across the Government, all generally aim to limit harm and warn potential downstream victims. Once an incident is publicly disclosed, however, that task becomes much more difficult to achieve. Using CIRCIA as an example, CISA will only have 24 hours to confidentially share threat indicators before an incident is publicly disclosed under the SEC rule. That leaves vulnerable companies with virtually no time to implement those controls before the incident is disclosed to the world. Rescinding the requirement that companies publicly disclose on-going cyber incidents will help eliminate unnecessary exposure to these threats.

Stop Duplicative New Requirements and Leverage CIRCIA

The financial sector complies with as many as 10 distinct incident reporting requirements in the United States alone.⁸ Many of these obligations were instituted over the past few years as agencies seemingly rushed to put out their own—and often conflicting rules. We understand that agencies have unique missions and therefore different information needs. Nonetheless, the patchwork of current requirements across the Government is past the point of helpful and now diverts finite resources away from incident response to filling out Government forms.

There are 3 general categories these rules fall into: (1) Incident notification; (2) confidential incident reporting; and (3) public incident disclosure. At one end of the spectrum, incident notification rules tend to be early during an incident investigation and simple—such as a phone call or email. They are used to inform an agency of an issue without requiring extensive data elements. We support and recognize the value of incident notification requirements for agencies with operational responsibilities or emergency authorities within critical infrastructure. An example of this is the financial regulatory agencies' Interagency Computer-Security Incident Notification Rule issued after substantive consultation with financial institutions.⁹

Confidential incident reporting requirements—like CIRCIA—involve more detailed responses and therefore often have slightly longer reporting time frames. They serve to provide Government with information to assess whether an incident might be wide-spread across different firms or sectors, to provide early warning to other entities or to contain an incident.

At the opposite end of the spectrum is the SEC disclosure rule which requires publicly alerting investors and others of an incident, regardless of whether mechanisms are in place—such as a software patch or the ability to disconnect from compromised networks—to prevent harm from spreading. As described above, this prioritization of investors' desire for information over critical incident response activities can exacerbate harm.

When enacting CIRCIA, Congress intended that it be “the primary means for reporting of cyber incidents to the Federal Government, that such reporting be through CISA, and that the required rule occupy the space regarding cyber incident

Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure Requirements (May 9, 2022), <https://bpi.com/wp-content/uploads/2022/05/05.09.22-BPI-ABA-ICBA-MCBA-SEC-Comment-Letter-2022.05.09.pdf>; Fin. Services Sector Coordinating Council, Comment Letter on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, <https://www.sec.gov/comments/s7-09-22/s70922-20128382-291285.pdf>.

⁷ AlphV files an SEC complaint against MeridianLink for not disclosing a breach to the SEC, DATABREACHES.NET (Nov. 15, 2023), <https://databreaches.net/2023/11/15/alphv-files-an-sec-complaint-against-meridianlink-for-not-disclosing-a-breach-to-the-sec/>.

⁸ DEPT OF HOMELAND SEC., HARMONIZATION OF CYBER INCIDENT REPORTING TO THE FEDERAL GOVERNMENT 9 (2023); U.S. DEPT OF HOUSING & URBAN DEVELOPMENT, FED. HOUSING ADMIN., MORTGAGEE LETTER 2024-23, REVISED CYBER INCIDENT REPORTING REQUIREMENTS (2024); U.S. DEPT OF HOUSING & URBAN DEVELOPMENT, GINNIE MAE, APM 24-02, CYBERSECURITY INCIDENT NOTIFICATION REQUIREMENT (2024).

⁹ Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers, 12 C.F.R. § 53 (2021).

reporting.”¹⁰ Because Congress was clear on this point, other Federal agencies should not create their own duplicative confidential reporting requirements.¹¹ Incident notification and disclosure requirements should also be reviewed to ensure they are critical to the agency requiring them and do not interfere with confidential reporting. Instead, agencies should leverage CIRCIA and enter into sharing agreements with CISA to receive relevant cyber threat information.

CONSOLIDATE CYBER REGULATORY REQUIREMENTS AND SUPERVISION

Financial institutions are continuously examined by the Office of the Comptroller of the Currency, Federal Reserve, and Federal Deposit Insurance Corporation, among others,¹² and often have hundreds of examiners on-site to review their cybersecurity practices. According to a survey of our member firms, bank chief information security officers now spend 30–50 percent of their time on compliance and examiner management. The cyber teams they oversee spend as much as 70 percent of their time on those same functions. In the lead-up to exams, financial institutions routinely receive over 100 requests for information, followed by 75 to 100 supplemental requests during an exam. Of those requests, firms report that roughly 25 percent duplicate requests from other agencies.

The cumulative effect of overlapping exams and regulatory requirements has created numerous unintended consequences. First, and as noted above, front-line cyber personnel now have significantly less time to perform their day-to-day security responsibilities as their bandwidth is consumed by compliance work. Relatedly, firms have paused or extended time frames for completing strategic program improvements to prepare for emerging threats. Finally, staff retention has become an issue as financial institutions report morale problems and burnout among staff driven by excessive compliance demands and rapid response deadlines.

Looking forward, there should be a careful review of the current regulatory regime to ensure it is calibrated appropriately. This should include actively exploring how to consolidate regulatory responsibilities in a way that better balances the oversight obligations of regulators and the security realities of private companies. Moreover, supervisory activities should primarily focus on outcomes and not box-checking procedural exercises unrelated to actual risk. Structured accordingly, regulators will better understand the true cybersecurity maturity of the firms they oversee and regulated entities will have the time they need to defend against sophisticated and well-resourced foreign threat actors.

CONCLUSION

We welcome the committee’s attention to this important issue. The financial sector has and will continue to support confidential information sharing to provide early warning and help prevent malicious attacks. This includes CIRCIA, which, if appropriately tailored to the statute and Congressional intent, will substantially improve awareness of cyber threats across the most important sectors of our economy. Harmonizing regulatory requirements is not a trivial task, but we are committed to working with this committee and other Federal agencies like CISA to advance that worthwhile goal.

Mr. GARBARINO. Thank you, Ms. Hogsett.

I now recognize Mr. Mayer for 5 minutes to summarize his opening statement.

¹⁰ Sen. Rob Portman, Comment Letter on SEC Proposed Rule on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure 4 (May 9, 2022), <https://www.sec.gov/comments/s7-09-22/s70922-20128391-291294.pdf>.

¹¹ See U.S. DEPT OF HOUSING & URBAN DEVELOPMENT, FED. HOUSING ADMIN., MORTGAGEE LETTER 2024–23, REVISED CYBER INCIDENT REPORTING REQUIREMENTS (2024); U.S. DEPT OF HOUSING & URBAN DEVELOPMENT, GINNIE MAE, APM 24–02, CYBERSECURITY INCIDENT NOTIFICATION REQUIREMENT (2024); CFTC Operational Resilience Framework for Futures Commission Merchants, 89 Fed. Reg. 4706 (Jan. 24, 2024).

¹² Other U.S. financial regulators include the Commodity Futures Trading Commission, Consumer Financial Protection Bureau, National Credit Union Administration, Securities and Exchange Commission, and State banking agencies.

**STATEMENT OF ROBERT MAYER, SENIOR VICE PRESIDENT,
CYBERSECURITY AND INNOVATION, USTELECOM, THE
BROADBAND ASSOCIATION**

Mr. MAYER. Chairman Garbarino, Ranking Member Swalwell, Chairman Green, and all honorable Members of the subcommittee, thank you for the opportunity to testify today on the critical issues of cybersecurity incident reporting and regulatory harmonization. We are committed to strengthening the public/private partnership to bolster our national security and stay ahead of our adversaries. This committee has an extraordinary opportunity to reset our national cybersecurity policies in ways that directly impact security outcomes.

Our Nation is under constant cyber attack with estimates of up to \$23 trillion in annual damages by 2027, increasing at a rate of more than 20 percent per year. We must take immediate action to eliminate redundant or conflicting cyber regulations, which can consume up to 70 percent of cybersecurity resources. By streamlining these requirements, we can free up critical resources for threat mitigation and incident response at virtually no cost.

Let me reaffirm our view that it is essential we fix how the Cyber Incident Reporting for Critical Infrastructure Act, CIRCIA, needs to be implemented. While well-intentioned, it is essential that we refine its execution to ensure consistency with the law's original intent, specifically key terms such as "covered incident," "covered entity," and "reasonable belief" must be clearly defined. The liability protections designed to safeguard cyber attack victims and promote candid reporting must be strengthened. As of today, none of these fundamental issues have been meaningfully addressed in a manner visible to industry, nor has our sector been substantively engaged in addressing these concerns.

We urgently need an ex parte process, which is to say, a formal, transparent, and common process that encourages CISA to hear and consider industry perspectives. In fact, USTelecom spearheaded a letter of 21 organizations that formally requested that CISA establish such a process, a request that was rejected. Had this request been granted immediately, we would've already been working together to resolve these challenges. If we do not act quickly, we will end up with a rule that does more harm than good.

We must also recognize that this law does not exist in isolation. The patchwork of Federal, State, and sector-specific cyber incident reporting requirements presents an ever-growing burden on organizations attempting to comply with multiple, often conflicting mandates. Fortunately, there is strong lawmaker interest to harmonize cyber regulations, including incident reporting requirements.

We believe that the Office of the National Cyber Director should play a leading role in rationalizing cybersecurity regulations and incident reporting regimes. Solving the problem of fragmented State laws will require clear Federal preemption, complemented by robust safe harbor provisions. This work must be prioritized, as it is directly tied to our national security.

We believe it is important that Congress acts now. We do not have time for further studies, requests for information, commissions, or pilot programs. Every moment spent delaying reform provides adversaries with additional opportunities to undermine our

collective security. We must move swiftly and decisively to enhance our cybersecurity posture.

Major recent cybersecurity incidents have highlighted the importance of stronger and more coordinated information sharing and incident response partnership between the Federal Government and the private sector. Congress advanced that project with the Cybersecurity Information Sharing Act of 2015, which set to sunset in September 2025. We ask that Congress extend the act and establish additional policies to improve the public/private partnership.

We must also be willing to reconsider policies that have failed to produce meaningful security benefits. One such example is the Securities and Exchange Commission's cyber disclosure requirements, which, rather than enhancing security, have inadvertently provided malicious actors with a road map to exploit vulnerabilities. These mandates must be reassessed to prevent them from serving as a tool for cyber criminals.

In conclusion, success in cybersecurity requires close collaboration between the industry and Government, including Congress and the Office of the National Cyber Director. We must act now to ensure that our cybersecurity policies are well-reasoned, well-informed, and designed to maximize efficiency and effectiveness. By fixing CIRCIA's implementation, harmonizing cyber regulations, and eliminating unnecessary burdens, we can strengthen our Nation's cybersecurity defenses and uphold our commitment to protecting national security.

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

[The prepared statement of Mr. Mayer follows:]

PREPARED STATEMENT OF ROBERT MAYER

MARCH 11, 2025

Chairman Garbarino, Ranking Member Swalwell, and Members of the subcommittee, thank you for the opportunity to testify today on the critical issues of cybersecurity incident reporting and regulatory harmonization. We are committed to strengthening the public-private partnership to bolster our national security and stay ahead of our adversaries. This committee has an extraordinary opportunity to reset our national cybersecurity policy in ways that directly impact security outcomes.

Our Nation is under constant cyber attack, with estimates of up to \$23 trillion in annual damages by 2027, increasing at a rate of more than 20 percent per year.¹ We must take immediate action to eliminate redundant or conflicting cyber regulations, which can consume up to 70 percent of cybersecurity resources.² By streamlining these requirements, we can free up critical resources for threat mitigation and incident response—at virtually no cost.

Let me reaffirm our view that it is essential we fix how the Cybersecurity Incident Reporting for Critical Infrastructure Act (CIRCIA) needs to be implemented. While well-intentioned, it is essential that we refine its execution to ensure consistency with the law's original intent. Specifically, key terms such as “covered incident,” “covered entity,” and “reasonable belief” must be clearly defined. The liability protections designed to safeguard cyber attack victims and promote candid reporting must be strengthened. As of today, none of these fundamental issues have been meaningfully addressed in a manner visible to industry, nor has our sector been substantively engaged in addressing these concerns.

We urgently need an ex parte process—which is to say a formal, transparent, and common process that encourages CISA to hear and consider industry perspectives.

¹ See The Economist, “Unexpectedly, the cost of big cyber-attacks is falling” (May 17, 2024).

² Chamber of Commerce, Briefing with Majority and Minority Staff of Senate Homeland Security and Government Affairs Committee (May 29, 2024).

In fact, USTelecom spearheaded a letter by 21 organizations that formally requested that CISA establish such a process; a request that was rejected.

Had this request been granted immediately, we would have already been working together to resolve these challenges. If we do not act quickly, we will end up with a rule that does more harm than good.

We must also recognize that this law does not exist in isolation. The patchwork of Federal, State, and sector-specific cyber incident reporting requirements presents an ever-growing burden on organizations attempting to comply with multiple, often conflicting, mandates. Fortunately, there is a strong lawmaker interest to harmonize cyber regulations, including incident reporting requirements.

We believe the Office of the National Cyber Director (ONCD) should play a leading role in rationalizing cybersecurity regulations and incident reporting regimes. Solving the problem of fragmented State laws will require clear Federal preemption, complemented by robust safe harbor provisions. This work must be prioritized, as it is directly tied to our national security.

We believe it is important that Congress acts now. We do not have time for further studies, requests for information, commissions, or pilot programs. Every moment spent delaying reform provides adversaries with additional opportunities to undermine our collective security. We must move swiftly and decisively to enhance our cybersecurity posture.

Major recent cybersecurity incidents have highlighted the importance of a stronger and more coordinated information sharing and incident response partnership between the Federal Government and the private sector. Congress advanced that project with the Cybersecurity Information Sharing Act of 2015, which is set to sunset in September 2025. We ask that Congress extend the Act, and establish additional policies to improve the public-private partnership.

Key pillars for improve this partnership include:

- *There Should Be a Single Responsible Federal Agency for Major Cybersecurity Incidents.*—In the midst of a major incident, an operator’s cybersecurity team is tightly focused on understanding and mitigating the challenge, and may be coordinating with other affected entities and/or with one or more law enforcement or national security agencies. It is practically difficult and often inadvisable to pull away from those operational imperatives to engage in briefings or other general information sharing and analysis activities (which takes substantial time and effort) with multiple Government stakeholders absent concrete benefits to doing so.
- Accordingly, Congress should ensure a unified, whole-of-Government approach to major cybersecurity incidents: In the wake of a major incident with national security implications, a single “Responsible Agency” should have formal responsibility for (i) coordinating with the private sector and (ii) overseeing Government information sharing during a cybersecurity event.
- *Power to Suspend Reporting Obligations.*—Congress should grant the Responsible Agency the power to suspend all Federal, State, and contractual reporting obligations upon a finding that doing so is in the national interest. Otherwise, the existing patchwork of reporting regimes (e.g., FCC, SEC, CIRCIA, Government contracts, private contracts) could cause highly sensitive information to be promulgated in a haphazard manner.
- *Expanded Government Sharing of Actionable Cybersecurity Information.*—Whether sharing information about a specific incident or a potential or known threat, the Government should focus on getting detailed, actionable tactical information in the hands of the private-sector personnel responsible for protecting communications networks.
- *Security Clearances for Private-Sector Leaders.*—Private-sector CISOs and other key cybersecurity professionals should be granted security clearances (subject to appropriate vetting). Security clearances should not be tied to whether an individual is involved in a particular Government project or program.
- *Secure transfer mechanisms.*—Congress should fund a streamlined method for Government agencies and the private sector to securely transmit and receive sensitive information.
- *Promote Meaningful Private-Sector Sharing of Sensitive Information.*—Policies for promoting information sharing need to promote voluntary private-sector information sharing:
- *Confidentiality of information shared by industry.*—Enact legislation that would create major penalties for individuals within the Government that breach confidentiality or share information without authorization during a national security cyber attack investigation. The private sector will not share

highly-sensitive information with the Government if there is a risk Government employees receiving the information will leak it.

- *Immunity for information shared by industry.*—Establish a strong “Reverse Miranda” regime where information shared by a private actor cannot be used against it in any future action or proceeding.
- *Limited number of recipients.*—Private actor needs assurances that sensitive information it shares will only be available to a small number of Government officials and companies. Operators will not meaningfully share information if the pool of recipients is too large or includes potentially untrusted persons/entities.

We must also be willing to reconsider policies that have failed to produce meaningful security benefits. One such example is the Securities and Exchange Commission’s (SEC) cyber disclosure requirements, which, rather than enhancing security, have inadvertently provided malicious actors with a road map to exploit vulnerabilities. These mandates must be reassessed to prevent them from serving as a tool for cyber criminals.

In conclusion, success in cybersecurity requires close collaboration between industry and Government, including Congress and the Office of the National Cyber Director. We must act now to ensure that our cybersecurity policies are well-reasoned, well-informed, and designed to maximize efficiency and effectiveness. By fixing CIRCIA’s implementation, harmonizing cyber regulations, and eliminating unnecessary burdens, we can strengthen our Nation’s cyber defenses and uphold our commitment to protecting national security.

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

Mr. GARBARINO. Thank you, Mr. Mayer.

I now recognize Mr. Schwartz for 5 minutes to summarize his opening statement.

STATEMENT OF ARI SCHWARTZ, COORDINATOR, CYBERSECURITY COALITION

Mr. SCHWARTZ. Thank you Chairman Garbarino, Ranking Member Swalwell, Chairman Green, Members of the subcommittee. Thank you for having me here to appear before you today. It’s an honor to be here to discuss the widely-shared goals of harmonizing cybersecurity regulations.

My name is Ari Schwartz. I am coordinator of the Cybersecurity Coalition, the leading policy coalition representing companies that develop cybersecurity products and services.

As cybersecurity threats continue to grow, calls for cybersecurity regulation around the world have increased as well. In the United States, choices that Congress made 10 to 15 years ago led most cybersecurity regulations to be overseen by the current sectorial regulators. This has the convenience of maintaining the current relationship between the regulated company and the regulator. Organizations are overseen by agencies that know that sector.

But each agency is not going to have full expertise in cybersecurity. New cross-sector and international regulations have continued to grow, making harmonization difficult. But it’s not impossible. Agencies must work extra hard to ensure that regulations can align so we are not overburdening organizations and putting so much work on compliance that we are draining resources that otherwise could go to actually improving security.

The example where this is most obvious today is around incident reporting. Incident reporting allows agencies to track what’s happening in and across sectors, and, in the best-case scenario, alert potential victims before it’s too late. However, as DHS pointed out in a report to Congress in 2023, 45 different incident reporting requirements have been created led by 23 different agencies. Inter-

nationally, the reporting regimes have grown equally large. These reports are on different time frames, use different types of information, and use different taxonomies to describe the information. This has led to duplication, misalignment, and general confusion.

In 2022, Congress passed CIRCIA, a law intended to have critical infrastructure standardized reporting and send it to CISA. CISA ran a process to receive comments on how this reporting should work and issued a notice of proposed rulemaking in 2024. It is the cybersecurity coalition's view that the proposed rule did not meet Congress' goal of adequately harmonizing incident reporting requirements.

First of all, there was a lack of engagement. While CISA clearly tried to follow the letter of the law in getting comments on the rule making, it failed to adequately engage the sectors. The open sessions that were held were rote and did not address known concerns of the community. The CISA representatives simply repeated the same questions CISA had originally posed.

Second, there is an overbroad scope in the proposed rule. Instead of harmonizing around existing rules or best practices identified by other sectors, CISA decided to create a new broad definition of covered entities. CISA also decided to create a new construct of what triggers reporting and when it needs to be reported.

Last, there is a failure to streamline the reporting. While CISA made some attempts to ensure that the report filed with CISA would be shared with others that might require it, the proposed rule did not go far enough to demonstrate that CISA was attempting to solve the problem of duplicative reporting, seemingly placing the onus on the reporting on the organizations.

We believe that these issues can be addressed if CISA makes a commitment to meeting with the sectors. We suggest this be done through an ex parte rule-making process using the critical infrastructure partnership known as CIPAC. However, we have heard that Secretary Noem last week shut down the CIPAC, which we think is a mistake for many reasons, with this process being a good example, where the CIPAC process can play a critical role in the public/private partnership.

Finally, while we were talking about the importance of sharing information with the Government, I would be remiss not to speak up in favor of reauthorization of the Cybersecurity Information Sharing Act of 2015. This law has provided the ability for companies to share cyber threat information among themselves and with Government. It has streamlined the definition of cyber threat information and has allowed multiple groups to form and to share that information to quickly stop in order to respond to incidents. We hope that reauthorization of that—of the law is a priority for this subcommittee.

I thank you, and I look forward to your questions.
[The prepared statement of Mr. Schwartz follows:]

PREPARED STATEMENT OF ARI SCHWARTZ

MARCH 11, 2025

INTRODUCTION

Thank you, Chairman Garbarino, Ranking Member Swalwell, and Members of the subcommittee for inviting me to appear before you today. It is an honor to be here to discuss the critical importance of harmonizing cybersecurity regulations.

My name is Ari Schwartz, and I am the coordinator of the Cybersecurity Coalition, the leading policy coalition representing companies that develop cybersecurity products and services.¹ In my role, I focus on advancing efforts related to regulatory harmonization, ensuring that cybersecurity laws and standards are streamlined, effective, and efficient for businesses and the public sector alike.

Over the past 20 years, Congress has made significant efforts to ensure our Nation is protected without also overburdening the companies that run our critical infrastructure. Between 2011 and 2015, Congress debated legislation that would have centralized control of critical infrastructure protection regulatory efforts and instead, chose to leave the majority of the control to each sector's existing regulators. Congress decided that the sectors had inherent differences—including terminologies and requirements—and therefore needed to maintain separate regulatory regimes.

Meanwhile, efforts to address the evolving cyber threat landscape have prompted the development of new sector-specific and cross-sector requirements. These requirements apply not only within the private sector but also across all levels and branches of Government, both in the United States and around the world. While necessary to secure our Nation's critical infrastructure and systems, these requirements have also resulted in a complicated, fragmented, and duplicative regulatory regime. This has created undue burdens and pressures for critical infrastructure owners and operators, making compliance both difficult and time-consuming. For example, companies face continuous updates to mapping exercises for various compliance regimes. Keeping pace with the flood of rule making and industry feedback opportunities requires resources: time, tracking tools, consultants, security leaders' input, and more. It is simply not a good use of limited security resources.²

CYBER INCIDENT REPORTING

One area where the burden of regulatory requirements on companies unquestionably continues to grow is around cyber incident reporting.

In many ways, incident reporting is a perfect demonstration of the broader issue. Governments continue to seek ways to utilize incident data to quickly spot patterns of incidents and respond to them. In order to get that information, there are increasing requests and requirements for more detailed incident response data to be sent to a growing number of organizations.³ As more organizations build reporting struc-

¹ Cybersecurity Coalition is dedicated to finding and advancing consensus policy solutions that promote the development and adoption of cybersecurity technologies. We seek to ensure a robust marketplace that will encourage companies of all sizes to take steps to improve their cybersecurity risk management. We are supportive of efforts to identify and promote the adoption of cybersecurity best practices, information sharing, and voluntary standards throughout the global community. Our members include Broadcom, Cisco, Cybastion, Google, Infoblox, Intel, Kyndryl, Microsoft, Palo Alto Networks, Rapid7, RedHat, Schneider Electric, Tenable, Trellix, Wiz, and Zscaler.

² During the last administration, several important steps were taken to address this issue: The White House Office of the National Cyber Director (ONCD) launched an initiative to review cybersecurity regulations, gathering input from stakeholders.

Request for Information Opportunities for and Obstacles to Harmonizing Cybersecurity Regulations, Office of the National Cyber Director, 88 Fed. Reg. 55694, Aug. 16, 2023, <https://www.whitehouse.gov/wp-content/uploads/2024/06/Cybersecurity-Regulatory-Harmonization-RFI-Summary-ONCD.pdf>.

Senators Peters and Lankford introduced the Streamlining Federal Cybersecurity Regulations Act, which sought to establish an ONCD-led process for developing a harmonized regulatory framework and review new regulations for alignment.

S. 4630, Streamlining Federal Cybersecurity Regulations Act, 118th Cong., <https://www.congress.gov/bills/118/congress/118th-congress/senate-bills/4630>.

Meanwhile, across the Atlantic, the European Union has acknowledged that its cybersecurity rules have created overlap and burden and is looking to streamline existing regulations, reduce administrative burdens and ensure a more cohesive approach to cybersecurity. https://commission.europa.eu/law/law-making-process/better-regulation/simplification-and-implementation_en.

³ The 2023 Department of Homeland Security Congressional Report, *Harmonization of Cyber Incident Reporting to the Federal Government*, "identified 45 different Federal cyber incident re-

Continued

tures for different purposes, duplication, misalignment, fragmentation, and other issues start to set in. This includes concerns around the amount and types of data fields, differing taxonomies, time frames for reporting, and more.

Harmonizing cyber incident reporting would bring benefits to both public and private-sector efforts to strengthen cybersecurity. It would improve coordination and response capabilities, enhance data quality, accelerate threat detection and mitigation, and enable more effective policy making and resource allocation.

The Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA)⁴ was enacted in 2022, requiring critical infrastructure owners and operators to report cyber incidents and ransomware payments to the Cybersecurity and Infrastructure Security Agency (CISA). CISA formally solicited input from industry to inform this reporting structure, including which entities should report and what type of data should be reported.

The Cybersecurity Coalition is generally supportive of CIRCIA's objectives, and we acknowledge that CISA was given a difficult task to develop a reporting regime that encompasses all critical infrastructure sectors. Congress specifically required CISA to prioritize harmonization efforts to "avoid conflicting, duplicative, or burdensome requirements" across the sectors. In its proposed rulemaking, we do not believe CISA met this essential goal.⁵ In particular:

- *Lack of Sectoral Engagement.*—CISA did not adequately engage in working with the critical infrastructure sectors to discuss how to best harmonize existing efforts. In particular, despite the explicit mention of the need for "coordination" with the Critical Infrastructure Partnership Advisory Committee (CIPAC) and information sharing and analysis organizations in CIRCIA, CISA included almost no means of ex-parte engagement for them. The Cybersecurity Coalition believes that CISA should immediately begin meeting with the Sector Coordinating Councils under the CIPAC and the members of the Council of Information and Sharing and Analysis Center in a coordinated ex-parte process that Congress intended.

CISA should also work more closely with the Office of Management and Budget and other Federal agencies to facilitate reciprocity and harmonization to streamline incident reporting under CIRCIA's statutory language. This includes promoting greater collaboration between DHS; Federal agencies; State, local, Tribal, and territorial (SLTT) agencies; as well as international partners.

- *Overbroad Scope.*—In its definition of "covered entities," rather than relying on existing definitions or trying to coordinate among existing efforts, CISA decided to create a complex new definition. It has two categories: those within critical infrastructure sectors, with exceptions for small businesses and those meeting sector-specific criteria.⁶ In many cases, it may not be immediately clear whether an entity is covered by the proposed reporting requirements but because the requirements focus on size rather than what the company actually does, it almost certainly covers companies who have probably never before been considered "critical infrastructure." We do not think that this was Congress' intent.

Also, mixing the broad scope of covered entities with a very broad definition of "covered cyber incidents," the Cybersecurity Coalition is concerned that this rule may lead to an overwhelming number of incident reports.⁷ This influx of less relevant reports could burden CISA's incident reporting system, requiring significant additional resources for analysis, triage, and transformation into actionable intelligence. While the goal of CIRCIA is to ensure enough data is provided to create a comprehensive picture to inform policy and response actions, we believe that there is a point where too much data creates unnecessary noise that distracts from the core mission. CISA should prove they can effectively

porting requirements created by statute or regulation" being "administered by 22 Federal agencies", with another "7 proposed rules that would create a new reporting requirement or amend a current requirement, and 5 additional potential new requirements or amendments under consideration but not yet proposed." <https://www.dhs.gov/sites/default/files/2023-09/Harmonization%20of%20Cyber%20Incident%20Reporting%20to%20the%20Federal%20Government.pdf>.

⁴Pub. L. 117–103 Title V, Div Y.

⁵Proposed Rule Cyber Incident Reporting for Critical Infrastructure Act Reporting Requirements, Cybersecurity and Infrastructure Security Agency, 89 Fed. Reg. 23644, Apr. 4, 2024, <https://www.federalregister.gov/documents/2024/04/04/2024-06526/cyber-incident-reporting-for-critical-infrastructure-act-circia-reporting-requirements>.

⁶89 Fed. Reg. 23644, 23660.

⁷Cybersecurity Coalition Comments, Request for Information on the Cyber Incident Reporting for Critical Infrastructure Act, June 28, 2024, [https://cdn.prod.website-files.com/660ec3caef47b817d72800ae/6684487fa6bfc5ed0c2a12a_Cybersecurity%20Coalition%20%20FINAL%20Comments%20to%20CISA%20re%20CIRCIA%20Proposed%20Rule%206.28.24%20\(2\).pdf](https://cdn.prod.website-files.com/660ec3caef47b817d72800ae/6684487fa6bfc5ed0c2a12a_Cybersecurity%20Coalition%20%20FINAL%20Comments%20to%20CISA%20re%20CIRCIA%20Proposed%20Rule%206.28.24%20(2).pdf).

work with the enormous influx of data we'd expect they would receive using the existing construction of critical infrastructure and with a more modest definition of types of reports requested before considering expanding their scope.

The Cybersecurity Coalition believes that CISA should narrow the scope of "covered entities" under CIRCIA. Instead of applying reporting requirements to all entities within critical infrastructure sectors, Congress should direct CISA to "focus on Systemically Important Entities (SIEs) that own or operate critical infrastructure systems and assets whose disruption would have a debilitating, systemic, or cascading impact on national security, the economy, public health, or public safety."⁸ This would help Congress uphold its original intent to focus on the most essential infrastructure while avoiding unnecessary regulatory burden on less critical entities.

- *Failure to Streamline Reporting.*—The proposed rule lacks clear measures to streamline reporting processes. Although the idea of "substantially similar" reporting requirements could help address duplicative reporting across different frameworks, the definition of "substantially similar" remains unclear. The proposed rule requires CISA and relevant agencies to establish a "CIRCIA Agreement" to ensure their reporting requirements align with this standard. However, CISA retains the authority to limit exceptions for substantially similar reports to agencies with formal agreements. The Cybersecurity Coalition is concerned that this broad and prescriptive approach could reduce reciprocity and create additional burdens for entities striving to align with these standards.⁹ The Cybersecurity Coalition believes that CISA should support efforts to streamline Federal cybersecurity regulations to ensure businesses are not burdened by multiple, conflicting obligations. By passing legislation that promotes the development of standardized incident reporting processes, Congress can make it easier for companies to comply with regulatory requirements while limiting agency overreach.

The Cybersecurity Coalition would prefer to see CISA issue a new version of the proposed rule that addresses these concerns and then receive comments on that draft and issue a final rule in the time frame originally proposed by Congress. Unfortunately, Secretary Noem has now reportedly disbanded the CIPAC,¹⁰ which will make getting comments from all of the sectors much more difficult. We hope the Secretary will reinstate the CIPAC. If not, in order to effectively receive feedback, it will likely be necessary for CISA to simply rescind the rule and start over. This would be a disappointing outcome considering the amount of time already expended on this effort and the fact that CISA would likely miss Congress' intended time line.

THE CYBERSECURITY INFORMATION SHARING ACT OF 2015

While we are discussing the importance of using data to address and prevent cyber incidents, I would be remiss not to mention the importance of the Cybersecurity Information Sharing Act of 2015 (CISA 2015).¹¹ CISA 2015 provides companies liability protections when sharing a very narrowly-defined set of cyber threat information.

We can think of CISA 2015 as lowering the burden on organizations by simplifying the way that companies share information amongst other companies and with the Government and the purposes of that sharing. While CISA 2015 was somewhat controversial at the time of its creation, it has been anything but controversial in practice. CISA should be commended for the fine job they did with the Department of Justice in creating the complicated guidance necessary for CISA 2015.

The Cybersecurity Coalition supports the reauthorization of CISA 2015. We urge this committee to take the lead in making its introduction and passage a priority. We look forward to working with you on this effort.

CONCLUSION

In conclusion, the path forward in strengthening our Nation's cybersecurity lies in harmonizing and streamlining regulations. It is critical that we create a regulatory environment that allows organizations to focus on meaningful cybersecurity practices rather than navigating complex, burdensome, and conflicting require-

⁸ Cybersecurity Coalition Comments, Request for Information on the Cyber Incident Reporting for Critical Infrastructure Act of 2022, Nov. 14, 2022, https://cdn.prod.website-files.com/660ec3caef47b817df2800ae/660ec3caef47b817df280233_Comments%20CISA%20CIRCIA-%20RFI%20%20Docket%20Number%202022-19551%20-%20CISA-2022-0010%2011.14.22.pdf.

⁹ Id.

¹⁰ <https://subscriber.politicopro.com/newsletter/2025/03/estonias-cyber-Ambassador-weighs-in-00220220>.

¹¹ 6 USC 1503.

ments. On behalf of the Cybersecurity Coalition, I strongly urge Congress to continue prioritizing this issue and push CISA to address key concerns in CIRCIA, including clarifying the definition of covered entity, refining the scope of covered cyber incident, and ensuring reciprocity across frameworks.

We appreciate the work Congress has done, and we are committed to working alongside you to ensure cybersecurity regulations are effective and efficient. Thank you for the opportunity to testify. I look forward to your questions.

Mr. GIMENEZ [presiding]. Thank you, Mr. Schwartz.

Members will be recognized by order of seniority for their 5 minutes of questioning. I want to remind everyone to please keep their questioning to 5 minutes. An additional round of questioning may be called after all Members have been recognized.

I now recognize the gentleman from Tennessee, the Chairman of the committee, Mr. Green, for 5 minutes of questioning.

Mr. GREEN. Thank you.

First, let me say, the testimony today has been superb. I—my questions will be to reiterate points you've made. In fact, I just told my senior staffer for cybersecurity to get copies of everyone's testimony and provide it at the cyber subs meeting. The cyber subs committee, I started this last year, some of you may be aware of this, where we meet all the cyber subcommittees to try to get a whole-of-Government approach here. We're going to send copies of your testimony to every cyber subcommittee Member in this Congress. This was excellent. Thank you.

You know, Congress has a duty—let me make this point: Congress has a duty that we have shirked over 40 years in both parties and passed off to the bureaucracy. The Constitution is really clear. A lot of these things that the administration is now closing, Chevron deference, and the Supreme Court have ruled it really belonged to Congress in the first place and we never should have passed it off to the doggone administration in the bureaucracy. Right? So I get that there's some frustration that certain things are being closed, but, I mean, Constitutionally, we need to do that here. It's a part of our oversight obligation. It's a part of our particularly reporting and review boards and things like that.

I was told yesterday—and I don't know if it's completely true. I've got to fact check this, but the VA spends \$1 billion on compliance. Does that seem reasonable, \$1 billion on compliance? These conflicting rules and this—all this time, I think, Ms. Hogsett, you said 30 percent on actual just checking the box compliance and 70 percent on real cybersecurity. Was that the ratio you quoted?

Ms. HOGSETT. Thirty to 50 percent of the chief information security officer's time is—

Mr. GREEN. Is on checking the box.

Ms. HOGSETT [continuing]. Spent on that and 70 percent of their team's.

Mr. GREEN. Ridiculous.

Let me ask this question: What is the average time to close a vulnerability when one has been identified? I—just, give me a number of days. I'm going to run the—the average vulnerability, closing the door takes how long? Take a guess.

Mr. AARONSON. You're going to hate this answer: It depends.

Mr. GREEN. Great.

Ms. HOGSETT. True. If it's a critical vulnerability firm has worked to close that within days if possible. It all depends on whether you align—

Mr. GREEN. What is it for?

Ms. HOGSETT. It would depend on how much control you have over it. If it something that resides within a third party, you have less control and ability to move quickly to close it.

Mr. GREEN. OK.

Mr. MAYER. Yes. I don't want to speculate, sir, on an average, but I will tell you that if you look at the recent attacks that are coming from nation-states, it's taken weeks, months, and it's still a process that is under way.

Mr. GREEN. Yes. Well, I'm not sure we've patched the telecom breach yet.

Mr. SCHWARTZ. So if we're talking about, like, browsers, they can close them in hours. But if you're talking operational technology, it takes days.

Mr. GREEN. Days?

Mr. SCHWARTZ. Yes.

Mr. GREEN. Yes. SEC pulls the number 4 days out of their backside and thinks that they're doing shareholders a positive. But when they announce that they've got a hole in the door, in the wall, and it's not going to be closed, it invites attack from everybody. It's the stupidest thing I've ever heard of.

Let me ask this question—we've got to go and figure out all this list of duplicity, list of conflicting—how best do we as Congress, does this subcommittee and the subcommittees across our Congress, figure out all the lists of duplicative requirements and contradictory requirements? How do we go get this information?

Mr. AARONSON. So, first of all, I appreciate what you said about the coordination across all the committees of jurisdiction. I think understanding—the first thing a cyber—a CISA or CSO is going to do is inventory their entire system to understand where vulnerabilities might be. I'd say that Congress needs to inventory the system, understand where all of the regulatory requirements are so that we can start to do the hard work of harmonizing.

Just to foot-stomp something that you said about the lunacy of the SEC rule, adversaries—and to talk about the vulnerabilities and a time to patch—adversaries watch our response. I understand, you know, the importance of sunshine and transparency, but we also have to understand that intelligent adversaries are leveraging our transparency when perpetrating attacks and seeing how we respond.

Mr. GREEN. Don't we list the identified vulnerabilities somewhere in a database, that the bad guys can sit there and take a look at, and then challenge and find where that vulnerability is anywhere in the system?

Mr. AARONSON. Those vulnerabilities become a little less important when everybody knows about them, so there is that—

Mr. GREEN. There's always that legacy system that's still running, the old thing that nobody catches and it's an open door. That's what worries me there, Mr. Schwartz.

Mr. SCHWARTZ. I was going to say, I mean, they shouldn't—you shouldn't post—this is one of the reasons we say don't—that we need a patch before you post a vulnerability. So—

Mr. GREEN. Yes, exactly.

Mr. SCHWARTZ [continuing]. The patch has to exist but then people actually have to patch.

Mr. GREEN. We've just got to get everybody to download the patch.

Thank you. I yield.

Mr. GIMENEZ. Thank you to our Chairman.

Now I recognize the gentlewoman from New York, the former Chair, Ms. Clarke.

Ms. CLARKE. Thank you very much, Mr. Chairman.

I thank Ranking Member Swalwell for letting me waive onto today's subcommittee hearing.

Thank you to our panelists of witnesses for joining us today.

Before I begin my formal comments, I'd like to associate myself with the sentiments of Ranking Member Swalwell regarding Congressman Sylvester Turner. We are grateful for his service to the people of Houston, Texas. To his family and loved ones, we extend our deepest condolences. May he rest in peace.

When I introduced CIRCIA back in 2021 with Ranking Member Thompson and Chairman Garbarino, I did so because I recognized the important need for increased visibility into the cyber incidents affecting critical infrastructure and the importance of a central hub for cyber incident reporting in the Federal enterprise. I worked with many of the witnesses here today to get CIRCIA across the finish line, and I appreciate their on-going efforts to make sure that we get the final rule right.

I also appreciate Mr. Swalwell's work encouraging CISA to effectively engage with the private sector on the rule.

I agree with my colleagues and the witnesses before us that there are necessary improvements to the proposed rule, but the urgency of implementing CIRCIA remains. I hope the new administration will work quickly to modify the proposed rule and publish a final one without undue delay.

I have 2 questions for our witnesses. First of all, to all of our witnesses, without a defined—well-defined cyber incident reporting rule and harmonization process for CISA, we run the risk of agencies across Government issuing a hodgepodge of duplicative cyber incident reporting requirements. How will scrambling to comply with multiple incident reporting requirements affect security?

Then, second, many stakeholders have weighed in that the proposed CIRCIA rule defined "covered entities" and "covered incidents" too broadly, unnecessarily increasing the burden on the private sector and potentially overwhelming CISA with too many reports to analyze. Indeed, CIRCIA instructed CISA to identify subsets of entities and incidents, instruct—excuse me, subject to reporting requirements to avoid that outcome. Can you give me your thoughts on that?

We'll start with Mr. Aaronson and then work our way across.

Mr. AARONSON. So, on the first question, I would just echo some of the things that Ms. Hogsett said about the time that information security teams are spending on compliance. It's somewhere be-

tween 30 and 50 percent. As you expand the hodgepodge—to use your word—of reporting requirements, it only gets more complicated.

To your point about the broadness of CIRCIA as it currently exists and the uncertainty that surrounds it, taken at its most sort-of broad interpretation of what is a covered entity and what is a covered incident, we had one of our companies report that they thought they would have as many as 65,000 reports between 2022 and 2033. I think the number that CISA had said would be somewhere in the 200,000 to 220,000 total in that time frame, so it seems to be off by—if that's just one company taken at a really broad interpretation, it seems to be off by an order of magnitude. This goes to the importance of getting the definitions and the details right so that we can get some signal from the noise and so that CISA can ingest the information in a meaningful way.

Ms. CLARKE. Very well.

Ms. Hogsett.

Ms. HOGSETT. Sure. Just to add to that, and thank you for the question, the challenge of responding to multiple requirements does have a direct impact on security because it is diverting the time and attention away from what we all want the cyber professionals to be doing, which is defending their networks, kicking out bad actors when there is an incident and focusing on that. Instead, they have to divert time away to basically make sure they're complying with different legal obligations.

With respect to the definitions and covered entities within CIRCIA and the proposed rule, this committee was very thoughtful—and Scott just alluded to it—to make sure that the law would be crafted in a way that we get signal from the noise. You wanted the incidents that were going to be most impactful so that CISA could very quickly have the capability to take that information and turn it back around to share with other entities that could also be a risk.

The very broad scope with which the proposed rule was put together would put a lot of noise out there and make that all the more challenging. For instance, the definition would potentially capture operational outages that have nothing to do with the cyber incident, and I don't think that that was really what you and the committee had intended in crafting that law.

Ms. CLARKE. Very well.

Mr. Mayer, my time is up.

Mr. MAYER. Yes. Thank you, Congresswoman Clarke. I think that we have to deal with the fact that the reporting requirements right now are extraordinarily fragmented. The CIRC itself, Cyber Incident Reporting Council, at the time, in September 2023, identified 45 different reporting regimes, 22 agencies, I believe. I can only imagine that number has increased since then.

CISA has indicated that they expect 300,000 entities to be responding to these kind of requests. I can only imagine with—in the absence of clear definitions around the terms that you folks identified and staying close to the intent, in the absence of revising that and refining that and making it operationally practical for companies to respond, the system will get overwhelmed. The system in

Government will get overwhelmed, and the system in the operating environment will also get overwhelmed.

The critical point here is that during a major cyber incident when we are in a—essentially in a triage mode, we can't take people and divert them from their front-line responsibilities to detect the problem, remediate it, and respond and recover. So we believe that this particular rule needs to be reconstructed to align with your intentions, and if it doesn't, we're going to be doing more—as I indicated, it'll create more harm than good.

Ms. CLARKE. Very well.

Mr. SCHWARTZ. I agree with everyone on the panel in answer to the first question. On the second question, I'll just briefly say that on the definition of covered entities, CISA decided to kind-of try to narrow the scope by the size of the company—by going to the size of the companies, which I think does help in terms of removing some of the small, medium-sized businesses that we might not want to report, but it doesn't get to the risk issue, right. So you're going to have a lot of large companies, very large companies that have a lot of incidents, getting—echoing what we heard from others here, that are going to be reporting a lot that is not of the same value as if we did it based on some kind of risk feature.

Ms. CLARKE. Very well.

Thank you for your indulgence, Mr. Chairman. I yield back.

Mr. GARBARINO [presiding]. The gentlelady yields back.

I now recognize the gentleman from Louisiana, Mr. Higgins, for 5 minutes of questions.

Mr. HIGGINS. Thank you, Mr. Chairman. I appreciate this hearing today.

I concur with Chairman Green; it's been excellent testimony, and I appreciate it. I'm going to review it very carefully.

Mr. Chairman, in the 118th Congress, last Congress, I introduced a bill, H.R. 101023, the Streamlining Federal Cybersecurity Regulations Act, which essentially cut down on duplicated or misaligned regulatory requirements and authorities on the cybersecurity industry. I'll be reintroducing that bill shortly in the 119th Congress, and I look forward to my colleagues' support on both sides of the aisle with that bill.

Because, Mr. Aaronson, how many Federal agencies, how many Federal cyber regulations is a typical energy company required to report to in a given year, just roughly?

Mr. AARONSON. I mean, I'll just give you the agencies that we definitely have reporting requirements—

Mr. HIGGINS. That list will be too long to enumerate. But you're talking about, just tell America, 2, 4, 10, a dozen?

Mr. AARONSON. More than a dozen.

Mr. HIGGINS. More than a dozen. The gentleman said more than a dozen cyber regulators require a report from the energy industry.

Ms. Hogsett, how many Federal agencies does a bank need to file away to remain in good cybersecurity standing?

Ms. HOGSETT. We're similar and that's only at the Federal level. You also have States and international requirements to adhere to.

Mr. HIGGINS. So at the Federal level, which we control, would you concur, Mr. Aaronson, somewhere north of 10 or a dozen?

Ms. HOGSETT. Yes.

Mr. HIGGINS. Thank you.

Mr. Mayer, similar question: How many Federal agencies does the telecommunications industry have to report to?

Mr. MAYER. Yes, I would agree with the number of over a dozen, but—

Mr. HIGGINS. Easily over a dozen.

Mr. MAYER. Easily over a dozen.

Mr. HIGGINS. Mr. Schwartz, do you have a comment there?

Mr. SCHWARTZ. For IT, I would say that it's—

Mr. HIGGINS. It's a lot, right?

Mr. SCHWARTZ [continuing]. In the same range, but it's spread out because it's people reporting to the different sectors.

Mr. HIGGINS. OK. So now that we've clarified that for America, the objective here for the U.S. Congress is to reduce that mess, so that the cybersecurity industry can actually perform its primary mission, which is to protect the Nation and the industries of the Nation from cyber attack, which we've become increasingly susceptible to as technologies emerge. While our cybersecurity industry is busy checking boxes that the Federal Government and bureaucracies has imposed upon the industry, they have that much less time to spend on that actual mission of protecting the Nation, the citizenry, and the industries of America.

So how many of these agencies that require a report—we've agreed it is over a dozen—how many of them have streamlined themselves, like coordinated with each other and said, let's eliminate this and this and this and combine it into one? Has that ever happened, Mr. Aaronson?

Mr. AARONSON. The Department of Energy has been fairly thoughtful. Because it's our sector risk management agency and it's nonregulatory, that has actually helped them to—

Mr. HIGGINS. So within themselves, they've done some streamlining.

Mr. AARONSON. To help—

Mr. HIGGINS. Across the departments and agencies, have you seen a similar effort just organically?

Mr. AARONSON. No, certainly not.

Mr. HIGGINS. Thank you.

Mr. AARONSON. Your oversight has helped.

Mr. HIGGINS. Ms. Hogsett, has there been any organic effort from the bureaucracies to streamline and reduce themselves?

Ms. HOGSETT. Yes and no. The yes is, when it comes to incident notification, we have good coordination across 3 of our primary banking regulators. They aligned. There is a single standard, single definition, and you provide information to one—

Mr. HIGGINS. They look for common definitions?

Ms. HOGSETT. Yes.

Mr. HIGGINS. This is a good sign—

Ms. HOGSETT. It is. However—

Mr. HIGGINS [continuing]. Within the banking industry.

Ms. HOGSETT. It is.

Mr. HIGGINS. But there's a "however" here.

Ms. HOGSETT. There is. That is with respect to incident reporting specifically.

Mr. HIGGINS. Ah, for an incident report.

Ms. HOGSETT. Broader cybersecurity we have even overlap and duplication among those agencies.

Mr. HIGGINS. Roger that.

Mr. Mayer.

Mr. MAYER. Same story. I'm not aware of any major or significant—

Mr. HIGGINS. Thank you. It was good to hear about the banking industry, but that's per incident reports. That's different. That's not total regulatory authority being streamlined.

Mr. Schwartz.

Mr. SCHWARTZ. No. It's just been work to gather that.

Mr. HIGGINS. OK. So, Mr. Chairman, this is why Congress must act to bring clarity to the regulatory authority. I will hand you for your review, Mr. Chairman, the bill from last year. I intend to introduce it in the 119th Congress in a slightly refined iteration, and I would appreciate your support.

Mr. Aaronson, you had mentioned—we haven't had time for this question. You said that adversaries watch our response. Is it possible at all for the cybersecurity industry to strike back? If you said the adversaries are watching you, you must be able to identify the bad actor. Can you strike back at all against a bad actor?

Mr. AARONSON. The private sector—well, I don't want to speak for the whole private sector.

Mr. HIGGINS. Private sector.

Mr. AARONSON. Electric companies do not want to be in offensive cyber engagements. That is the purview of the Government.

Mr. HIGGINS. Well, we are going to probably give you that opportunity.

Mr. Chairman, my time has expired. I will have questions to submit in writing to each of these witnesses, and I appreciate this hearing, sir.

Mr. GARBARINO. The gentleman yields back. We probably will have a second round of questions if you do—if you have time, but we will take them in writing, as well.

Mr. HIGGINS. Thank you. They have to be in writing. I've got another committee.

Mr. GARBARINO. I thank the gentleman.

I now recognize the Ranking Member, the gentleman from California, Mr. Swalwell, for 5 minutes of questions.

Mr. SWALWELL. Mr. Schwartz, how should CISA revise its comment process to better engage stakeholders, and how would you recommend CISA structure additional feedback opportunities to maximize stakeholder input without unduly delaying issuing a final rule?

Mr. SCHWARTZ. Yes. CISA has the tools today to do this, and Congress gave them the tools to engage with the private sector in a way that they can get direct advice on issues and do it under—protected from FACA, protected from Freedom of Information Act, so that companies can feel free to share and that it only goes into the process of writing this rule. They should use that as—to define their ex parte process. It is the CIPAC authority that provides them to do that, and that's exactly what we recommend that they do.

Mr. SWALWELL. To each witness—and feel free to jump in—

Mr. MAYER. I'll start.

Mr. SWALWELL [continuing]. A decade ago—actually, sorry, a new question for each witness—Congress passed the Cybersecurity Information Sharing Act of 2015, which facilitates the voluntary sharing of cybersecurity information between the private sector and the Government. It expires, as I noted in my opening remarks, in September. What are the consequences of CISA expiring?

Ms. Hogsett.

Ms. HOGSETT. I'll start. So the CISA 2015 protections really forming the foundation for how we collaborate not just with Government but also across industry to ensure that we are sharing necessary information to protect everybody. So it's a key foundation for our collective defense. It provides information-sharing protections, liability protections, antitrust protections. We've now had the benefit of that for the last 10 years, and I think over that time, we've certainly seen an increase in collaboration.

I think our sector has always collaborated well within itself, but the expansion to across sectors and with other companies has been very valuable. We would hate to see that disappear and that we walk back some of the gains that we've made in that space. Also, as we noted earlier, CIRCIA itself with respect to incident reporting, refers back to the CISA 2015 protections.

Mr. SWALWELL. Right.

Ms. HOGSETT. So as we're getting ready to share more sensitive information, more detailed information to the Government, we do want to make sure that it is well-protected.

Mr. SWALWELL. Yes, Mr. Mayer.

Mr. MAYER. I'll go. Thank you. So at a minimum, we think it's absolutely essential that the CISA 2015 Act be reauthorized. As pointed out, I think we've learned things in the last 10 years, what has encouraged additional information sharing, what has constrained it, so there are opportunities to make enhancements improvements in the law.

The cost of not doing this is monumental. It will cause companies to be very careful about what they submit, reluctant to submit with the protections that Heather alluded to, and we'll be undermining our national security if we don't have something in place to either continue it in its current form, but ideally to reflect what we've learned over the past decade.

Mr. SWALWELL. Yes, Mr. Schwartz.

Mr. SCHWARTZ. Yes. We've seen information sharing organizations grow around this law, and that they are specifically created—the Cyber Threat Alliance, for example, is specifically built around this law, that the way that the financial sector ISAC shares out with other groups, not internally but with other organizations is built around the pieces of this law. If this law disappears, they will have to redo what they—how they are structured, so we—and we will lose critical time just doing that. Then, as well—

Mr. SWALWELL. I'm OK—I would just say this, I'm OK with like—I believe in like the principles of sunk costs, and, like, just because you've been doing it doesn't mean that's—

Mr. SCHWARTZ. Yes.

Mr. SWALWELL [continuing]. The best way to do it. But, like, is it beneficial is my—

Mr. SCHWARTZ. But it will—it will definitely slow and, in some cases, totally stop information sharing that has prevented threats—

Mr. SWALWELL. Got it.

Mr. SCHWARTZ [continuing]. From—and prevented incidents from happening.

Mr. SWALWELL. Great.

Mr. SCHWARTZ. Thank you.

Mr. AARONSON. So I want to slide in here. I agree with everything that my fellow panelists have said, so I would just associate myself with that. Those protections, the—I sort-of think of it north/south industry and Government sharing information. East/west across critical sectors has really grown up because of those protections in CISA.

I also want to respond a little bit to something that Mr. Higgins was saying. Incident reporting and information sharing are both incredibly valuable, but understanding what the difference between those 2 things is. Information sharing is about on-going threats where we don't have full certainty of what an adversary might be doing. Sharing tactics, techniques, and procedures across critical sectors so we can all collectively defend is incredibly valuable.

Incident reporting has value too. Once we know what that risk was, helping identify those patterns, helping to socialize those broadly, helping Government to set priorities, helping to set policy that is informed by what is actually happening in cyber space is incredibly valuable. So we like incident reporting. We like information sharing. It just needs to be done with protections and in an effective way that, again, Government can ingest all of this and not put undue burden on the people who are just trying to defend networks.

Mr. SWALWELL. I appreciate that.

Yield back.

Mr. GARBARINO. The gentleman yields back.

I now recognize the gentleman from Florida, Mr. Gimenez, for 5 minutes of questions.

Mr. GIMENEZ. Thank you very much, Mr. Chairman.

Today I had actually a meeting with the airline industry and we talked about this issue. We asked about, OK, when they have an incident how many different reporting requirements. They have at least 10 different agencies that they have to report the same incident to, which seems a little bit inefficient.

So—and I—you know, Mr.—you know, Representative Higgins asked the same question. You were saying it's 10, 12, et cetera.

Would it make sense to have 1 form sent to 1 place and then that 1 place disseminate that information?

Mr. MAYER. Can I start? It would absolutely make sense. It's critical—

Mr. GIMENEZ. We're not going to do it then. OK, thanks. You're asking us to do the impossible.

So, moving on, how many reportable incidents do you think there are? I guess you would know in your particular case, but across the United States how many reportable incidents do you think there are per day?

Mr. MAYER. Per day?

Mr. GIMENEZ. Per day, yes.

Ms. HOGSETT. What definition are you using, and what threshold?

Mr. GIMENEZ. I mean something that requires a report, something that requires an industry to write a report. How many of those incidents occur per day here in the United States? Does anybody have any idea?

Mr. MAYER. I would speculate—I'd take a guess here. I think over a thousand incidents would be reported daily.

Mr. GIMENEZ. Over a thousand?

Mr. MAYER. Over a thousand collectively across the entire—our sector.

Mr. GIMENEZ. Just your sector?

Mr. MAYER. Just my sector.

Mr. GIMENEZ. His sector. How about banking?

Ms. HOGSETT. I struggle to answer that because of the threshold. You have incidents or events that might occur constantly, but they don't necessarily rise—

Mr. GIMENEZ. No, I'm saying report—I'm saying reportable. You have to report.

Ms. HOGSETT. We have notification requirements that are private, so I wouldn't even know. A firm wouldn't be able to tell me because they're not allowed to.

Mr. GIMENEZ. Can you give me a guess?

Ms. HOGSETT. I would have to get back to you to have an informed response on that.

Mr. GIMENEZ. OK. How about an uninformed response? Just, you know, give me a swag, OK?

Ms. HOGSETT. Honestly, I hesitate.

Mr. GIMENEZ. OK. What about—OK. And energy?

Mr. AARONSON. So the same thing Ms. Hogsett said. There are wildly different reporting requirements. There are some that, you know, a pretty low bar. There are some that have an extremely high bar.

I can go back to the statistics that I know from one company that did a relatively deep dive on its reporting requirements, especially pursuant to CIRCIA's broadest definitions, and that was going to be 65,000 over 10 years.

So that's one company, 65,000 incidents over 10 years. Six thousand five hundred a year, that's 500 a month. Trying to do the math here.

Mr. GIMENEZ. Just one company?

Mr. AARONSON. That's just one company.

Mr. GIMENEZ. How many companies do you have?

Mr. AARONSON. EEI represents 62 investor-owned electric companies.

Mr. GIMENEZ. Sixty-two?

Mr. AARONSON. That's right.

Mr. GIMENEZ. So could I assume 62 times 500?

Mr. AARONSON. Sure.

Mr. GIMENEZ. Per day?

Mr. AARONSON. Sure.

Mr. GIMENEZ. Or is that a month?

Mr. AARONSON. Well—

Mr. GIMENEZ. Is that a month?

Mr. AARONSON. That's also—that's one of our larger companies, and that was 500 a month. So maybe it might be easy to get to several thousand a month.

Mr. GIMENEZ. Several thousand a month? OK. Does anybody know how this data is analyzed? No, nobody knows how it's analyzed. So we require you to send a bunch of stuff, but you guys don't know how it's analyzed by wherever it is we send it to. OK. I'll bet you it's not because of the overwhelming volume, all right?

So we need to look at that, Mr. Chairman, OK? If you require them to do something and then we don't use the data for anything, then it's actually worse, right, because you're making them do stuff that nobody looks at.

So we need to bring some other folks and say, how do you analyze all the data that you're getting that you require from everybody else to see that actually we're doing any good?

Mr. Aaronson, you talked about—we asked about offensive capability. You don't have an offensive capability. You don't want to use offensive. You don't want to use offensive capability.

Mr. AARONSON. So that's a pretty thorny topic. I'll go—

Mr. GIMENEZ. No, I just want to ask would you like to use offensive capability?

Mr. AARONSON. No, the private sector would not like—the electric companies would not like to get into—

Mr. GIMENEZ. You just want to get punched over and over again, just get punched once and punched again and punched again.

Mr. AARONSON. Well, this is where the Government comes in. So there are 2 ways you deter, right? Deterring, the attack does not have the intended consequence. That's on the private sector to protect its systems in a way that we can withstand a lot of punches.

The other way you deter is an attack has a consequence, and we would believe that that is fully the purview of our intelligence and national security apparatus.

Mr. GIMENEZ. But we don't have the resources to do that, I mean, all the time. So we would—what if we charged the—or allowed the private sector, with all their resources, et cetera, to allow to counter-punch. You wouldn't want that?

Mr. AARONSON. So it depends how you define counter-punch. I don't want to speak for the banks, but this notion of inking the money bag, that could be construed as—

Mr. GIMENEZ. My time is up, and hopefully we'll have another round because I really want to get into that one, OK?

Thank you, and I yield back.

Mr. GARBARINO. The gentleman yields back. We will have another round.

I now recognize myself for 5 minutes of questions.

Thank you all for being here today, back again, I guess.

In my submitted comment to former CISA Director Easterly on the CIRCIA notice of proposed rulemaking, I highlighted that Congress did not intend for CISA to subject numerous entities to its reporting requirements. Rather, Congress intended for CIRCIA to facilitate rapid information sharing, and I—that's not being achieved.

So we're all here talking about it and what should happen with future CIRCIA.

Ms. Hogsett, you said BPI sent a letter saying withdraw and re-issue the rule. Mr. Aaronson and Mr. Mayer both said ex parte could be a way to do it.

Mr. Schwartz, I'm sorry, I had to leave in the middle of your testimony so I don't know what position you took. What was—

Mr. SCHWARTZ. I'm with ex parte, yes.

Mr. GARBARINO. Ex parte. So do you believe—I mean, Ms. Hogsett, do you believe an ex parte could work? I understand we have a timing issue, which is the problem under the law. There's a timing issue, and I'm not sure we could meet the timing that the law requires if we fully withdraw and reissue.

Can ex parte fix the issues?

Ms. HOGSETT. We would very much support an ex parte process. We asked for further engagement and never got it, frankly, through the process thus far.

We believe that that rule, as proposed, should not be implemented, and we would rather take additional time. We are prepared to work with CISA and would like an iterative dialog to make sure that we get this right. It's too important.

We stand ready. We want to see this be successful. So we—I think the stakeholder engagement, given the complexities of the issue here, we do need that. We just—that rule, as proposed, please do not implement that.

Mr. MAYER. Mr. Chairman, I think that this committee can be very helpful in urging CISA to grant our request for ex parte, starting tomorrow. If we can work with the agency and provide our expertise and the information about how we operationalize incident reporting, that can be integrated into their rules in the fall. But if we don't have that possibility to engage with them, which they clearly rejected—time and time again we've made the request—I think this is going to go down a path that's going to be very problematic for CISA and extraordinarily burdensome and costly for our sector.

Mr. GARBARINO. As you said in your testimony, this will be more harm than good here.

Mr. MAYER. Yes.

Mr. GARBARINO. I agree with all of you that this rule should not be implemented as currently presented, and if it was I would lead the effort to CRA it.

But it's good to hear that you all think an ex parte could work, because I want this to work. I know the Ranking Member and the former Chair, Clarke, all want—they want this rule to work.

This is a big focus of mine, a big focus of now Chairman Green's—I'm happy he was here today—harmonization, making sure incident and information sharing happens and happens in the correct way.

So I want this rule to work, and I will be—following this hearing I'll work with committee staff on both sides to make sure that we reach out to CISA. I know they just nominated a new potential director this morning. I'm excited—no, not you. But Mr. Plankey I think could do a very good job. I've met with him. Director Easterly

had very nice things to say about him. So I think—I think they may be willing to relook at this and move into an ex parte.

One of you mentioned something, and I want to go with this because we talk about harmonization and how agencies don't listen to you all. One of you brought up the SEC rule. Maybe all of you brought up the SEC rule, which I've been fighting. We passed the CRA out of committee, but because the Senate moved so slow our time clock ran out over there. I know the Ranking Member was also against it.

But one of you brought up the national security concerns, ONCD I think has national security concerns with that rule in your testimony. Can you speak to those, please? It might have been all of you that talked about it.

Mr. MAYER. It may have been me who brought that up.

So it's a perfect example of rules that don't add to security and, in fact, create vulnerabilities, as I mentioned. Bad guys, cyber criminals, enterprises can manipulate the process of disclosure in ways that certainly were not intended and will not be helpful.

So, from a national security perspective, that particular rule, I am not sure it does anything to enhance our national security.

Mr. GARBARINO. Ms. Hogsett.

Ms. HOGSETT. I would actually say it probably harms our national security. I think this is the challenge that we've kind-of talked about now here is you have independent agencies that are doing something within their narrow lane. So for the SEC, they think that investors need to know this information.

I think we would argue that investors aren't really utilizing this information. It's not helpful to them. It's actually putting them at greater risk. But because an agency continues to look without somebody at the top sitting across and exercising oversight to say, does this really make sense, is it in the best interests of the Nation, we wind up with a lot of these duplicative, overlapping, deeply harmful rules.

So, to the extent that Congress and this committee is ready to engage and help lead this effort, we do need an overall view to look at what is helpful versus what is harmful, and the SEC rule is classic of what is harmful.

Mr. GARBARINO. I appreciate that. When I had Chairman Gensler in front of Financial Services, I asked him which was more important, investor knowledge or—if investor information was more important than national security. He said no.

So I think now it's time for the new SEC to look at this rule and correct it, because I've been told by people at CISA and industry that they've had to stop sharing information before, timely information, in order to comply with the SEC rule. That is not good for anybody.

I believe everybody who's been here for first round is done, so we're going to start a second round of questions.

I recognize the Ranking Member from California, Swalwell, for his second round.

Mr. SWALWELL. I appreciate that, Chairman.

Last week, the Secretary of Homeland Security disbanded more advisory committees at the Department, including CIPAC, the Critical Infrastructure Partnership Advisory Committee. For over 15

years, CIPAC has played a significant role in the implementation of the National Infrastructure Protection Plan and has facilitated coordination of critical infrastructure protection and resilience activities across all levels of Government and in partnership with the private sector.

How will a termination of CIPAC affect the coordination of critical infrastructure protection activities? I'll just go across the witness table.

Mr. Aaronson.

Mr. AARONSON. Thank you, Ranking Member Swalwell.

So the answer is it will depend on what it ultimately is replaced with. I understand every new administration gets the privilege of populating advisory committees. CIPAC is not an advisory committee. It is an authority that the Secretary of Homeland Security has to facilitate public-private partnership.

To all the discussion we had about offensive versus defensive capabilities and resilience and the fact that industry and Government, again, 90 percent—as I mentioned in my opening comments, 90 percent, give or take, of critical infrastructure is owned by the private sector, this is a team sport.

CIPAC is the rule book for how that—how those teams, industry and Government, can work collaboratively with protections, with the ability to have on-going dialogs, with sector coordinating councils that facilitate information sharing to prepare for and respond to all of these hazards.

I will say the Electricity Subsector Coordinating Council has been a CEO-led body since after Superstorm Sandy in 2012. This isn't just about cyber. This is about storms and physical threats and all the things that can impact critical infrastructure, which impact our ability to provide services to customers and communities across the United States and be prepared for all of these risks. CIPAC or something like it is vital to our ability to use that partnership effectively.

Mr. SWALWELL. Does anyone have an answer different than that that they want to add?

Mr. SCHWARTZ. I'll just add that CIPAC is different. I strongly agree with Chairman Green's comments. There are too many advisory committees, and DHS has too many advisory committees. Getting rid of some of them made sense. As Mr. Aaronson said, this is not an advisory committee, right? It has the word "Advisory Council," but it's not an advisory committee.

The sectors organized themselves, right, and have their own bodies that then meet with the Government. That comes with the protections that that can happen in a way that provides for open discussions. We get more information from the Government because it exists. It is a good two-way conversation. It's been successful.

All the nice things you've said about JCDC earlier, I agree with those. This is the policy equivalent of that, and it goes back even further and it's in some ways—we can talk about more success stories from it. That's all.

Mr. SWALWELL. Mr. Aaronson, I want to go back to something that Mr. Gimenez brought up, because I've thought about this for many years. I have a Congressional district that has a lot of tech and biotech companies, large and small, headquartered there, and

they get hit all the time. I have Cowbell Cyber headquartered there. They do cyber insurance.

It's long frustrated me knowing the limited resources that we have at Cyber Command and at the Bureau and at the NSA and CIA. I get the hesitancy for a business, even a large energy company, to go on offense. I'm imagining the concern is that if you do that, you're still going up against a large nation-state that could take you out. But—and then you're looking at forced retirements at some of these agencies that are happening right now, and so the resources are going to get even thinner.

Is there an environment where we could credential third-party cybersecurity contractors who could be offensive, and that could be utilized by small- and medium-size businesses, again, credentialed by the Government, bonded and insured, but also with liability protections that they would probably need to operate.

It just seems, as Mr. Gimenez said, you're just getting punched in the face right now, and the best you can do is put up your hands and like protect yourself, but you're not really able to punch back. I don't know what the deterrent is on the other side if the U.S. Government isn't able to punch back against all those entities.

If the Chairman would indulge me for his answer.

Mr. GARBARINO. Absolutely.

Mr. AARONSON. It's something I'd want to take back to the sector. I think there's 2 concerns. You highlighted 1 of them, which is if you are punching back, now you are in effectively a fight with a potentially very well-resourced nation-state. As we've talked about, we're—many electric companies are resource-constrained even on defense. EEI's member companies, investor-owned electric companies, have a little bit better resource, but there's cooperatives and municipals across the sector as well. It could be—that's daunting. So that's one set of concerns.

The other is not quite in response to what you said, but an escalating cyber war perpetrated by the private sector might have some unintended consequences. So it goes back to this being the team sport and the value of CIPAC and the value of CISA 2015 and the value of industry-Government partnership.

Industry can be both defensive and resilient. So that the attack may happen, but we'll still be operational. We would really rely, much like we would in any land war, on our Government for it to be responsible for national security.

Mr. SWALWELL. I understand that concern. I guess the way I look at it, though, is it's not as if the resources that we have in the Federal Government are decreasing cyber attacks. It's actually going in the opposite direction. More and more people are getting hit.

I'll yield back. I imagine Mr. Gimenez may go back.

Mr. GARBARINO. The gentleman yields back.

I now recognize Mr. Gimenez from Florida for a second round.

Mr. GIMENEZ. Thank you. Thank you for the tag team. Here we go. OK.

Look, the only way that you're going to stop this is if the offensive party fears more the retaliation than what we do is just put up our hands and, gee, I hope you don't hurt me too bad.

If you do that, just like nations, nations go to war. When they find somebody weaker, they're going to go to war and take it over.

They find you just sitting there, OK, please don't hit me, they're going to hit you because there's no repercussion for it. There's no consequences for their action.

So everything we've done, have cyber attacks been reduced? Are they going down or are they going up?

Mr. MAYER. They're going up.

Mr. GIMENEZ. They're going up. So whatever we're doing isn't working. Why? Because there's no consequences to their action.

So eventually, we're going to have to go on offensive, and it's going to have to hurt them as much as it hurts you or actually maybe hurt them worse than what they hurt you.

Yeah, you know, we in the Federal Government, we are not sourcing or putting up the necessary folks that it needs in order to protect you, because it's such a big domain. I think that the private sector, with its resources, both in terms of people and money, is going to have to be the way to go.

How much is cyber attack, how much is that costing you? How much is it costing you all to protect against it or the damages caused by cyber attacks?

Mr. MAYER. We're in the hundreds of millions of dollars of investment in cybersecurity technology and defensive capabilities.

I will say that on the issue of what comes under the umbrella of active defense, there's a range of options. The most extreme one is letting private sector engage in hack backs.

I think the issue is Government is doing something. They empowered U.S. Cyber Command to engage in offensive capabilities. We would support them in any effort where we have certain assurances and there are guardrails.

What we don't want to do is deputize a front-line practitioner to respond in haste to an attack where we may not have the right attribution or there could be substantial repercussions.

So this is an area that requires real close collaboration with Congress, with the intelligence community, with U.S. Cyber Command. I mean, we have to do that. I know—

Mr. GIMENEZ. The only way that you're ever going to be assured, OK, that you're not—it's not going to have dire consequences is that you have to have a mutually assured destruction, OK?

Mr. MAYER. The Government can do that.

Mr. GIMENEZ. Well, I'm not sure they can, OK? So, you know, that's what worked. That was—you know, the MAD theory actually kind-of worked, because if you know that I can take you—if you do something to me I can destroy you too, you probably aren't going to pull that trigger, all right?

If the other side feels that they can continually just hammer you and keep you in business, because they want you in business because they want to have the revenue and all that, but eventually when a nation-state says, OK, we're going to do the knockout blow and we don't have a knockout blow in response, they're going to knock you out, all right?

So I don't know the best way. Maybe it is that we do something where we have this Cyber Force. You know, we have the Space Force now, now we have the Cyber Force that has offensive capabilities somehow funded through industry, or we have a third-party, you know, entity funded by industry that is deputized or

given a warrant whenever there is—a retaliatory strike is authorized. Because, frankly, I just see this spiraling completely out of control.

So anybody have any comments on that?

Ms. HOGSETT. I'll comment. I think what you're getting at is the need to use all the tools we have in the toolbox, whether that's offensive, defensive, diplomacy.

Mr. GIMENEZ. Yes.

Ms. HOGSETT. One of the things Robert actually noted is the need for greater operational collaboration between industry and Government. Our firms will see things on their networks, but they don't necessarily have attribution that it is a specific national security threat actor. They would welcome a greater ability to work and share that with the appropriate authorities in Government to get feedback on that.

Oftentimes, we think that there are things we see, there are things that Government sees that if we both knew what was happening we could better direct some of our activities. I think that would be to us the next step to really try to drive at combating this where it's happening.

Mr. GIMENEZ. Mr. Chairman, my last comment—and I'm a little bit over time—is that this is—it's going to be an everybody, you know, on board effort, the Government and the private sector.

Just like we fought the last world war, right? Everybody got on board and we're fighting, we're going in the same direction. I think that this is where it's heading, anyway.

I yield back.

Mr. GARBARINO. The gentleman yields back.

I now recognize the gentlelady from New Jersey, Mrs. McIver, for 5 minutes of questions.

Mrs. MCIVER. Thank you, Mr. Chairman. Thank you, Ranking Member, and to the witnesses for joining us today on a nice day. Thank you for being here.

A strong and timely cyber incident reporting framework is critical to our national security, which I'm sure you've heard multiple times and has been mentioned multiple times in today's committee hearing.

CISA must move quickly to establish a process that engages the private sector, aligns with the distinct regulations and meets Congressional intent, all without delay. But we cannot achieve this without a robust Federal work force.

With staff and resources being cut each and every minute, it's crucial we support the personnel needed to get this done. In order to properly implement CIRCIA—make sure, because CIRCIA and CISA kind-of gets me tied up—we'll need to have the staff and resources to process and analyze incident reports.

I am concerned that any cuts to CISA's funding or staffing could leave it without the capacity to properly implement this crucial new program. To each witness, how important is it that CISA be adequately staffed and resourced to implement CIRCIA? What kind of funding and staffing is most important to properly implement?

Mr. SCHWARTZ. I would say it's taken a long time to get up to this point where we have adequate staffing at CISA, and we are

concerned about cuts to CISA and what the impact will be, especially as they get more information like this.

There is an effort to tie all the information together that they're getting from inside the Government, from contractors, and this information together.

Being able to analyze that is going to be a big. It's going to take a lot—it's going to use a lot of AI, but it's also going to use a lot of human resources as well.

Mrs. McIVER. Thank you.

Mr. MAYER. I would say it's not in my purview in terms of telling the Federal Government how to organize themselves right now. But we will continue to engage them. I think, for example, the partnership, if the rules are written in a way that is consistent with the intent of Congress, we could significantly reduce the amount of noise that would be generated in this information-sharing process. I think there would be opportunities for efficiency associated with getting back to that original intent.

The other thing I'm just going to use this as an opportunity to share with you, that we talk about incident reporting, but it's connected to incident response and it's connected to how we engage in this process.

One of the things I think we need help from you and potentially with ONCD is to have a single point of contact during a major crisis. Because right now the experience has been we're getting inundated with multiple agency requests during the crisis. We're even getting multiple requests within the Department, and then we're getting multiple requests to different pieces, parts of our operators or service providers.

That has to stop. We have to really rationalize that and ask ourselves some serious questions here about how to organize this effort, how to engage in the appropriate information sharing.

The last thing I'll say is, when it comes to CIRCIA, there was an assumption that there would be reciprocity, and we still have that assumption. So the benefit of submitting information is so the Government in real time or as quickly as possible comes back to us with mitigation guidance, new information on how to protect our networks.

There's a lot of work to do here. I'm hearing that there's a lot of alignment in this subcommittee around how to reduce the inefficiencies associated with all of this.

So we look forward to working with you, and hopefully we'll be working with CISA shortly on how to remedy some of the infirmities in the CIRCIA rule making.

Mrs. McIVER. Thank you so much for that, Mr. Mayer.

I would assume that getting 1 point of contact would not be that difficult. Thank you.

Mr. MAYER. You would think.

Ms. HOGSETT. We certainly want CISA and CIRCIA to be successful, and we are committed to that.

For CIRCIA to work, CISA will need certain capabilities. That's not only technological, but also there is a human element to that. So we look forward to engaging with the new leadership once it is—once they are appointed and confirmed.

Mrs. McIVER. Thank you for that.

Mr. AARONSON. The only thing I'd add, so people, processes, technology are going to be critical to the success of CIRCIA being implemented effectively. Let's not forget about the security of this really critical information.

As incident reports are shared, that can be a road map to a potential threat actor. So we need to make sure that we're not just collecting this information but protecting it as well.

Mrs. MCIVER. Thank you so much to each of you for those responses.

With that, I yield back, Mr. Chairman.

Mr. GARBARINO. The gentlelady yields back.

I now recognize myself for a second round of questions.

Chairman Gimenez brought up before attacks are going up and you agreed, but are successful attacks going up or is the work that you all are doing on the Sector Coordinating Councils and preparation and work with CISA—I know attacks are going up, but are we seeing positive results from all the information sharing and the work that you're doing amongst each other?

Mr. SCHWARTZ. There are a lot of reports out there and they say different things. So some reports I've seen tend to suggest that we are being—that we are more successful and that the bad guys, there's just a lot more attacks so, therefore, the number of incidents goes up with it.

Some have shown that in certain areas there are more successful attacks than there used to be, and so then we have to move more resources over to those.

Mr. MAYER. What you propose and what you're discussing is there's a counterfactual element here in that we don't know what would happen in the absence of doing some of these activities.

But I would say there's a lot of redundancy. There are a lot of reports that are produced within the Government that, in our view, don't lend themselves to security improvements. So we have to get better at thinking about how we use Government resources, how we use industry resources, focusing on what is the expected outcome that we're looking for. That will fix, I think, a lot of the noise in the system.

Ms. HOGSETT. I think there are mixed signals. I think it's hard not to overlook the fact that we are increasingly being attacked by nation-states.

You have private industry that has very strong, very powerful nation-state actors infiltrating their systems. Even the best, most sophisticated private firm is going to struggle to deal with that.

So I will say I think our capabilities have certainly improved. Our information sharing has improved. We can respond faster when things occur.

We within the banking sector continue to see certain challenges and weak spots with third parties or vendors that we rely on, things that cut across multiple sectors and can be embedded in your infrastructure. Those areas can still be very challenging to deal with.

Mr. AARONSON. I think Ms. Hogsett put it really well there, so I'll just associate with that.

I'll give another example, though, of some really effective coordination that's happening where a nation-state may be responsible

for an attack, private sector sees it, develops mitigation strategies, socializes those, and then works with Government to kind-of load the gun back for potential offensive operations should it become necessary.

We've heard about all the different typhoons that are out there. Volt Typhoon was something that was impactful to—could have been impactful to the electric power sector; but because of industry being on the defensive and working with and across the Energy Threat Analysis Center and a lot of our partners in Government, we were able to identify that, develop a remediation strategy and socialize those for the benefit of all electric power sector participants.

Mr. GARBARINO. Thank you very much. I just want to say for the record I am supportive of Extending the Cyber Information Sharing Act of 2015, however we get that done, whether we include CISA actually in the legislation of the text, who is the priority lead. I just want to make sure we get it in front of the right committee in the Senate so it doesn't get bogged up like CIPAC did.

I also want to say that you all brought—you listed some grave concerns today with CIPAC being disbanded. I mean, I've met with—Mr. Mayer, we've met and you've testified twice. You are the head of the Sector Coordinating Council. I have met with Ron Green, who's Financial Services, and Pedro Pizarro. They've already reached out. Edison International has already reached out to have a meeting.

So I'm going to look into this and hopefully speak to the administration and try to fix this, because this is something we don't want industry not sharing information with us. We don't want industry not sharing information with each other, because when that happens it just increases the vulnerabilities that are out there.

This is where I want to get to. There is a lot of—Mr. Mayer, you said it. There is a lot of duplicative paperwork and rules out there. You know, the idea behind CIRCIA was to get some harmonization on incident reporting, but that's not all we deal with.

CIRCIA doesn't really have the teeth, though, to force other agencies to do it. Who does? I mean, who do we have run the harmonization effort? I think you said ONCD before, but who's got the actual juice to make these agencies fall in line?

Mr. MAYER. That's a great question.

Mr. GARBARINO. You can all go.

Mr. MAYER. Quickly. So this is the problem. We have multiple agencies committed to a mission. Cybersecurity has become an interesting area for their involvement. A lot of it is duplicative.

We think that the was Office of the National Cyber Director, consistent with its statutory responsibility to coordinate some of these responsibilities, can play a significant role going forward in rationalizing this effort.

In the absence of that, we're going to be still dealing with all of these silos, multiple reporting requirements, and they're just going to be duplicative and not effective.

Ms. HOGSETT. At this point, I think we need White House-level leadership, because that's really the top-down to really effect change here. We are seeing some signs that it looks like the Office of Management and Budget may get more involved in this.

So I think between OMB, Office of the National Cyber Director, which did do quite a bit of work on this to sort-of socialize the problem, the Cyber Incident Reporting Council that you all authorized in CIRCIA has put a lot of information out there. We just need someone sitting at the top to say, you guys need to rethink this.

Mr. AARONSON. Congressional oversight is incredibly valuable. I don't know what the number is these days, but at one point it was like 37 different committees and subcommittees had responsibility for cyber in some way.

I think that work that you guys are doing to coordinate the cyber subcommittees across Congress and then work with the agencies of jurisdiction to also harmonize, there's value there too.

Mr. SCHWARTZ. I agree on the OMB and ONCD approach. I think that's the way to go.

Mr. GARBARINO. Chairman Green is doing a great job, working with the—getting the committees of jurisdiction together. But, yes, I agree with you all. We need someone to be able to tell these guys to fall in line. We didn't really see that. We haven't seen that since I've been here.

We need to keep up our oversight, but I promise we're going to work on ex parte for the CIRCIA rule, hopefully get that fixed. We will continue working on harmonization. I know the committee is working on a report that we can hopefully get to the administration, and they can start acting on making your lives more focused on cybersecurity and not finishing a report.

So, with that, I want to thank the witnesses for their valuable testimony and the Members for their questions.

The Members of the committee may have some additional questions for the witnesses, and we would ask the witnesses to respond to these in writing. Pursuant to committee rule VII(E), the hearing record will remain open for 10 days.

Without objection, the committee stands adjourned.

[Whereupon, at 11:43 a.m., the subcommittee was adjourned.]

APPENDIX I

STATEMENT OF CTIA—THE WIRELESS ASSOCIATION

MARCH 11, 2025

CTIA—The Wireless Association® (“CTIA”)¹ is pleased to submit this statement for the record in the hearing of the Subcommittee on Cybersecurity and Infrastructure Protection, Regulatory Harm or Harmonization? Examining the Opportunity to Improve the Cyber Regulatory Regime.² This hearing is timely and of critical importance, given that there is much work to be done before the Cybersecurity and Infrastructure Security Agency’s (“CISA” or “agency”) can address stakeholder concerns and finalize its proposed Cyber Incident Reporting for Critical Infrastructure Act (“CIRCIA”)³ regulations.

CTIA welcomes this opportunity to provide input to the committee to add the perspective of the wireless industry on CIRCIA specifically and cybersecurity policy more generally. CTIA and its members are invested partners with the Federal Government, developing operational and policy solutions on cybersecurity for decades. And CTIA members contend with duplicative, inconsistent, or contradictory incident reporting and other cybersecurity requirements and regulatory frameworks from multiple Federal agencies and an array of State entities. Based on this experience and expertise, CTIA urges Congress to consider how CISA can better fulfill its mission to help critical infrastructure owners and operators prepare for and respond to significant cyber incidents in an environment marked by serious nation-state adversary activity. In particular, we encourage Congress to:

- Help facilitate a forward-looking, stronger, and more coordinated approach for the U.S. Government to respond to serious cybersecurity incidents that have national security implications, including promoting meaningful and actionable information sharing on these sophisticated and sustained cyber intrusions and attacks between industry and Government, without undue regulatory requirements or liability exposure for industry.
- With respect to the on-going CIRCIA rule making, carefully evaluate and oversee the agency’s decisions to: (1) Ensure a more focused and harmonized cyber incident reporting framework that allows companies that are victims of cyber incidents in this growing threat landscape to focus on critical remediation and response activities, rather than navigating overbroad reporting requirements; and (2) enable stakeholder engagement and collaboration through an ex parte process to reorient the direction contemplated in CISA’s Notice of Proposed Rulemaking (“NPRM”).⁴

¹ CTIA—The Wireless Association® (www.ctia.org) represents the U.S. wireless communications industry and the companies throughout the mobile ecosystem that enable Americans to lead a 21st-Century connected life. The association’s members include wireless providers, device manufacturers, suppliers as well as apps and content companies. CTIA vigorously advocates at all levels of government for policies that foster continued wireless innovation and investment. CTIA represents a broad diversity of stakeholders, and the specific positions outlined in these comments may not reflect the views of all individual members. The association also coordinates the industry’s voluntary best practices, hosts educational events that promote the wireless industry, and co-produces the industry’s leading wireless tradeshow. CTIA was founded in 1984 and is based in Washington, DC.

² Regulatory Harm or Harmonization? Examining the Opportunity to Improve the Cyber Regulatory Regime: Hearing Before the H. Homeland Sec. Subcomm. on Cybersecurity and Infras. Prot., 118th Cong. 1 (2025) (“Regulatory Harm or Harmonization”).

³ Consolidated Appropriations Act, 2022, Pub. L. No. 117–103, div. Y, Cyber Incident Reporting for Critical Infrastructure Act, 136 Stat. 49, 1038–59 (2022), <https://www.congress.gov/117/plaws/publ103/PLAW-117publ103.pdf> (codified at 6 U.S.C. § 681b et. seq.).

⁴ CISA, Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements, Notice of Proposed Rulemaking, 89 Fed. Reg. 23644 (Apr. 4, 2024) (“CISA NPRM”).

THE WIRELESS INDUSTRY HAS BEEN A LEADER ON CYBERSECURITY ENHANCEMENT AND COLLABORATION

CTIA has been engaged on cybersecurity policy for decades, bringing together industry stakeholders to address issues in multiple fora. CTIA's Cybersecurity Working Group ("CSWG") convenes all parts of wireless—service providers, manufacturers, and wireless data, internet, and applications companies—to facilitate innovation, research, and cooperation in response to threats.⁵

Through the CSWG, CTIA and its members have been leaders in partnering with the Government. For example, the Department of Homeland Security ("DHS") has long been the sector risk management agency ("SRMA") for the Communications Sector,⁶ and CTIA members have worked with CISA and its predecessor agencies for years, including on developing cross-sector cybersecurity performance goals ("CPGs")⁷ and identifying critical functions and assets for the Communications Sector.⁸ CTIA and its members collaborate with a wide array of other Federal partners, including the Federal Communications Commission ("FCC") and its Communications Security, Reliability, and Interoperability Council ("CSRIC"), the National Institute for Standards and Technology ("NIST"), and the White House.

CTIA is also a leader in operationalizing security standards for the benefit of consumers, manufacturers, and operators. As key examples:

- CTIA manages a 5G Security Test Bed, which brings together "wireless providers, equipment manufacturers, cybersecurity experts, and academia to demonstrate and validate how 5G security will work, using real 5G networks."⁹
- CTIA's Internet of Things ("IoT") Cybersecurity Certification Program establishes a baseline for IoT device security on wireless networks and uses widely adopted standards from NIST, among others.¹⁰

CTIA has been engaged in every major Federal cybersecurity rulemaking and policy issue for the last 15 years, including but not limited to proceedings at the FCC, the Securities and Exchange Commission ("SEC"), the Federal Trade Commission ("FTC"), and the Department of Defense ("DoD"). CTIA members know first-hand how the agencies are approaching complex questions of cybersecurity and data governance in regulation and other activity.

Likewise, for more than a decade, CTIA has been engaged in legislative discussions about cybersecurity impacting wireless, urging Congress for years to preserve and enhance the vital partnerships that make effective cyber readiness and response possible. For example, CTIA supported the landmark Cybersecurity Information Sharing Act of 2015 ("CISA 2015"), which provides an essential foundation for voluntary collaboration on cybersecurity and includes important liability and confidentiality protections for private companies who volunteer information to DHS.¹¹

As Congress considered cyber incident reporting requirements in what became CIRCIA, CTIA, like others in the private sector, urged Congress to take a targeted and risk-based approach to reporting that focused on the most impactful incidents affecting the most critical companies.¹² CTIA and other stakeholders have called on CISA to do the same.

CONGRESS HAS AN IMPORTANT ROLE TO PLAY TO ENSURE A STRONGER AND MORE COORDINATED APPROACH FOR RESPONDING TO NATIONAL SECURITY INCIDENTS

As sophisticated cybersecurity threats—including but not limited to threats from nation-state adversaries—continue to pose serious cybersecurity and national secu-

⁵ See CTIA, *About CTIA: Cybersecurity Working Group*, <https://www.ctia.org/cybersecurity-working-group> (last visited Mar. 11, 2025).

⁶ See CISA, *Sector Risk Management Agencies*, <https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/sector-risk-management-agencies> (last visited Mar. 11, 2025).

⁷ Comments of CTIA, *Cross-Sector Cybersecurity Performance Goals and Objectives*, Final CPGs, GitHub Submission (filed Feb. 15, 2023), <https://github.com/cisagov/cybersecurity-performance-goals/discussions/40>.

⁸ CISA, *Executive Order 13873 Response: Methodology for Assessing the Most Critical Information and Communications Technologies and Services* (Apr. 2020), https://www.cisa.gov/sites/default/files/publications/eo-response-methodology-for-assessing-ict_v2_508.pdf ("CISA EO 13873 Response").

⁹ 5G Security Test Bed, LLC, *5G Security Test Bed*, <https://5gsecuritytestbed.com/> (last visited Mar. 11, 2025).

¹⁰ CTIA Certification, *IoT Cybersecurity Certification*, <https://ctiacertification.org/program/iot-cybersecurity-certification/> (last visited Mar. 11, 2025).

¹¹ 6 U.S.C. § 681b. CISA 2015 sunsets in October 2025. CTIA supports reauthorization of the CISA 2015 with an expansion of the range of information and activities protected and additional liability protections.

¹² CISA EO 13873 Response, *supra* note 8.

urity risks to the Communications Sector and others throughout critical infrastructure, it is critical that the Federal Government iterate its deterrence and response approaches and establish processes that meet the evolving threats our Nation is facing now and will continue to face in the future. Key principles that should guide this forward-looking approach include:

- *Coordination among Federal agencies and between Federal agencies and industry must be improved.*—CTIA agrees with USTelecom’s testimony calling for a single “Responsible Agency” that in the wake of a national security event will be responsible for coordinating with the private sector and overseeing Government information sharing with respect to that event.¹³ While the current structure for invoking the Unified Coordination Group (“UCG”) is intended to achieve this goal, there continue to be significant challenges with interagency coordination in the wake of major incidents. Congress should work with the administration to (1) establish a single Responsible Agency when an incident rises to the level of forming a UCG; (2) prohibit duplicative and contradictory requests or investigations from other Government agencies; and (3) establish stronger protections for information that is shared with the Responsible Agency and tighter parameters for how information is shared between the Responsible Agency and other agencies, to ensure that such information is not leaked and is not subject to disclosure under the Freedom of Information Act (FOIA) or State laws.
- *Victim companies should not face undue regulatory requirements or liability exposure.*—Further, Congress should ensure that victim companies do not face undue, burdensome requirements, which only serve to divert resources away from responding to and mitigating the impacts from the incident. To this end, and as USTelecom testified,¹⁴ Congress should ensure that the Responsible Agency has the authority to suspend all Federal and State reporting requirements, upon finding that doing so in the wake of a national security incident serves the national interest. This will reduce the risk that highly sensitive information is disseminated haphazardly across various Federal and State agencies, and will address the fundamental flaws with the current fragmented reporting ecosystem—described in more detail below—at a time when harmonization is critically necessary, in the wake of a serious national security incident. Further, Congress should ensure that victim companies are not subject to liability for such national security incidents. To this end, Congress should consider establishing a safe harbor for companies that have reasonable cybersecurity risk management programs that are consistent with NIST’s Cybersecurity Framework 2.0, and it should ensure that information that companies share with the Responsible Agency cannot be used against such companies in regulatory enforcement or civil litigation.
- The Federal Government should establish a National Deterrence Strategy. There is a need to increase the cost on the People’s Republic of China and other foreign adversaries so they cannot operate with impunity. To this end, the White House, in consultation with relevant agencies, should develop a National Deterrence Strategy with the goal of leveraging an all-of-Government approach to increase the costs for these bad actors, including but not limited to diplomatic, financial, and other means.
- The Federal Government should harmonize the development and imposition of baseline cybersecurity requirements. Across the Federal Government, agencies have sought to address cybersecurity by imposing a patchwork of extensive, often conflicting or duplicative, baseline cybersecurity requirements. These are in addition to the extensive patchwork of incident-reporting requirements at the Federal and State levels. At the FCC alone, CTIA addressed 4 different regulatory proceedings over the last 2 years that proposed 4 different approaches to cybersecurity baseline requirements.¹⁵ Last session, Senators Peters and

¹³Regulatory Harm or Harmonization, *supra* note 2 (Statement of Robert Mayer, Senior Vice President, Cybersecurity and Innovation, USTelecom, The Broadband Association) (“Mayer Testimony”).

¹⁴Mayer Testimony (Mar. 11, 2025).

¹⁵See, e.g., Comments of CTIA, *Protecting the Nation’s Communications Systems from Cybersecurity Threats*, PS Docket No. 22–329, (filed Jan. 24, 2023), <https://www.fcc.gov/ecfs/search/search-filings/filing/1012468668036>; Comments of CTIA, *Review of International Section 214 Authorizations to Assess Evolving National Security, Law Enforcement, Foreign Policy, and Trade Policy Risks*, Order and NPRM, IB Docket No. 23–119 (filed Aug. 31 2023), <https://www.fcc.gov/ecfs/document/108311863500689/1>; Comments of CTIA, *Connect America Fund: A National Broadband Plan for Our Future High-Cost Universal Service Support*, WC Docket No. 10–90 et. al., (filed Dec. 12, 2023) <https://www.fcc.gov/ecfs/document/1212267425956/1>; Com-

Lankford and Representative Higgins proposed legislation in an effort to address this whole-of-Government challenge through the creation of a harmonization committee to study and implement a pilot program.¹⁶ In the wake of increasing threats, it is imperative that Congress consider approaches that will speedily and effectively ameliorate this regulatory blind spot, compelling executive and independent agencies to harmonize their cybersecurity requirements, including by instructing them to use the NIST Cybersecurity Framework 2.0, which would collectively increase our national security and ensure the use of resources for security instead of compliance.

CONGRESS SHOULD ENSURE THAT CISA’S IMPLEMENTATION OF CIRCIA HONORS THE
DIRECTION OF CONGRESS

As CTIA has advised CISA, the agency’s CIRCIA rules should focus on the most serious incidents and should take concrete steps to harmonize the deeply fragmented Federal incident reporting landscape. There are several important areas where CISA can address these and other critical issues.

CISA Should Take a More Targeted Approach to the CIRCIA Rulemaking—Heeding Its Statutory Mandate to Focus on Substantial Incidents and Avoiding Rules that Will Result in Overreporting.—Taken together, CISA’s proposed rules to implement CIRCIA raise serious issues. If adopted, they would impose enormous costs on the private sector and inundate CISA with information of limited value and utility. Accordingly, as many stakeholders have consistently urged, CISA should take the opportunity to adapt and adjust its proposal, honor the direction of Congress in CIRCIA, and minimize disruption to existing public-private partnerships. CTIA is optimistic that CISA wants to get this right and will heed the numerous public comments submitted in response to its NPRM to ensure that covered entities can provide meaningful, actionable information, while minimizing the burden on victims of cybersecurity incidents to generate, report, and update voluminous and ever-changing information. Toward this goal, there are several areas of concern that the committee should work with CISA to improve:

- CISA should revisit its overly broad proposed definition of substantial cyber incident.¹⁷ Unfortunately, in the NPRM, CISA proposed an economy-wide incident reporting regime that would inundate the agency with reports about an array of events that extend well beyond what is needed for CISA to satisfy its statutory directives to render assistance to victims of serious incidents and share information with network defenders to warn other potential victims of serious threats. Consistent with stakeholder feedback from CTIA and others to take a more focused approach, and consistent with the statutory guidance requiring consideration of the impact of an incident, CISA should rethink its definition of substantial cyber incident and adopt a definition that ties a substantial cyber incident to an impact on critical infrastructure that harms national or economic security.¹⁸ Further, CISA should limit the definition of substantial cyber incident to the system or network that a covered entity needs to provide the products or services that make it a part of critical infrastructure, and CISA should exclude any incidents that do not involve the U.S. critical infrastructure facility or function.
- CISA should also reframe its definition of covered entity, which is similarly too broad and will result in over-reporting.¹⁹ CISA should limit mandatory reporting to a critical infrastructure facility or function and not require reports from the entire entity, as CISA proposed to do in its NPRM.²⁰ Failure to limit the definition of covered entity will substantially increase the volume of reportable incidents because incidents affecting non-critical business units or operations will be swept into the CIRCIA framework. Further, CISA should clearly define “entity” to clarify a parent company may not be a “covered entity” if it has a sub-entity that is distinct from the parent company, has “legal standing and is

ments of CTIA, *Establishing a 5G Fund for Rural America*, GN Docket No. 20–32, (filed Oct. 23, 2024) <https://www.fcc.gov/ecfs/document/102322146024/1>.

¹⁶Streamlining Federal Cybersecurity Regulations Act, S. 4630, 118th Cong. (2024), <https://www.congress.gov/bill/118th-congress/senate-bill/4630>; H.R. 10123, 118th Cong. (2024), <https://www.congress.gov/bill/118th-congress/house-bill/10123?s=1&r=1> (companion bill).

¹⁷CISA NPRM at 23767, Proposed § 226.1.

¹⁸CTIA proposed edits to the definition of “substantial incident” in Appendix A of its comments. Comments of CTIA, Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements, Dkt. No. CISA–2022–0010, at App. A (July 3, 2024), <https://www.regulations.gov/comment/CISA-2022-0010-0422>.

¹⁹CISA NPRM at 23684, Proposed § 226.2.

²⁰Id.

uniquely identifiable from other entities,”²¹ and meets the definition of “covered entity.”

CISA Has the Opportunity to Make Meaningful Progress Toward Harmonization and Deconfliction, Consistent with Congress’s Direction in CIRCIA.—Congress emphasized harmonization in the passage of CIRCIA, launching substantial work through the Cyber Incident Reporting Council (“CIRC”) to identify opportunities to address the problematic fragmentation of cyber incident reporting obligations. This makes sense and is good government. In the Communications Sector alone, companies are subject to multiple overlapping incident reporting obligations that can include rules from the SEC, FCC, DoD, FTC, and more. These Federal rules are in addition to State regulations that include data breach notice obligations in all States and territories, as well as cyber incident reporting requirements like those required by the New York Department of Financial Services.

The CIRC issued a report in 2023 that identified the multiplicity of cyber incident reporting requirements and offered “key recommendations” including creating a model cyber incident reporting form that Federal agencies can adopt; and streamlining the reporting and sharing of information about cyber incidents, and a potential single reporting web portal.²²

Unfortunately, however, CISA missed the opportunity to make progress to address fragmentation with its NPRM. Indeed, CISA received comments from the Congressional sponsors of CIRCIA and critical infrastructure stakeholders in response to its NPRM that were critical of the agency’s failure to promote and pursue meaningful harmonization of incident reporting obligations.²³ To help address this, CISA should take the opportunity now to fulfill the harmonization promise of CIRCIA. In particular:

- CISA should reconsider its proposed approach to addressing reporting regimes that are “substantially similar.”²⁴ Harmonization should not be limited to formal agreements with other agencies that are predicated on their adoption of the same demands that CISA included in its NPRM.
- CISA should create a voluntary option for covered entities to use a single point of entry and single Common Form for Federally-mandated cyber incident reports. Having a single Federal agency to report to during substantial cyber incidents with national security implications is essential for critical infrastructure organizations who will have “all hands on deck” dedicated to incident response with the priority to secure networks and systems. Requiring victim companies to report to multiple Government agencies with disparate requirements within condensed time frames would be detrimental to these efforts, requiring redirection of vital security resources away from incident response. Accordingly, harmonizing these requirements through reporting to a single agency via a single Common Form will provide meaningful relief to victim organizations struggling with incident response.

There Are Other Important Steps CISA Should Take to Improve and Focus the Incident Reporting Requirement.—Although not an exhaustive list, there are a number of other aspects of CISA’s proposed rules that should be re-evaluated.

- CISA should streamline the information required in reports because as drafted, the NPRM would mandate far too much information with too little clarity. The proposed reporting fields in the NPRM call for too much detail, including information that is not relevant or actionable, such as the name and role of third-party vendors helping with the incident.²⁵ The NPRM also uses vague, undefined terms and calls for details that are unclear or indeterminate. The proposed on-going supplementation of an initial incident report will be burdensome and may not provide additional information of value.

²¹ Id. at 23676.

²² DHS, *Harmonization of Cyber Incident Reporting to the Federal Government*, (Sept. 19, 2023), <https://www.dhs.gov/sites/default/files/2023-09/Harmonization%20of%20Cyber%20Incident%20Reporting%20to%20the%20Federal%20Government.pdf>.

²³ Comments of Andrew Garbarino (R-NY), Chairman, H. Homeland Sec. Subcomm. on Cybersecurity and Infrast. Prot., Dkt. No. CISA-2022-0010 (July 3, 2024), <https://www.regulations.gov/comment/CISA-2022-0010-0464>; Comments from Bennie Thompson (D-MS), Ranking Member, H. Homeland Sec. Comm., Eric Swalwell (D-CA), Ranking Member, H. Homeland Sec. Subcomm. on Cybersecurity and Infrast. Prot. & Yvette Clarke (D-NY), Dkt. No. CISA-2022-0010 (Jul. 3, 2024), <https://www.regulations.gov/comment/CISA-2022-0010-0463>; Comments of Gary Peters (D-MI), Chairman, S. Homeland Sec. and Gov’t Aff. Comm., Dkt. No. CISA-2022-0010 (Jul. 2, 2024), <https://www.regulations.gov/comment/CISA-2022-0010-0424>.

²⁴ 6 U.S.C. § 681b(a)(5)(B)(i) (creating an exception for a covered entity “required by law, regulation, or contract to report substantially similar information to another Federal agency within a substantially similar time frame.”).

²⁵ CISA NPRM at 23722.

- The proposed data retention obligations are drafted broadly and will be burdensome in scope, duration, and governance obligations.²⁶ Because of the vast amounts of network traffic that communications providers transmit, retention for 2 years of information may make the retention obligations untenable.
- CISA's enforcement approach misses an opportunity to protect victims and promote partnerships. It would substitute the collaborative relationship CISA currently has with critical infrastructure for what the NPRM suggests may be the agency's predisposition to take a punitive or adversarial approach.
- CISA should adopt adequate protections for all information submitted to the agency under CIRCIA including information in response to a request for information or subpoena. Further, the existence of such a request for information or subpoena itself should be treated as confidential.

Congress Should Encourage CISA To Establish Processes to Solicit and Meaningfully Incorporate Public Feedback.—To date, there has not been ample opportunity for stakeholders to meaningfully engage with CISA in developing the CIRCIA rules. Given the breadth and detail of the NPRM, a single opportunity for comment on the proposed rules is not sufficient to provide CISA with public input. Among other things, CISA should create a process for ex parte communications in the CIRCIA rule-making proceeding—as is common practice for other regulatory agencies.²⁷

CTIA and its members look forward to working with this committee, as well as the administration, to develop a more coordinated, forward-looking approach to responding to serious national security incidents, a more workable reporting regime, and a more harmonized cybersecurity landscape across the Federal Government.

²⁶ Id., Proposed § 226.13.

²⁷ Chairman Garbarino and Ranking Member Swalwell both spoke in support of the adoption of an ex parte process for the CIRCIA rule making during the March 11 hearing. “I promise we’re going to work on ex-parte through the CIRCIA rule, hopefully get that fixed.” Regulatory Harm or Harmonization, supra note 2. (Statement by Chairman Garbarino). “I also called on CISA [in comments on the NPRM] to establish an ex parte process to facilitate on-going engagement with the private sector.” Id. (Statement by Ranking Member Swalwell).

APPENDIX II

QUESTIONS FROM CHAIRMAN ANDREW R. GARBARINO FOR SCOTT I. AARONSON

Question 1. How does your sector view the role of regulation? What is the importance of regulation for your industry?

Answer. The electricity subsector employs a risk-based, defense-in-depth approach to cybersecurity, which includes a variety of tools and strategies that support existing voluntary and mandatory cybersecurity standards and regulations. These regulatory standards are valuable tools that set a baseline for cybersecurity of critical infrastructure for all jurisdictional owners and operators of the Bulk Power System that supports the interconnected North American energy grid. Electric companies work closely with the Federal Energy Regulatory Commission (FERC), the North American Electric Reliability Corporation (NERC), the Transportation Security Administration (TSA), and the Department of Energy (DOE) to comply with various sector regulations and reporting requirements.

Throughout the country, investor-owned electric companies are meeting and exceeding existing cybersecurity regulations and standards. As the Federal Government, States, and private sector work together to reduce risk holistically and continue to enhance cybersecurity protections of critical infrastructure, it is important that new cybersecurity requirements are not duplicative, conflicting, overlapping, or inefficient.

Regulations that are risk-based, while important, are only one part of this defense-in-depth strategy. EEI's members also focus on resilience, response, and recovery as strategies that help electric companies protect the electric grid. We also need to have strong partnerships in place across key, interdependent sectors and with Government in order to maintain the robust cybersecurity posture needed to face the realities of potential cyber warfare.

Question 2. How can the Trump administration ensure it incorporates industry feedback as it seeks to streamline the cyber reporting regime?

Answer. The Trump administration may consider existing public comments made on behalf of industry as it seeks to streamline cyber reporting. As mentioned in my testimony, EEI submitted comments on the Office of the National Cyber Director's (ONCD) Request for Information on Cybersecurity Regulatory Harmonization. In summary, EEI's comments recognized that cybersecurity regulations must keep pace with the evolving threat landscape but must also be developed in close coordination with the private sector to ensure we can implement them effectively.

EEI also submitted 3 sets of comments on the proposed rule for the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA). In summary, these comments requested that the Cybersecurity and Infrastructure Security Agency (CISA) raise the threshold and limit the scope of the definition of a "substantial cyber incident." In addition, EEI and several other critical infrastructure sectors also requested CISA implement an ex parte process for the CIRCIA rule making.

In addition to these public comments, the administration may consider the recommendations in Cyber Incident Reporting Council's (CIRC) Report on Harmonization of Cyber Incident Reporting to the Federal Government when incorporating feedback on streamlining reporting.

Question 3a. How has the cyber incident reporting process helped or hindered your ability to effectively respond to nation-state threats such as Volt Typhoon?

Question 3b. What changes, if any, to cyber incident reporting would improve your ability to respond to nation-state threats?

Question 3c. Can cyber incident reporting serve as a tool for understanding cross-sector trends for actors such as Volt Typhoon? If yes, how so?

Answer. Both the cyber incident-reporting process and the cyber information-sharing process have helped the electric power sector implement successful mitigation efforts in the face of threats such as Volt Typhoon. Specifically, the Energy Threat Analysis Center (ETAC) has proven its capabilities by enabling critical information

sharing following the Federal Government's release of threat intelligence related to Volt Typhoon. The expertise of the private sector was leveraged to develop mitigation strategies quickly that ultimately helped members of the electricity subsector, and other critical infrastructure operators, to address the threats from Volt Typhoon. This model is critical to our success in combatting sophisticated cyber adversaries and is helped by open lines of communication, highlighting the difference between threat information sharing and regulatory reporting requirements.

Streamlining Federal cyber incident reporting requirements through fewer agencies would allow our most skilled cyber experts to spend their time responding to nation-state threats rather than filling out paperwork.

One of the stated goals of the original CIRCIA legislation was to strengthen national security, including through rapidly deploying resources to victims, analyzing reporting across sectors to spot trends, and then quickly sharing that information to warn other potential victims. The final CIRCIA rule has the potential to create greater visibility into cross-sector risk, however, the proposed rule as written does not sufficiently separate the signal from the noise and thus would not be useful in understanding cross-sector trends for actors such as Volt Typhoon. CISA, as the national coordinator, should amend the definition of a substantial cyber incident in the proposed CIRCIA rule in order to glean greater insight into cross-sector risk.

Question 4. According to CISA, the total estimated cost of completing incident reports from 2024 to 2033 is approximately \$79.1 million—just short of \$8 million per year. Please explain whether you agree with CISA's estimate.

Answer. Redundant regulations add to electric companies' operational costs and misallocate limited resources from the industry's core obligation—namely, to provide safe, reliable, and affordable service to customers. EEI testified that one of our member electric companies estimated they could file roughly 65,000 reports through 2033 under the proposed rule—vastly exceeding CISA's estimate of more than 200,000 total reports during that period. Accordingly, CISA's cost estimate of approximately \$79.1 million from 2024 to 2033 is far too low.

Question 5. How can Congress ensure CISA has the tools it needs to manage the information received from CIRCIA requirements if/when the rule goes into effect?

Answer. CISA faces several challenges in improving the existing proposal to better align with Congressional intent. These include difficulties in collaborating with industry stemming from the lack of an established ex parte process, as well as issues related to natural attrition and staff turnover following the change in administration. Additionally, uncertainty around Congressional appropriations may impact CISA's ability to effectively intake incident reports by the end of 2025.

To ensure CISA is well-equipped to manage the information received from CIRCIA, Congress may consider conducting oversight regarding its current status—including staffing levels, resource needs, the projected time line for final rule completion, and anticipated future engagement with industry stakeholders. Specifically, Congress should pursue oversight to ensure that CISA has the appropriate infrastructure in place to intake a high volume of incident reports and secure this sensitive information accordingly.

Question 6. How can Congress support cyber risk management regulatory harmonization?

Answer. As stated in my testimony, Congress should work with CISA to reduce the burden of the proposed CIRCIA rule and focus on a few areas for improvements.

First, conduct oversight regarding the current status of CIRCIA, including staffing levels, resource needs, the projected time line for final rule completion, and anticipated future engagement with industry stakeholders.

Second, facilitate coordination amongst Congressional committees of jurisdiction to align CISA, Sector Risk Management Agencies, and other regulators, and to review concerns with existing Federal reporting requirements, including the national security concerns associated with the public disclosure of incidents required by the U.S. Securities and Exchange Commission (SEC).

Third, further clarify CISA's role in cybersecurity regulatory harmonization in relation to other Federal entities.

Fourth, reauthorize the Cybersecurity Information Sharing Act of 2015. Mandatory incident reporting and voluntary information sharing both are valuable tools in ensuring the cybersecurity of critical infrastructure.

Question 7. Is there a need to ensure cybersecurity regulations impacting one sector do not negatively impact other dependent sectors? Please explain.

Answer. Currently, CISA serves as the National Coordinator for the Security and Resilience of Critical Infrastructure, pursuant to Presidential Policy Directive-21 and its successor document, National Security Memorandum-22. As national coordinator, CISA is charged with leading a whole-of-Government effort to secure U.S. critical infrastructure. As part of this role, CISA has a duty and an obligation to

ensure any new or existing regulations do not negatively impact other dependent sectors.

In addition, ONCD has a role to play in ensuring cybersecurity regulations do not negatively impact other dependent sectors. As an office within the White House, ONCD has a unique role in bringing independent regulators and other Federal agencies to the table to streamline regulations. ONCD may consider reviewing the negative impacts associated with existing cross-sector Federal reporting requirements, including the national security concerns associated with the public disclosure of incidents required by the SEC.

Question 8. What are the challenges to harmonization and reciprocity in the energy sector?

Answer. For years, EEI members have worked with Federal, State, and local governments to protect and defend the electric grid from cyber-related disruptions. Through various cyber initiatives, information-sharing activities, and exercises, EEI members have strengthened their resilience to cyber attacks because they understand that a reliable and secure supply of electricity is necessary to power the U.S. economy and safeguard this country's national security.

The energy sector has been subject to NERC's Reliability Standards (including its Critical Infrastructure Protection (CIP) Standards), as approved and enforced by the Federal Energy Regulatory Commission (FERC), for years. One of the greatest challenges to harmonization is that any new proposed cybersecurity and voluntary standards must be developed in harmony with these existing standards to ensure as little conflict as possible. To avoid confusion and challenges during a cybersecurity incident, EEI members believe it would be valuable to designate one Government agency that would be responsible for coordinating with other agencies. In addition, it is important to remember that electric companies exist in diverse, ever-changing operating environments and therefore need to have the ability to tailor each of their individual preparation, response, and recovery activities accordingly.

QUESTIONS FROM CHAIRMAN ANDREW R. GARBARINO FOR HEATHER HOGSETT

Question 1. How does your sector view the role of regulation? What is the importance of regulation for your industry?

Answer. Financial institutions are subject to complex and multifaceted regulatory requirements from the Office of the Comptroller of the Currency (OCC), the Federal Reserve Board (FRB), the Federal Deposit Insurance Corporation (FDIC), the Consumer Financial Protection Bureau (CFPB), the Securities and Exchange Commission (SEC), and the Commodity Futures Trading Commission (CFTC), among others at the State and international levels. Included in the regulatory regime is rigorous supervision and examinations from the prudential banking regulators—the OCC, FRB, and FDIC. Supervision by the banking agencies seeks to ensure that financial institutions operate in a safe and sound manner. During these reviews, on-site examiners evaluate compliance with statutory requirements and whether firms implement appropriate controls in areas such as information security, third-party risk management, operational resilience, capital and liquidity management, and appropriate board oversight.

The financial sector has been highly regulated for many years and firms have established governance and compliance teams to engage with regulators. In a number of areas, cybersecurity included, there is significant overlap between agencies that diverts attention of critical staff toward compliance. A reassessment of this approach is warranted to ensure the overall regulatory regime appropriately balances compliance demands with security realities. For instance, examiners should focus on enhancing security outcomes rather than requiring extensive documentation of processes and procedures.

Question 2. How can the Trump administration ensure it incorporates industry feedback as it seeks to streamline the cyber reporting regime?

Answer. The best way to incorporate industry feedback and streamline cyber reporting is to have an active and iterative dialog with critical infrastructure sectors. This is particularly true for CIRCIA, where close collaboration with industry is necessary not only to inform the final rule and achieve the balanced reporting structure contemplated by the underlying statute, but also to monitor implementation and determine if adjustments are necessary.

The Trump administration could also leverage the authorities outlined in Executive Order 142151¹ to limit the ability of independent agencies to promulgate dupli-

¹Executive Order No. 14,215, Ensuring Accountability for All Agencies, 90 Fed. Reg. 10447 (Feb. 24, 2025).

cative rules. This could help prevent unhelpful regulatory requirements—like the SEC’s cyber incident disclosure rule—that directly conflicts with the intent behind CIRCIA and arms cyber criminals with information they can leverage to inflict further harm on victim companies.

Question 3. According to CISA, the total estimated cost of completing incident reports from 2024 to 2033 is approximately \$79.1 million—just short of \$8 million per year. Please explain whether you agree with CISA’s estimate.

Answer. In its proposed rule, CISA calculated that \$79.1 million figure by estimating that cyber incident and ransom payment reports would take 3 hours to complete respectively, joint cyber incident and ransom payment reports would take 4.25 hours, and supplemental reports would take 7.5 hours.² CISA then assumed a weighted average compensation rate of \$86.29 for the staff compiling the reports.³

Because CIRCIA has not yet gone into effect, it is difficult to say with certainty whether CISA’s estimate is accurate. Nevertheless, 1 financial institution noted it takes them an average of 20.5 hours to complete reporting requirements associated with the European Union’s Digital Operational Resilience Act. Moreover, another firm noted that the average compensation rate for personnel responsible for completing reports was \$100—up from \$75 several years ago. Both data points indicate that CISA likely underestimated the time and cost it will take firms to complete required reports.

Question 4. How can Congress support cyber risk management regulatory harmonization?

Answer. The central challenge for most financial institutions is the collective impact of overlapping cyber examinations by multiple regulators. Compliance obligations associated with exams now consume up to 70 percent of cyber teams’ time. During exams, which can take weeks, firms frequently produce hundreds, and sometimes thousands, of pages of documents responding to regulators’ requests.

Congressional action is needed to help ensure new and existing cybersecurity requirements support better security and resilience outcomes instead of simply adding additional procedural mandates unrelated to real risk. To realize this goal, it is imperative that regulators enhance their coordination and not duplicate efforts by better leveraging each other’s documentation, tests, evaluations, and findings.

Leadership from 1 or more White House offices (e.g., Office of the National Cyber Director, Office of Management and Budget, etc.) would help ensure independent regulatory agencies work together to avoid duplication and conflict among their respective requirements. Agencies should be required to take into consideration the full scope and impact of regulatory requirements that firms adhere to rather than only looking at a subset. While each individual regulatory requirement (including rules, supervision, examination, and enforcement) may be well-intended, the collective impact of multiple requirements can interfere with a firm’s ability to operate and focus on security improvements. Congressional attention and oversight on this vital issue can help inform a streamlined approach and hold regulatory agencies accountable.

Question 5. Is there a need to ensure cybersecurity regulations impacting 1 sector do not negatively impact other dependent sectors? Please explain.

Answer. Numerous large-scale cyber incidents over the last several years demonstrate the interconnected nature of our systems and the need for all critical infrastructure sectors to implement appropriate security controls. For cyber incident reporting requirements, it is particularly important that those obligations be appropriately tailored and do not detract from response efforts.

Without proper streamlining, the purpose behind many reporting mandates—to improve information sharing, prevent harm from spreading, and help impacted entities resume operations quickly—will be undermined as victim companies are consumed by filling out Government forms and reducing litigation and compliance risks. This can lead to delays and a reticence to share information confidentially and risks cascading harm between and across critical infrastructure sectors.

Question 6. What are the challenges to harmonization and reciprocity in the financial sector?

Answer. Achieving regulatory harmonization and reciprocity in the financial sector is challenging due to slight variations in the authorities of each banking regulator. Despite those modest differences, each agency’s cybersecurity requirements generally apply to the same activities, policies, and procedures within firms. Therefore, it is the cumulative effect of overlapping requirements that leads to the unintended consequence of diverting resources away from security operations. For exam-

²Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements, 89 Fed. Reg. 23644, 23745 (Apr. 4, 2024).

³Id.

ple, financial institutions reported that roughly 25 percent of regulatory requests during an exam are duplicative of those already received from other agencies.

A more effective approach would be to have banking agencies conduct a single coordinated cyber review each year and leverage existing documentation to fulfill those obligations rather than creating unique work product for each evaluation.

Question 7. Are financial institutions utilizing artificial intelligence and automation to reduce compliance burdens and help their security teams focus on incident response and threat mitigation?

Answer. Financial institutions have used AI tools for threat detection and mitigation for more than a decade and continue to expand its use to better serve and protect customers and improve internal efficiencies. Machine learning models have been used for several years to detect fraud in credit and debit card transactions, check transactions, digital payments, and account openings. AI-driven network security systems are employed to continuously monitor both incoming and outgoing network traffic and detect anomalies (such as unusual login times, atypical data transfers, or irregular access patterns) that may signify a breach attempt. As another example, AI is also used to automate responses to spam and phishing attempts, mitigating risks before they escalate.

Firms also use AI to reduce regulatory compliance burdens, freeing personnel and resources to better focus on security risks. For example, a BPI member bank has used generative AI to complete a preliminary review of third-party cybersecurity assurance responses and subsequently direct relevant human reviewers to potential gaps in response completeness against the bank's requirements.

QUESTIONS FROM CHAIRMAN ANDREW R. GARBARINO FOR ROBERT MAYER

Question 1. How does your sector view the role of regulation? What is the importance of regulation for your industry?

Answer. USTelecom and its members are steadfast in their commitment to cybersecurity. Our members meet—and very often exceed—cybersecurity requirements as conditions for authorization to provide services, receive Government funding, bid on Government contracts, and participate in Government programs, as well as to ensure customer trust in the competitive global marketplace. USTelecom's Cybersecurity Culture Report, focusing on small and medium enterprises, found that telecom providers of all sizes, including smaller ones, have a mature cybersecurity culture—along with financial services and IT respondents—when compared to other critical infrastructure sectors.¹

The majority of cybersecurity regulations applicable to our sector generally fall into 1 of 2 principal categories: (1) baseline cybersecurity requirements; (2) cyber incident reporting requirements.

Baseline Cybersecurity Requirements.—Currently, the broadband industry contends with cybersecurity baselines across various programs and initiatives, including multiple FCC cybersecurity proceedings—such as those addressing the Emergency Alert System/Wireless Emergency Alerts system, section 214 authorizations, the Uniendo a Puerto Rico Fund, the Connect USVI Fund, and the Connect America Fund—as well as the Broadband Equity, Access, and Deployment (“BEAD”) Program administered by the National Telecommunications and Information Administration (“NTIA”), and the Department of Justice (“DOJ”) U.S. Bulk Sensitive Data regulation.

There is a relatively easy way for policy makers to bring consistency to these proceedings: by grounding all cybersecurity baselines for our sector in the bipartisan requirements adopted by the Federal Communications Commission (“FCC”) as conditions for receiving 5G funding—an approach firmly grounded in the broadly utilized National Institute of Standards and Technology (“NIST”) Cybersecurity Framework (“CSF”).

Specifically, we would propose that broadband providers’ “cybersecurity risk management plans must reflect at least the [NIST Framework], or any successor version of the NIST Framework” and these plans “must reflect established cybersecurity best practices that address each of the Core Functions described in the NIST

¹ *Cybersecurity Culture Report: The State of Small and Medium-Sized Critical Infrastructure Enterprises 4*, USTelecom (Feb. 15, 2023), <https://www.ustelecom.org/research/2023-cybersecurity-culture-report> (“The IT and Communications (Comms) sectors stood out as having the strongest cybersecurity cultures, with the Comms sector scoring most consistently high across the 5 dimensions. The IT, Comms, and Financial Services sectors were the most likely to perform important cybersecurity culture practices including performance appraisals, rewards for proactive behavior, training initiatives, and routine communications with internal stakeholders.”).

Framework”.² These core functions, which were updated in 2024 to include governance, would ensure companies are implementing practices necessary to Govern, Identify, Protect, Detect, Respond, and Recover.

Importantly, in the above-mentioned proceeding, the FCC had the foresight to avoid picking winners and losers among competing sets of best practices, and also avoiding practices that, due to their prescriptiveness and inflexibility, would not stand the test of time. For example, according to CISA, their Cybersecurity Performance Goals (“CPGs”) require revisions on a frequent basis “with a targeted revision cycle of at least every 6 to 12 months”.³ A given company’s practices may need to change even more quickly in response to real-world developments, with shifts measured in hours and minutes—not months. Nobody on the industry or Government side of the public-private partnership can predict with certainty today which cybersecurity practices will best serve the ecosystem long-term, which is why the private sector needs the flexibility to innovate.

Congress should, at a minimum, encourage all current and prospective Federal agencies with jurisdiction over the communications sector to align with this approach. Moreover, this framework may prove adaptable to other sectors as well. Such harmonization would streamline compliance efforts, reduce administrative burdens, and allow providers to direct resources toward meaningful, risk-based security initiatives that genuinely strengthen the Nation’s critical communications infrastructure.

Cyber Incident Reporting.—USTelecom’s members are or soon will be subject to incident reporting rules or requirements promulgated by the SEC, FCC, FTC, DOJ (Team Telecom), FAR Council, FISMA, and State governments. In addition, our members have voluntary information-sharing relationships with a broad array of Government agencies, including the intelligence community, and of course DHS. Put simply, the need for harmonization has never been greater.

When incident reporting guidelines are harmonized, response efforts can be more coordinated and efficient. This streamlining is critical during cyber crises, where the speed and accuracy of information sharing and response can determine the severity of impact. A unified reporting framework enables faster mobilization of resources, clearer communication, and more effective incident resolution.

Harmonized reporting requirements are easier for entities to follow and for regulators to enforce. This clarity can lead to higher compliance rates, as entities are less likely to be overwhelmed by complex and conflicting requirements. In turn, better compliance enhances the overall security posture of critical infrastructure sectors. Moreover, a unified approach to data collection can improve the quality and security of the data submitted. With standardized protocols, security measures can be more robustly implemented and maintained. This is crucial in a field where data sensitivity and integrity are paramount.

Given the importance of harmonization, our members find it very concerning that the harmonization that CISA is trying to accomplish will be effectively null because covered entities will still be subject to a multitude of conflicting and duplicative reporting requirements across Federal agencies. This is due to the rule making not sufficiently addressing Congress’s directive to solve for this issue. If CISA is serious about harmonizing reporting requirements, it must work to mitigate this challenge and address it in the rules.

Question 2. How can the Trump administration ensure it incorporates industry feedback as it seeks to streamline the cyber reporting regime?

Answer. USTelecom, joined by 20 other organizations, previously submitted a letter urging the establishment of an ex parte process to facilitate further stakeholder engagement and dialog on the implementation of CIRCIA. Although this request was declined by prior CISA leadership, we remain convinced that such a process is essential to correcting course.

As the implementation deadline nears, we are deeply concerned that the rule, as currently proposed, deviates substantially from Congressional intent and would, if finalized, do more harm than good to our national security. Without immediate action to initiate an ex parte process, it may fall to Congress and CISA to consider all available remedies—including potential rescission—to ensure the rule aligns with the statute and serves the national interest.

Question 3a. How has the cyber incident reporting process helped or hindered your ability to effectively respond to nation-state threats such as Volt and Salt Typhoon?

² *Establishing a 5G Fund for Rural America*, FCC 24–89, at ¶122.

³ CISA, Cross-Sector Cybersecurity Performance Goals (2023) at 14, https://www.cisa.gov/sites/default/files/2023-03/CISA_CPG_REPORT_v1.0.1_FINAL.pdf.

Answer. The current incident reporting landscape, which lacks harmonization across agencies and frameworks, can increase the complexity of responding to cyber incidents, including those involving nation-state actors.

Question 3b. What changes, if any, to cyber incident reporting would improve your ability to respond to nation-state threats?

Answer. A single, streamlined point of contact during incidents would help reduce operational friction and support more effective coordination.

Question 3c. Can cyber incident reporting serve as a tool for understanding cross-sector trends for actors such as Volt and Salt Typhoon? If yes, how so?

Answer. Potentially, yes. Incident reporting, when aggregated and appropriately shared, can offer insights into broader threat patterns. This kind of visibility may help inform risk management decisions across sectors. We appreciate efforts by Government partners to analyze and contextualize threat data in support of shared security objectives.

Question 4. According to CISA, the total estimated cost of completing incident reports from 2024 to 2033 is approximately \$79.1 million—just short of \$8 million per year. Please explain whether you agree with CISA's estimate.

Answer. While we appreciate CISA's effort to provide a cost estimate, we respectfully disagree that the projected figure accurately reflects the true burden of compliance under the proposed rule.

First, the proposed reporting requirements, as currently drafted, lack sufficient clarity regarding critical thresholds, definitions, and triggering events. Without a more precise understanding of what constitutes a "covered cyber incident" or the scope of entities subject to reporting, it is not possible to develop a reliable estimate of reporting frequency or the corresponding financial and administrative burden.

Second, even under conservative assumptions, the volume of reports that CISA may receive—particularly during and immediately after high-impact events—could far exceed what its current infrastructure is equipped to manage. This raises substantial concerns about both the Government's capacity to process, analyze, and respond to the information in a timely manner, and the costs that private entities will incur to ensure compliance in the face of ambiguity.

In short, while the \$79.1 million estimate may serve as a starting point for discussion, it does not, in our view, reflect the scale, complexity, or fluidity of the real-world costs associated with the rule as proposed. Any meaningful assessment of compliance burden must await further clarity around key definitional elements and implementation thresholds.

Question 5. How can Congress support cyber risk management regulatory harmonization?

Answer. Congress has a critical role in reinforcing agency harmonization efforts through strategic oversight and, if necessary, legislative support, as well as by tackling the problem of State-level fragmentation. We are increasingly concerned about the proliferation of inconsistent State-level cyber regulations, which risk fragmenting the national cybersecurity landscape. To preserve coherence and legal certainty in this domain, Congress should explore policy mechanisms such as Federal preemption and safe harbor provisions, thereby ensuring that State actions do not undermine the development of a unified and effective national cybersecurity framework.

Question 6. Is there a need to ensure cybersecurity regulations impacting 1 sector do not negatively impact other dependent sectors? Please explain.

Answer. Yes, it is important to ensure that cybersecurity regulations directed at 1 sector do not create unintended legal or operational consequences for other, interdependent sectors. From a regulatory design perspective, clarity and precision are essential. Cross-sector dependencies are complex, and imposing obligations on 1 industry without a clear understanding of how those rules interact with adjacent systems can lead to conflicting requirements, duplicative compliance regimes, and operational inefficiencies. In the case of telecommunications, which frequently supports—but does not control—the systems of other sectors, regulatory spillover can result in unnecessary friction without materially advancing cybersecurity outcomes.

Question 7. What are the challenges to harmonization and reciprocity in the communications sector?

Answer. The core obstacle is that regulators act independently, with no binding framework or mechanism for alignment. Compounding this is a lack of centralized strategic direction—there's no top-down leadership driving coherence across jurisdictions. That is why the Office of the National Cyber Director ("ONCD") needs to lead: not just as a facilitator, but as the central thought leader ensuring national alignment in cyber policy.

Question 8. Would more voluntary reporting encourage more information sharing from regulated entities? Why or why not?

Answer. More voluntary reporting could encourage increased information sharing from regulated entities—but only if there are sufficient legal protections in place for the information shared. Entities are often reluctant to report cybersecurity incidents or vulnerabilities voluntarily due to concerns about legal liability, regulatory consequences, or reputational harm. Therefore, the presence of robust protections is critical to fostering trust and cooperation.

This is why it is essential that Congress reauthorize the Cybersecurity Information Sharing Act of 2015 (CISA 2015) and also consider mechanisms to enhance its protections. CISA 2015 established important liability, regulatory, and FOIA protections for entities that voluntarily share cyber threat indicators and defensive measures with the Federal Government. However, under the current law, these protections typically are more difficult to obtain, or are less certain, unless information is shared directly with the Department of Homeland Security.

To truly encourage broad and timely information sharing, protections should follow the information, not just the pathway. For example, entities should receive the same legal safeguards if they share cyber threat information with any relevant Federal agency involved in cybersecurity, such as the FBI, NSA, or sector-specific agencies like the Department of Energy or the FDA. This would reduce confusion about the “correct” reporting pathway and lower barriers to voluntary participation.

In short, more voluntary reporting can lead to greater information sharing—but only if the legal framework makes that sharing safe and practical. Strengthening and updating CISA 2015 is a necessary step in that direction.

QUESTIONS FROM CHAIRMAN ANDREW R. GARBARINO FOR ARI SCHWARTZ

Question 1. What can the Federal Government do to ensure businesses do not need to choose between regulatory compliance and cybersecurity?

Answer. As this question suggests, too frequently, governments are requiring organizations to follow a set of rote and static checkbox assessments or audit standards that are often duplicative and not dynamic enough to address current and future cyber threats. Several approaches that the Federal Government should consider are streamlining cybersecurity regulations, facilitating regulatory harmonization and reciprocity, pivoting from compliance to risk management, and providing clear implementation and compliance guidance and tools.

Regulatory Streamlining

Regulatory streamlining can be accomplished in 2 ways. First and foremost, the Federal Government should strive to ensure that cybersecurity regulations only include controls that have demonstrably provided resilience for the sector in question. This approach will allow entities to focus limited resources on ensuring the timely and comprehensive implementation of controls known to improve security and resiliency. An excellent example of this approach is the Cyber Risk Institute’s (“CRI”) development of the financial sector profile¹ for the National Institute of Standards and Technology’s (“NIST”) Framework for Improving Critical Infrastructure Cybersecurity (“CSF”).² Additionally, the Federal Government can achieve a measure of regulatory streamlining by ensuring the processes required to be compliant with cybersecurity regulations are as clear and simple as possible.

Regulatory Harmonization

As I detailed in my testimony, cyber incident reporting is an excellent example of how similar but disparate requirements across a growing number of reporting regimes has become burdensome for businesses. “As more organizations build reporting structures for different purposes, duplication, misalignment, fragmentation, and other issues start to set in. This includes concerns around the amount and types of data fields, differing taxonomies, time frames for reporting, and more.”³

While there are understandable motivations for Federal regulators of different sectors to approach cybersecurity regulations with a nuanced, sector-specific lens, the Federal Government should encourage as much regulatory harmonization across regimes as is practicable. As the Cybersecurity Coalition has previously stated on this topic, we believe that “building compliance schemes that focus on consistent

¹Cyber Risk Institute, CRI Profile. <https://cyberriskinstitute.org/the-profile/>.

²NIST, Cybersecurity Framework. <https://www.nist.gov/cyberframework>.

³Cybersecurity Coalition, Testimony Before the U.S. House of Representatives Homeland Security Committee Cybersecurity and Infrastructure Protection Subcommittee on “Regulatory Harm or Harmonization? Examining the Opportunity to Improve the Cyber Regulatory Regime,” March 11, 2025. <https://homeland.house.gov/wp-content/uploads/2025/03/2025-03-11-CIP-HRG-Testimony.pdf>.

standards, and that enable automation and reuse of compliance artifacts would create meaningful efficiencies.”⁴

One method that the Cybersecurity Coalition has previously advocated for consideration as a means to providing regulatory harmonization is a co-regulatory model.⁵ We consider “coregulatory models such as Federal Financial Institutions Examination Council (“FFIEC”) to be a potentially effective method to establish uniform requirements and oversight across multiple regulatory regimes and supervisory agencies.”⁶

Regulatory Reciprocity

The Federal Government should also look to support cyber regulatory reciprocity. At a high level, cyber regulatory reciprocity would enable a business to have their existing certification of compliance with one regulation be considered proof of meeting overlapping requirements from other regulations.

The Coalition has previously pointed to the Federal Risk and Authorization Management Program (“FedRAMP”), which was established to provide a cost-effective, risk-based approach for the adoption and use of cloud services by the Federal Government, as a potential model.⁷ As the Cybersecurity Coalition has previously noted, “FedRAMP’s legal and governance structure, as well as FedRAMP’s principle of ‘reusability,’ are designed to enable compliance with less redundancy,” and that “elements of the FedRAMP model could be leveraged as the basis for coregulatory approaches that encompass a broader set of cybersecurity issues.”⁸ While we acknowledge that there are well-known challenges and implementation issues facing FedRAMP itself, the reciprocity principles at the core of the program are sound.

Pivoting to Risk Management

As was mentioned at the beginning, many current Federal regulatory compliance regimes are static checkbox assessments or audit standards that often fail to keep pace with evolutions within the technological and threat landscape. Furthermore, this type of compliance regime is prone to giving a false sense of security and maturity. This is often a result of binary “yes/no” questions that fail to adequately interrogate cybersecurity complexity and that can often be successfully complied with despite failing to actually achieve an intended underlying security goal.

The Federal Government can address these shortcomings and better harmonize the cyber regulatory environment by pivoting existing regimes toward alignment with a single framework that is centered on cyber risk management. Cyber risk management and risk-based approaches enable businesses to better understand their security posture, prioritize risks based on their unique environment and mission, and ensure their security investments are effective.

The Cybersecurity Coalition urges Congress and the administration to embrace a risk management approach. Such a transition would be eased by the fact that NIST has been a global leader in cyber risk management for years. The constellation of frameworks they have developed in conjunction with industry includes the aforementioned CSF, the Privacy Framework,⁹ the Risk Management Framework,¹⁰ the Cybersecurity Supply Chain Risk Management,¹¹ and, most recently, the Artificial Intelligence Risk Management Framework.¹²

In particular, we would urge the Federal Government to ensure that regulatory regimes are aligned with the NIST CSF. The CSF is particularly well-regarded, is applicable across sectors, agnostic to size and structure, and is already widely adopted. The CSF is also seen as a model for partner nations, which is helpful for U.S. companies conducting business in other regions. Regulatory alignment with the CSF would minimize regulatory duplication and fragmentation through an existing industry-approved framework.

⁴ Cybersecurity Coalition, Response to the Office of the National Cyber Director. *RE: Request for Information on Cybersecurity Regulatory Harmonization* https://cdn.prod.website-files.com/660ec3caef47b817df2800ae/660ec3caef47b817df28023f_Cybersecurity%20Coalition%20Comments%20to%20ONCD%20RFI%20on%20Cybersecurity%20Regulatory%20Harmonization%2020231031.pdf.

⁵ Ibid.

⁶ Ibid.

⁷ Ibid.

⁸ Ibid.

⁹ NIST, Privacy Framework. <https://www.nist.gov/privacy-framework>.

¹⁰ NIST, Risk Management Framework. <https://csrc.nist.gov/projects/risk-management/about-rmf>.

¹¹ NIST, Cybersecurity Supply Chain Risk Management (C-SCRM). <https://csrc.nist.gov/projects/cyber-supply-chain-risk-management>.

¹² NIST, AI Risk Management Framework. <https://www.nist.gov/itl/ai-risk-management-framework>.

Tools and Guidance

Streamlining, harmonization, and reciprocity would be the most impactful approaches to ensuring that businesses do not have to choose between regulatory compliance and cybersecurity. However, additional efficiency can be found by ensuring that regulatory requirements and processes are accompanied by clear implementation and compliance guidance and tools. Less time spent on understanding what is being asked of businesses and more tools being available to simplify and ease compliance means more time and resources actually being dedicated to cybersecurity.

Question 2. How would you evaluate interagency cooperation in regard to cyber incident reporting? Do Federal agencies adequately collaborate and share information? Please explain.

Answer. Currently, there is a patchwork of voluntary and required cyber incident reporting from private-sector entities to Federal departments and agencies. For example, the Transportation Security Administration's Security Directives for surface transportation, rail, and pipelines require covered entities to report to CISA Central within 24 hours. Within the financial sector, covered entities are required to directly notify their regulators—the Office of the Comptroller of the Currency, the Federal Reserve System, and Federal Deposit Insurance Corporation—of a computer-security incident within 36 hours. Contractors within the Defense Industrial Base report to the Department of Defense's Cyber Crime Center using an on-line portal. This is all on top of the Federal Government's push for voluntary cyber incident reporting to either CISA Central or to a local FBI Field Office. Once received by the Government agencies through these various means, there is not a routinized method or process for sharing cyber incident reports among the relevant agencies. Rather, the experience of Coalition members is that information is shared ad-hoc or specific to a single incident. Furthermore, there is little bi-directional information sharing. Coalition members often don't know what happens with the information they provide to the Government—with whom it was shared or what was even done with the information. To the greatest extent possible, Federal entities receiving cyber incident information should collect, analyze, contextualize, and enrich that data; and then share it back into the larger community along with any mitigation techniques and strategies in order to prevent additional, similar incidents.

This perspective appears to be supported by Government reports. The Cybersecurity Coalition's previous comments to the Office of the National Cyber Director ("ONCD") on this issue cited "a 2020 Government Accountability Office report reviewed the assessment processes employed by several large Federal agencies for security of data provided to States."¹³ The report found that none of the agencies had policies for coordinating assessments with each other despite OMB requirements under Circular A-130 requiring agencies to coordinate.¹⁴ While this report was "focused on State assessments, it demonstrates coordination challenges among Federal agencies and highlights the potential value in streamlined regulatory models that incorporate multiple levels of agency communication."¹⁵

Without established processes that can be tracked against security outcomes, it is difficult, if not impossible, to evaluate the effectiveness of interagency sharing of cyber incident reports.

Question 13. According to CISA, the total estimated cost of completing incident reports from 2024 to 2033 is approximately \$79.1 million—just short of \$80 million per year. Please explain whether you agree with CISA's estimate.

Answer. The Cybersecurity Coalition has not thoroughly evaluated CISA's estimate and is not in a position to comment on the potential cost of completing cyber incident reporting. It is difficult to assess how the constantly-changing legal and regulatory environment, threat environment, and the industry's growing cybersecurity maturity and resiliency all contribute to incident reporting costs over an extended period. Additionally, it is not clear if this estimate represents the cost for victims to report incidents, and/or the cost for CISA to ingest and take action on incident reports. There are associated costs on both ends of cyber incident reporting.

¹³ GAO, *Selected Federal Agencies Need to Coordinate on Requirements and Assessments of States*, May 2020, <https://www.gao.gov/assets/gao-20-123.pdf>.

¹⁴ OMB Circular A-130, *Managing Information as a Strategic Resource*, Jul. 28, 2016, <https://www.federalregister.gov/documents/2016/07/28/2016-17872/revision-of-omb-circular-no-a-130-managing-information-as-a-strategic-resource>.

¹⁵ Cybersecurity Coalition, *Response to the Office of the National Cyber Director. RE: Request for Information on Cybersecurity Regulatory Harmonization* https://cdn.prod.website-files.com/660ec3cae47b817df2800ae/660ec3cae47b817df28023f_Cybersecurity%20Coalition%20Comments%20to%20ONCD%20RFI%20on%20Cybersecurity%20Regulatory%20Harmonization%2020231031.pdf.

Question 4. How can Congress ensure CISA has the tools it needs to manage the information received from CIRCIA requirements if/when the rule goes into effect?

Answer. CISA's ability to manage the information received from CIRCIA's requirements once it goes into effect will be largely dependent on the volume of reporting that they must contend with. As I noted in my testimony, the Cybersecurity Coalition feels that CISA's scope in the breadth of covered entities and covered incidents is too broad.

CISA would be in a far better position to manage the information they receive through CIRCIA if they narrow the scope of entities. The Cybersecurity Coalition advocates for abandoning the approach of applying reporting requirements to all entities within critical infrastructure sectors and instead have them "focus on Systemically Important Entities (SIEs) that own or operate critical infrastructure systems and assets whose disruption would have a debilitating, systemic, or cascading impact on national security, the economy, public health, or public safety."¹⁶ Additionally, we would advocate for a more modest definition of types of reports requested.

Question 5. How can Congress support cyber risk management regulatory harmonization?

Answer. Congress can support cyber risk management regulatory harmonization by bolstering on-going Governmental efforts. In particular, the Cybersecurity Coalition would again highlight NIST's work in this field.

Among their many important cybersecurity contributions, the NIST CSF is likely the most domestically and internationally successful. For over a decade, the NIST CSF has showcased American leadership in cyber risk management by providing a framework to help organizations identify, manage, and reduce cyber risk. Widespread adoption of the NIST CSF has helped create a common perspective and language through which organizations can understand this issue. The proven track record and wide-spread adoption of the CSF makes it an ideal candidate as the basis for the Federal Government to align existing and future cyber regulatory regimes. The Cybersecurity Coalition would encourage the Federal Government to continue to support the development and maintenance of the CSF alongside such alignment as a way to improve cyber risk management harmonization while generally improving the U.S. cybersecurity ecosystem.

Question 6. How is the private sector using AI-enabled and automation software to improve their cyber defense posture and make compliance easier and more effective?

Answer. The private sector has long used AI-enabled and automation technologies to strengthen cybersecurity and streamline compliance processes, and new advancements in AI have quickly become part of industry's toolkit. These tools are enhancing existing capabilities for threat detection, response, and vulnerability management, but also have the potential to change how organizations approach risk management and compliance.

Artificial intelligence has long been used to detect threats with more precision and speed than traditional tools or human analysts can do alone. By analyzing vast amounts of data—network traffic, user behavior, system logs—AI systems can identify anomalies and potential threats that might otherwise go unnoticed. Behavioral analytics, in particular, allow organizations to detect insider threats and subtle indicators of compromise, such as lateral movement or privilege escalation, with a level of context-aware insight that manual methods cannot achieve.

Once certain kinds of threats are detected, automation can be used to isolate endpoints, disable accounts, or block malicious IP addresses within seconds. These security orchestration platforms can integrate with other parts of the IT stack to ensure a coordinated, organization-wide response that dramatically reduces the time it takes to contain incidents.

In parallel, AI is playing a growing role in vulnerability management. Rather than relying solely on scheduled scans and manual prioritization, modern systems use machine learning to continuously monitor codebases, applications, and infrastructure for vulnerabilities. They assess each issue in terms of exploitability and business impact, allowing organizations to prioritize patching efforts in a more strategic way. This integration of AI into operations (devops) practices also enables real-time code scanning during development, reducing the risk of deploying insecure software.

Compliance—once viewed as a burdensome and reactive function—is also being reshaped by AI. Natural language processing tools can now analyze regulatory texts and map them to internal controls, highlighting gaps and inconsistencies automati-

¹⁶Cybersecurity Coalition, Comments to CISA: *Re: Request for Information on the Cyber Incident Reporting for Critical Infrastructure Act of 2022*. <https://www.cybersecuritycoalition.org/filings/comments-to-cisa-circia-rfi-docket-number-2022-19551-cisa-2022-0110>.

cally. Instead of assembling audit evidence manually, compliance platforms that are powered by automation can collect logs, access records, and other necessary documentation in real time. This not only reduces labor, but also improves the accuracy and timeliness of reporting.

Identity and access management has similarly benefited from AI integration. Traditional access control models are being replaced or supplemented by dynamic, risk-based systems that adapt to contextual factors such as location, device health, and user behavior. These systems can detect and respond to anomalies that suggest compromised credentials or unauthorized activity, strengthening defenses without impeding legitimate workflows.

Data protection and privacy compliance—particularly important under regulations like GDPR and CCPA—have also become more manageable through AI. Automated data discovery and classification tools can identify sensitive information across disparate systems, even in environments with limited visibility or extensive use of shadow IT. Combined with AI-enhanced data loss prevention tools, organizations are better equipped to enforce policies around data handling and respond quickly to potential breaches.

The cumulative effect of these technologies is a more proactive, scalable, and resilient security and compliance posture. Organizations are no longer solely reacting to threats and regulations—they are leveraging automation to anticipate risks, enforce policies consistently, and maintain continuous audit readiness. While no technology eliminates the need for skilled human oversight, AI and automation are significantly enhancing the capabilities of security and compliance teams and enabling them to operate at a strategic level.

Question 7. How can the Trump administration ensure it incorporates industry feedback as it seeks to streamline the cyber reporting regime?

Answer. Providing ample opportunity for industry feedback and then adequately incorporating that feedback is critical to ensuring cyber incident reporting streamlining and harmonization efforts are as successful as possible. The insight gained through feedback from businesses that are required to implement and comply with these various reporting regimes is valuable and often nuanced.

Despite this, and as I testified, there was a distinct lack of industry engagement by CISA under the previous administration when contemplating this aspect of CIRCIA. This was a mistake that the Trump administration should rectify. We would encourage the Trump administration to work both inside and outside the existing regulatory structures to achieve this.

From inside the existing regulatory structures, this feedback can be ensured through a process that places emphasis on broad engagement. This may include holding appropriately numerous and lengthy Request for Information (“RFI”) or Request for Comment (“RFC”) periods and listening sessions. In addition, we would encourage the Trump administration to ensure there are appropriately lengthy opportunities for industry to review and submit comments on public drafts of proposed cyber incident reporting regimes. Additionally, the Cybersecurity Coalition advocates for the use of ex-parte processes, where necessary, to fill in areas that are necessary but weren’t addressed in the regular APA rule-making process.

While this can be achieved within existing regulatory structures, it is easier to do so from the outside. The Cybersecurity Coalition has generally supported the ONCD as taking the lead on regulatory harmonization efforts up to this point. The Cybersecurity Coalition recommends that the committee review comments that were submitted to ONCD on this issue in 2023 that remain relevant today.¹⁷



¹⁷ Cybersecurity Coalition, Response to the Office of the National Cyber Director. *RE: Request for Information on Cybersecurity Regulatory Harmonization* https://cdn.prod.website-files.com/660ec3caef47b817df2800ae/660ec3caef47b817df28023f_Cybersecurity%20Coalition%20Comments%20to%20ONCD%20RFI%20on%20Cybersecurity%20Regulatory%20Harmonization%2020231031.pdf.