SURVEYING CIRCIA: SECTOR PERSPECTIVES ON THE NOTICE OF PROPOSED RULEMAKING

HEARING

BEFORE THE

SUBCOMMITTEE ON CYBERSECURITY AND INFRASTRUCTURE PROTECTION

OF THE

COMMITTEE ON HOMELAND SECURITY HOUSE OF REPRESENTATIVES

ONE HUNDRED EIGHTEENTH CONGRESS

SECOND SESSION

MAY 1, 2024

Serial No. 118–60

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

57–946 PDF WASHINGTON : 2025

COMMITTEE ON HOMELAND SECURITY

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

MICHAEL T. MCCAUL, Texas
CLAY HIGGINS, Louisiana
MICHAEL GUEST, Mississippi
DAN BISHOP, North Carolina
CARLOS A. GIMENEZ, Florida
AUGUST PFLUGER, Texas
ANDREW R. GARBARINO, New York
MARJORIE TAYLOR GREENE, Georgia
TONY GONZALES, Texas
NICK LALOTA, New York
MIKE EZELL, Mississippi
ANTHONY D'ESPOSITO, New York
LAUREL M. LEE, Florida
MORGAN LUTTRELL, Texas
DALE W. STRONG, Alabama
JOSH BRECHEEN, Oklahoma
ELIJAH CRANE, Arizona

BENNIE G. THOMPSON, Mississippi, *Ranking Member*
SHEILA JACKSON LEE, Texas
ERIC SWALWELL, California
J. LUIS CORREA, California
TROY A. CARTER, Louisiana
SHRI THANEDAR, Michigan
SETH MAGAZINER, Rhode Island
GLENN IVEY, Maryland
DANIEL S. GOLDMAN, New York
ROBERT GARCIA, California
DELIA C. RAMIREZ, Illinois
ROBERT MENENDEZ, New Jersey
THOMAS R. SUOZZI, New York
YVETTE D. CLARKE, New York

STEPHEN SIAO, *Staff Director*
HOPE GOINS, *Minority Staff Director*
SEAN CORCORAN, *Chief Clerk*

SUBCOMMITTEE ON CYBERSECURITY AND INFRASTRUCTURE PROTECTION

ANDREW R. GARBARINO, New York, *Chairman*

CARLOS A. GIMENEZ, Florida
MIKE EZELL, Mississippi
LAUREL M. LEE, Florida
MORGAN LUTTRELL, Texas
MARK E. GREEN, MD, Tennessee *(ex officio)*

ERIC SWALWELL, California, *Ranking Member*
SHEILA JACKSON LEE, Texas
TROY A. CARTER, Louisiana
ROBERT MENENDEZ, New Jersey
BENNIE G. THOMPSON, Mississippi *(ex officio)*

CARA MUMFORD, *Subcommittee Staff Director*
MOIRA BERGIN, *Minority Subcommittee Staff Director*

CONTENTS

SURVEYING CIRCIA: SECTOR PERSPECTIVES ON THE NOTICE OF PROPOSED RULEMAKING

Wednesday, May 1, 2024

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

The subcommittee met, pursuant to notice, at 2:05 p.m., in room 310, Cannon House Office building, Hon. Andrew R. Garbarino (Chairman of the subcommittee) presiding.

Present: Representatives Garbarino, Ezell, Lee, Green (ex officio), Swalwell, Menendez, and Clarke.

Mr. GARBARINO. The Committee on Homeland Security's Subcommittee on Cybersecurity and Infrastructure Protection will come to order.

The purpose of this hearing is to receive testimony from a panel of experts and industry leaders who provide their perspectives on CISA's Notice of Proposed Rulemaking relating to the implementation of the Cyber Incident Reporting for Critical Infrastructure Act of 2022, commonly referred to as CIRCIA.

I now recognize myself for an opening statement.

About 2 years ago, Congress woke up to gaps in cyber incident reporting. Public and private-sector entities have long complied with a patchwork of disparate niche cyber incident reporting requirements managed by an array of regulators.

As stated in the Notice of Proposed Rulemaking that we will discuss today, there are currently more than 3 dozen different Federal cyber incident reporting requirements in effect, 3 dozen.

In an age of increasingly sophisticated cyber attacks on our critical infrastructure, our fragmented approach to incident reporting has proven anything but nimble and useful. It is cumbersome and oftentimes redundant, creating a compliance burden on private-sector partners who could be spending their resources on security rather than fulfilling multiple reporting requirements. A confusing and reactive, rather than proactive, reporting regime increases the risk of the security of our homeland.

After significant national attacks on Colonial Pipeline and solar winds, Congress recognized an urgent need for better and more coordinated cyber incident reporting for our critical infrastructure. This included a need to develop a process for reporting ransom payments which didn't exist, despite the rise impact of ransomware attacks.

As a result, in March 2022, Congress passed the bipartisan Cyber Incident Reporting for Critical Infrastructure Act, or CIRCIA. This landmark legislation tasked the Cybersecurity and Infrastructure Security Agency to develop regulations to set the standard for cyber incident reporting across critical infrastructure sectors.

As the Nation's risk manager, CISA must be empowered to identify cross-sector points of vulnerability and share information to mitigate such risks. As the lifeline of our national security, economic security, and public health and safety, critical infrastructure entities must be supported as they adapt to a world where cyber attacks are not an "if" but a "when."

Since CIRCIA was signed into law, the American people have continued to feel the impacts of numerous costly intrusions into critical infrastructure sectors by cyber threat actors from the water sector to the health care sector. This cannot continue.

It is imperative that we get the CIRCIA rule right. CIRCIA should serve as the standard, not another regulation standing in the way of effective cyber defense. Because it is so important we get this right, I'm encouraged to hear that CISA is granting a 30-day extension for submitting comments.

Members of this subcommittee have eagerly awaited the draft rule that we are going to discuss in depth, especially considering conflicting rules such as the SEC's public cyber disclosure rule. Therefore, we are devoting this hearing to CIRCIA because we know this is an opportunity, one to ensure regulatory effectiveness and harmonization.

I want to thank our witnesses, Scott Aaronson from Edison Electric Institute, Heather Hogsett from Bank Policy Institute, Robert Mayer from the USTelecom, and Amit Elazari from OpenPolicy Group for being here today to help us understand how specific sectors will be impacted.

We cannot effectively implement CIRCIA without private-sector perspective. So thank you for your partnership.

Implementation of CIRCIA's more important than ever for our cyber preparedness. The final CIRCIA rule, expected late next year, will mark a pivotal turning point for America's ability to mitigate cyber risks and protect our national security, economy, and way of life.

I look forward to our witness' testimony and discussing how the proposed CIRCIA rule can ensure a more capable and ready national cyber defense.

[The statement of Chairman Garbarino follows:]

STATEMENT OF CHAIRMAN ANDREW R. GARBARINO

MAY 1, 2024

About 2 years ago, Congress woke up to the gaps in cyber incident reporting. Public and private-sector entities have long complied with a patchwork of disparate, niche cyber incident reporting requirements managed by an array of regulators. As stated in the Notice of Proposed Rulemaking that we will discuss today, there are currently more than 3 dozen different Federal cyber incident reporting requirements in effect.

In an age of increasingly sophisticated cyber attacks on our critical infrastructure, our fragmented approach to incident reporting has proven anything but nimble and useful. It is cumbersome and oftentimes redundant, creating a compliance burden

on private-sector partners who could be spending their resources on security rather than fulfilling multiple reporting requirements. A confusing and reactive, rather than proactive, reporting regime increases the risks to the security of our homeland.

After significant national attacks on Colonial Pipeline and SolarWinds, Congress recognized an urgent need for better and more coordinated cyber incident reporting for our critical infrastructure. This included a need to develop a process for reporting ransom payments, which didn't exist despite the rise and impact ransomware attacks.

As a result, in March 2022, Congress passed the bipartisan Cyber Incident Reporting for Critical Infrastructure Act, or CIRCIA. This landmark legislation tasked the Cybersecurity and Infrastructure Security Agency, or CISA, to develop regulations to set the standard for cyber incident reporting across critical infrastructure sectors. As the Nation's risk manager, CISA must be empowered to identify cross-sector points of vulnerability and share information to mitigate such risks. As the lifeline of our national security, economic security, and public health and safety, critical infrastructure entities must be supported as they adapt to a world where cyber attacks are not an "if" but a "when."

Since CIRCIA was signed into law, the American people have continued to feel the impacts of numerous costly intrusions into critical infrastructure sectors by cyber threat actors, from the water sector to the health care sector. This cannot continue.

It is imperative that we get the CIRCIA rule right. CIRCIA should serve as the standard, not another regulation standing in the way of effective cyber defense. Because it is so important we get this right, I'm encouraged to hear that CISA is granting a 30-day extension for submitting comments.

Members of this subcommittee have eagerly awaited the draft rule that we are going to discuss in depth, especially considering conflicting rules, such as the SEC's public cyber disclosure rule. Therefore, we are devoting this hearing to CIRCIA because we know this is an opportunity: one to ensure regulatory effectiveness and harmonization.

I want to thank our witnesses—Scott Aaronson from Edison Electric Institute, Heather Hogsett from the Bank Policy Institute, Robert Mayer from USTelecom, and Amit Elazari from OpenPolicy Group—for being here today to help us understand how specific sectors will be impacted. We cannot effectively implement CIRCIA without the private-sector perspective, so thank you for your partnership.

Implementation of CIRCIA is more important than ever for our cyber preparedness. The final CIRCIA rule, expected late next year, will mark a pivotal turning point for America's ability to mitigate cyber risks and protect our national security, economy, and way of life.

I look forward to our witnesses' testimony and discussing how the proposed CIRCIA rule can ensure a more capable and ready national cyber defense.

Mr. GARBARINO. I now recognize the Ranking Member, the gentleman from California, Mr. Swalwell, for his opening statement.

Mr. SWALWELL. I thank the Chairman for giving our subcommittee an opportunity to hear from the private sector on CISA's proposed cyber incident reporting rule which is the agency's, frankly, most significant undertaking since it was established.

I told the witnesses, before we began, you'll see a lot of fireworks in this room. You'll see both sides battle it out. But on this issue of cybersecurity, we are aligned. There's really no daylight between us on making sure that we give America's businesses and Government agencies the resources they need to defend against attacks from abroad and from within.

Before I begin, Chairman, if it's OK, I would like to just take a moment to acknowledge the passing of Congressman Donald Payne, Jr. Congressman Payne had an important impact on CISA, the agency we oversee. Because of his advocacy, CISA has a standing school security mission within the Infrastructure Security Division which works to make schools K–12 and universities safer and more secure.

Personally, Congressman Payne and I were both elected in the class of 2012. I sat next to him on this committee for all of my

going-on-12 years in Congress. He will be greatly missed by Members of this committee, as we send out our most sincere condolences to his family and constituents.

Turning to CIRCIA, CIRCIA was born out of crisis. A series of high-profile cyber incidents occurred in 2020 and 2021 like solar wind supply chain attack, the Kaseya compromise, and the Colonial Pipeline ransomware attack. They revealed unacceptable blind spots in the Federal Government's awareness of malicious cyber activity on U.S. networks.

The Federal Government was forced to rely on voluntary cyber incident reporting. So we will never know the full extent of who was impacted by the Solar Winds attack. Reporting from the Colonial Pipeline was initially delayed.

Incomplete information frustrates our ability to understand the motives and goals of our adversaries and delays information sharing, limiting our ability to prevent additional attacks.

Congress passed CIRCIA so CISA and its partners could detect and quickly disrupt malicious actors as soon as possible and identified the evolving tactics of our adversaries so that we could strategically reduce risk.

CIRCIA's success rests on getting this final rule right. I appreciate CISA's work to engage with the private sector early in the rulemaking process and to extend the comment period.

Moving forward, it's imperative that CISA strongly consider and incorporate feedback from the private sector, particularly as it refines key definitions including covered entity and covered cyber incident and the required components of cyber incident reports.

I also urge CISA to apply lessons learned from programs like Automated Indicator Sharing, also known as AIS. When Congress authorized AIS nearly a decade ago, we hoped it would achieve some of the same goals we have for CIRCIA today. But AIS never achieved its potential in part because it focused too often on quantity over quality.

New technology may enable CISA to draw insights from a higher volume of CIRCIA reports more quickly, particularly the advancements in AI. But I question whether it will be able to adequately overcome complications from the kind of overreporting that is likely to occur, given the breadth of current definitions.

Implementation of CIRCIA will be expensive for both the Government and private sector, and we must ensure that it yields real value. To just specify more plainly and frankly, we have to make sure that we don't wrap up nonrelevant small and medium-sized businesses in recording requirements that can both be cumbersome and expensive to the businesses and provide worthless data to CISA.

I understand, again, that CISA plans to grant an extension. We're pleased that they're doing so. I also share Chairman Garbarino's frustration with duplicative cyber incident reporting requirements, particularly with the SEC's unworkable rule and unrealistic rule.

Now that NPRM is public, I hope the Cyber Incident Reporting Council will redouble its efforts to promote harmonization and that my colleagues in Congress will refrain from passing additional redundant reporting requirements.

Again, I commend my colleagues, especially Ms. Clarke on this committee, and the witnesses here today for the work they're putting in to getting CIRCIA across the finish line. CIRCIA showed that improving the Nation's cybersecurity posture is a bipartisan goal and one that the private sector was willing to work with us to accomplish.

I hope we can continue to work together with the private sector and on this committee to do big things like passing important legislation that will improve how the Federal Government collaborates with the private sectors by authorizing the Joint Cyber Defense Collaborative, JCDC.

I'd also like to congratulate CISA on the publication of the NPRM. It's an important milestone and an enormous undertaking, and I look forward to working with CISA to clarify reporting requirements and to build out the analytical capacity necessary to derive actionable insights from CIRCIA reporting.

Again before I close, I'd like to ask unanimous consent that the Congresswoman from New York, Yvette Clarke, be permitted to participate in today's hearing.

Mr. GARBARINO. Agreed.

Mr. SWALWELL. Yield back.

[The statement of Ranking Member Swalwell follows:]

STATEMENT OF RANKING MEMBER ERIC SWALWELL

MAY 1, 2024

I would like to thank the Chairman for giving the subcommittee the opportunity to hear from the private sector on CISA's proposed cyber incident reporting rule—the agency's most significant undertaking since it was established. But before I begin, I would like to take a moment to acknowledge the passing of Congressman Donald Payne, Jr.

Although Congressman Payne did not sit on this subcommittee, he had an important impact on CISA, the agency we oversee. Because of Congressman Payne's advocacy, CISA has a standing school security mission within the Infrastructure Security Division, which works to make K–12 schools and universities safer and more secure. He will be greatly missed by Members of this committee, and we send our most sincere condolences to his family and constituents.

Turning to the subject of today's hearing: Implementation of the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA). CIRCIA was borne out of crisis. A series of high-profile cyber incidents in 2020 and 2021—like the SolarWinds supply chain attack, the Kaseya compromise, and the Colonial Pipeline ransomware attack—revealed unacceptable blind spots in the Federal Government's awareness of malicious cyber activity on U.S. networks. The Federal Government was forced to rely on voluntary cyber incident reporting, so we never knew the full extent of who was impacted by the SolarWinds attack, and reporting from Colonial Pipeline was initially delayed. Incomplete information frustrates our ability to understand the motives and goals of our adversaries and delays information sharing—limiting our ability to prevent additional attacks.

Congress passed CIRCIA so CISA and its partners could detect and disrupt malicious cyber campaigns sooner and identify the evolving tactics of our adversaries to more strategically reduce risk. CIRCIA's success rests on getting the final rule right. I appreciate CISA's work to engage with the private sector early in the rulemaking process through the Request for Information and for the thorough NPRM published earlier this month.

Moving forward, it is imperative that CISA strongly consider and incorporate feedback from the private sector, particularly as it refines key definitions—including "covered entity" and "covered cyber incident"—and the required components of cyber incident reports. I also urge CISA to apply lessons learned from programs like Automated Indicator Sharing (AIS).

When Congress authorized AIS nearly a decade ago, we hoped it would achieve some of the same goals we have for CIRCIA today. But AIS never achieved its potential, in part, because it focused on quantity over quality and produced too many

reports that lacked value. New technology may enable CISA to draw insights from a higher volume of CIRCIA reports more quickly, but I question whether it will be able to adequately overcome complications from the kind of overreporting that is likely to occur given the breadth of current definitions.

Implementation of CIRCIA will be expensive for both the Government and private sector, and we must ensure that it yields real security value. Toward that end, I understand many stakeholders, including some of our witnesses, have requested CISA extend the public comment period by 30 days. I understand that CISA plans to grant that extension and am pleased they are doing so. I also share Chairman Garbarino's frustration with duplicative cyber incident reporting requirements—particularly the SEC rule.

Now that the NPRM is public, I hope the Cyber Incident Reporting Council will redouble its efforts to promote harmonization and that my colleagues in Congress will refrain from passing additional redundant reporting requirements.

I commend my colleagues, especially Ms. Clarke, and the witnesses here today for the work they put into getting CIRCIA across the finish line. CIRCIA showed that improving the Nation's cybersecurity posture is a bipartisan goal, and one that the private sector was willing to work with us to accomplish.

Moving forward, I hope we can continue to work together to do big things, like passing important legislation that will improve how the Federal Government collaborates with its private-sectors partners by authorizing the Joint Cyber Defense Collaborative, JCDC.

I would also like to congratulate CISA on the publication of the NPRM—it is an important milestone in an enormous undertaking, and I look forward to working with CISA to clarify reporting requirements and to build out the analytical capacity necessary to derive actionable insights from CIRCIA reporting.

Mr. GARBARINO. I now—thank you, Ranking Member Swalwell.

I now recognize the Chairman of the full Committee on Homeland Security, Chairman Green, for an opening statement.

Mr. GREEN. Well, thank you to our witnesses for being here today and to give us your perspective and your expertise. It's deeply appreciated.

It's—you know, as we pass legislation, getting feedback on that legislation is always helpful and in future endeavors to pass laws that work, particularly as it relates to cyber and fighting against nation-states and criminals who use the cyber space for their advantages. So thank you for coming here and providing your thoughts.

I also want to thank Chairman Garbarino and the Ranking Member, Mr. Swalwell, for their bipartisanship. They do a great job in working together to advance not only legislation but oversight that shines light on some challenges that we have. I appreciate both of them and the way they work together.

I, too, want to say something about the tragic passing of Congressman Payne. You know, up here when you're—as Ranking Member Swalwell said, it sometimes gets contentious between the two sides as we vie for ideologies, quite frankly, that have less and less overlap over the years. But there are a few things that really overlap, cyber being one of them.

But in the case of Mr. Payne, you know, despite our differences, he was a friend. He longed for the unity and opportunity for when we can get together and work together on issues. I worked very closely with him on the Colorectal Cancer Caucus because he lost his father and I had, myself, colon cancer 8 years ago. So we worked very closely together on that.

To his family, I know you're going to miss him. We miss him. Our deepest condolences go out to you at this time.

You know, when we passed the act, our goal was to ensure shared visibility and, of course, substantial—all of the substantial

incidents impacting our homeland's critical infrastructure. With nation-state actors such as China and Russia continuing to target us, we knew that we needed a better understanding and to better understand and defend against increasingly fraught cyber threats. However, we knew we needed to do this without imposing undue regulatory burden on our companies that are already stretched very thin.

Duplicative efforts tend to wind up costing businesses money that they could actually use on real cybersecurity, and so getting to the bottom of those is one of our priorities. It's imperative that we strike the balance, of course, and ensure that the rule is harmonized with regulations.

I look forward to hearing from our witnesses today. Again, I want to thank you for being here and for being in this fight with us and for the future of the country.

Thank you.

[The statement of Chairman Green follows:]

STATEMENT OF CHAIRMAN MARK E. GREEN, MD

MAY 1, 2024

When we passed CIRCIA, our goal was to ensure shared visibility of substantial cyber incidents impacting our homeland's critical infrastructure.

With nation-state actors such as China and Russia continuing to target us, we knew that we needed to better understand and defend against increasingly fraught cyber threats. However, we knew we needed to do this without imposing undue regulatory burden on our companies that are already stretched very thin. Duplicative efforts tend to wind up costing businesses money that they could actually use on real cybersecurity, and so getting to the bottom of those is one of our priorities.

It is imperative that we strike this balance and ensure the rule is harmonized with regulations.

I look forward to hearing from our witnesses today.

Mr. GARBARINO. Thank you, Chairman Green.

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

[The statement of Ranking Member Thompson follows:]

STATEMENT OF RANKING MEMBER BENNIE G. THOMPSON

MAY 1, 2024

Four years ago, this committee began work on developing a mandatory cyber incident reporting framework to address the Federal Government's lack of visibility into the cyber incidents that impact all critical infrastructure sectors.

Last Congress, then-Subcommittee Chairwoman Clarke conducted an extensive process to introduce CIRCIA, consider and address stakeholder feedback, and ultimately negotiate the final enacted bill. Thanks to Congresswoman Clarke's leadership, a policy concept that cybersecurity experts had been suggesting for years finally became a reality.

In the 2 years since enactment, CISA has undertaken the significant work necessary to turn statutory text into a proposed rule. For an agency that generally relies on voluntary partnerships rather than regulation, that is no easy task, and I acknowledge the hard work by CISA staff to get this done.

In particular, I appreciate CISA's efforts to engage with stakeholders early and to draft a detailed rule that considers the input CISA received. This proposed rule, however, is only one step in the implementation process. Now, CISA must consider additional stakeholder feedback as it works to develop a Final Rule. I encourage CISA to ensure stakeholders have sufficient time to develop thoughtful comments on the many complicated issues that will need to be resolved. Getting this right will be essential to achieving the benefits Congress sought when enacting this legislation.

The goal of CIRCIA is to increase the Federal Government's visibility into the cybersecurity incidents impacting critical infrastructure, helping CISA improve its analysis of the cyber threats facing our Nation and ultimately develop better tools, products, and services to help strengthen our national cyber defenses. As we evaluate this proposed rule, we must consider how it helps further these goals while minimizing unnecessary burdens on the victims of cyber attacks. One key aspect of reducing the burden on critical infrastructure will not just be determined by the final CIRCIA Rule, but on the willingness of other Federal agencies to work with CISA to improve the harmonization of cyber incident reporting mandates.

As more Federal regulators have sought cyber incident information, many entities are currently subject to duplicative and inconsistent requirements, and it was this committee's expectation in passing CIRCIA that creating a mandatory reporting requirement across critical infrastructure would help relieve that regulatory burden, so entities can focus on preventing and responding to cyber intrusions.

I appreciate the work of the Cyber Incident Reporting Council to issue its initial report last year, which helped inform this proposed rule, and encourage the Council and all Federal agencies with current or proposed cyber incident reporting mandates to increase their engagement with CISA on regulatory harmonization now that the proposed rule has been released.

We also must ensure that CISA has the resources and tools necessary to turn incident reports into meaningful information that can be used to drive down cyber risk. I look forward to continuing to oversee CISA's plans for how to operationalize the large amounts of data the agency will receive and to work with our colleagues to provide CISA the necessary funding. CIRCIA is a demonstration of how this committee can enact significant national security legislation when we work together in a bipartisan way and engage in the hard work of considering stakeholder feedback and negotiating with our colleagues.

I hope this hearing today reminds us all of how important our work is and how productive we can be when we prioritize finding common ground. Our witnesses here today represent a range of critical infrastructure sectors and have worked with the committee on cyber incident reporting for years. Their feedback will be valuable as the committee continues its CIRCIA oversight, and I thank them for being here today.

Before I close, I would also like to take a moment to acknowledge the loss of a Member of the full committee, Congressman Donald Payne Jr., who got things done by working across the aisle and with stakeholders. I send the committee's condolences to his wife, Bea, and their triplets.

Mr. GARBARINO. I'm pleased to have a distinguished panel of witnesses before us today on this very important topic.

I ask that our witnesses please rise and raise their right hand.

[Witnesses sworn.]

Let the record reflect that the witnesses have answered in the affirmative.

Thank you. Please be seated.

I would now like to formally introduce our witnesses.

Mr. Scott Aronson currently serves as the senior vice president for security and preparedness 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 structure sectors that enhance security for the energy sector.

In addition to his role at EEI, Scott also serves as the secretary for the Electricity Subsector Coordinating Council, ESCC.

They also stole Emily from me on this committee, but that's OK. I will forgive you.

Ms. Heather Hogsett is the—yes—Ms. Heather Hogsett is the senior vice president for technology and risk strategy for B–I–T–S, BITS, the technology policy division of the Bank Policy Institute.

In this position, she develops and leads initiatives on emerging technology, security, and resilience matters facing the Nation's largest financial firms. Ms. Hogsett also chairs the Policy Com-

mittee of Financial Services Sector for Coordinating Council and is a board member of the FTD—FTLD Registry Services.

She's been a witness before and always gives me some great talking points. So I'm happy to have her back.

Mr. Robert Mayer is the senior vice president of cybersecurity with USTelecom Association. He's responsible for leading cyber and national security policy and strategic initiatives.

In addition to his role, he serves as chairman of the Communications Sector Coordinating Council which represents the broadcast, cable, satellite, wireless, and wireline industries in connection with DHS and public-private partnership activities across the U.S. Government. He also serves as co-chair to the Council to Secure the Digital Economy.

Ms. Amit Elazari is cofounder and CEO of OpenPolicy, the world's first policy intelligence and engagement technology platform providing government affairs value to entities of all sizes. She also teaches at the University of California, Berkeley School of Information, mass—Master in Information and Cybersecurity and serves as an advisor to the U.C. Berkeley Center of Long-Term Cybersecurity.

Prior to OpenPolicy, she served as head of cybersecurity policy for Intel Corp. where she was responsible for shaping and executing Intel's global security policy engagement across all of Intel's products and technologies.

I thank all 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, SECURITY AND PREPAREDNESS, EDISON ELECTRIC INSTITUTE

Mr. AARONSON. Thank you, Chairman Garbarino.

Before I get started, thank you for sharing Emily with us. Still fighting the good fight, just from a different address.

As Chairman Garbarino, Ranking Member Swalwell, Members of the subcommittee, thank you for the opportunity to testify today on cyber incident reporting requirements, specifically in the context of CISA's proposed rule pursuant to the Cyber Incident Reporting for Critical Infrastructure Act of 2022. I'm just going say CIRCIA.

My name is Scott Aaronson. I am senior vice president for security and preparedness at the Edison Electric Institute. EEI is the trade association that represents all of the Nation's investor-owned electric companies. These companies provide electricity to nearly 250 million Americans and operate in all 50 States and the District of Columbia.

EEI and its members appreciate Congress passing CIRCIA. Critical infrastructure security is a shared responsibility, and cyber incident report can go help Government and industry identify trends across sectors, leading to more effective policy making, information sharing, resource allocation, and mitigation strategies.

That said, details matter when it comes to how CIRCIA or any mandatory cyber incident reporting regime is implemented. Both my written testimony and comments today focus on three related themes that will help ensure cyber reporting requirements generate meaningful information without unnecessary compliance bur-

dens: First, the need to harmonize Federal mandates to ensure consistency and avoid duplication of efforts; second, the importance of leveraging sector risk management agencies, both as existing collectors of incident reports, as well as venues for effective information sharing and operational collaboration between industry and government; and, third, narrowing the scope of reporting requirements to truly impactful incidents so that we can separate signal from noise and glean meaningful insights that address real risks.

With respect to harmonization, as you are well aware, CIRCIA is being developed among an existing patchwork of Federal and State incident reporting requirements. While President Biden's National Cybersecurity Strategy highlighted the importance of harmonizing incident reporting, there are many definitions, time lines, and expectations for reporting across the Federal Government including new requirements from the Securities and Exchange Commission's cyber reporting rule. We hope CIRCIA does not create additional burdens.

Specifically we would like to see CISA referral existing reporting regimes from Federal counterparts to limit duplicative reporting through the substantially similar exception in CIRCIA, and we would like to see sector risk management agencies utilized as entry points for critical sectors rather than CISA trying to be all things to all sectors.

While CIRCIA is the first Federal cybersecurity requirement focused specifically on reporting across all critical sectors, the electricity subsector has been subject to similar reporting for years through NERC's CIP 008–6 and the DOE OE–417 form.

EEI appreciate your leadership, Chairman Garbarino, on this issue and is prepared to support future committee efforts to advance our shared harmonization goals.

In addition to harmonizing Federal mandates, we believe there are aspects of CISA's proposed rule that remain overly broad and may add extraordinary compliance burdens with little to no benefit. As I testified before you alongside the banking and telecommunication sectors representing some of the most sophisticated critical infrastructure operators, there's a real concern that even the most mature sectors will be overburdened by the proposed rule if it were finalized as is.

The committee should work with CISA to reduce the burden by focusing on a few areas for improvement. For example, the scope of substantial cyber incident definition will result in CISA receiving more reports than they are capable of triaging. CISA's estimate of 210,525 reports through 2033 seems extremely low. In fact, based on the current criteria, just one of EEI's larger members estimates at least 600 reports per month, which would be about 65,000 reports from a single electric company through 2033.

Ingesting, parsing, triaging, protecting, and synthesizing this data is a monumental task, not only for CISA but for the companies responsible for providing these reports. Coupled with the 2-year data preservation requirements, CIRCIA will be utilizing resources that instead could be used for actual security mitigation measures rather than compliance.

Instead, CISA should consider reviewing the type of information requested by NERC's CIP 008–6 and OE–417 to help guide the energy sector specific information required under CIRCIA.

Finally, protection of this information is paramount. CISA must ensure FOIA and Critical Electric Infrastructure Information, or CEII, protections for these reports. As the committee knows, no entity, public or private, is immune to cyber risk. A treasure trove of incident reporting data will be a prime target.

Mandatory incident reporting—report and volunteer information sharing both are valuable tools in ensuring the cybersecurity of critical infrastructure operators. EEI and its members are committed to working with both public and private partners across all sectors to comply with incident reporting requirements in a way that prioritizes and enhances critical infrastructure security.

We look forward to working with you and CISA to develop a rule that leverages existing regimes, provides meaningful insights to government and industry, and protects sensitive information.

CIRCIA is an important law with an important goal of identifying cyber risk across all sectors of the economy. We appreciate the committee's work to this point and your interest in making sure CISA gets it right.

I genuinely appreciate the opportunity to testify today, and I look forward to the questions.

[The prepared statement of Mr. Aaronson follows:]

PREPARED STATEMENT OF SCOTT I. AARONSON

MAY 1, 2024

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 security and preparedness at the Edison Electric Institute (EEI). EEI is the association that represents all U.S. investor-owned electric companies. 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. EEI's member companies invest more than $150 billion annually to make the energy grid stronger, smarter, cleaner, more dynamic, more flexible, and more secure against all hazards, including cyber threats. I appreciate your invitation to discuss this important topic on their behalf.

The energy grid powers our way of life and is critical to America's security and economic competitiveness. Today, demand for electricity is growing dramatically across the economy to support evolving customer needs, as well as critical technologies like artificial intelligence and the proliferation of data centers that connect our digital lives. Ensuring a secure, reliable, resilient energy grid is a responsibility that EEI's member companies and the electricity subsector take extremely seriously.

THREAT LANDSCAPE

For years, the U.S. intelligence community has warned of the potential for malicious nation-state exploitation of U.S. critical infrastructure. Today, we know from our Federal partners that People's Republic of China state-sponsored cyber actors known as Volt Typhoon have compromised multiple U.S. critical infrastructure providers with the intent of disrupting operational controls, including in the energy sector.[1] With the increasingly complex geopolitical threat landscape and the sophistica-

[1] *CISA and Partners Release Advisory on PRC-sponsored Volt Typhoon Activity and Supplemental Living Off the Land Guidance,* CISA.GOV, *https://www.cisa.gov/news-events/alerts/2024/02/07/cisa-and-partners-release-advisory-prc-sponsored-volt-typhoon-activity-and-supplemental-living-land* (February 7, 2024).

tion of ransomware operations by transnational organized criminals, we have seen an uptick in threats to critical infrastructure organizations across all sectors. These threats are a stark reminder of the need to continue to harden U.S. critical infrastructure.

Critical infrastructure security is a shared responsibility and a national imperative. While most critical infrastructure is owned by the private sector, Government at all levels can and must play a role in protecting it, especially when it comes to defending against nation-state actors. Cyber incident reporting may support Government efforts to protect U.S. critical infrastructure by creating visibility into cross-sector cyber risk, but reporting also should be supplemented with Federal support to mitigate risk and harden the critical infrastructure assets that are vital to national security.

HARMONIZATION OF FEDERAL CYBER INCIDENT REPORTING

EEI recognizes the committee's intent in passing the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) was to enhance and to standardize cyber incident reporting to improve the Federal Government's visibility into cyber threats and to allow the Government to share information quickly with critical infrastructure owners and operators across all 16 sectors. According to the Cyberspace Solarium Commission, prior to the passage of CIRCIA, the Federal Government lacked a mandate to collect cyber incident information reliably, systemically, and at the scale necessary to differentiate campaigns from isolated incidents and to support the development of more generalized conclusions.[2] However, it is important to note that the Cybersecurity and Infrastructure Security Agency's (CISA's) new cyber incident reporting requirements are being developed among an existing patchwork of Federal and State incident reporting requirements. Harmonization is paramount.

As part of CIRCIA's mandate, the Department of Homeland Security's (DHS's) Cyber Incident Reporting Council (CIRC) issued a report on harmonization of cyber incident reporting to the Federal Government. That report identified several key findings, including that there are currently 45 different Federal cyber incident reporting requirements administered by 22 Federal agencies.[3] Given this context, CISA should thoroughly explore opportunities with Federal counterparts to limit duplicative reporting through the "substantially similar" exception of CIRCIA. This exception includes "when a covered entity reports substantially similar information in a substantially similar time frame to another Federal agency pursuant to an existing law, regulation, or contract when a CIRCIA Agreement is in place between CISA and the other Federal agency."[4]

ELECTRICITY SUBSECTOR CYBER INCIDENT REPORTING

While the CIRCIA proposed regulations are the first Federal cybersecurity requirements focused specifically on reporting across all critical infrastructure sectors, the electricity subsector has been subject to similar reporting to other Federal entities for years, including through the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) Reliability Standards and the U.S. Department of Energy (DOE) Electric Emergency Incident and Disturbance Report OE–417 form. EEI appreciates CISA's commitment to working with DOE, the Federal Energy Regulatory Commission (FERC), and NERC to explore the applicability of the proposed rules' substantially similar reporting exception to enable entities subject to CIRCIA and either or both the CIP Reliability Standards or Form OE–417 requirements to be able to comply through the submission of a single report to the Federal Government.

Pursuant to the Federal Power Act and through FERC oversight, the electricity subsector is subject to NERC's CIP Reliability Standards that cover cyber and physical security requirements, including CIP–008–6: Cyber Security—Incident Reporting and Response Planning. Entities found in violation of CIP standards face penalties that can exceed $1 million per violation per day. These mandatory standards continue to evolve using the process created by Congress to allow for input from subject-matter experts across the industry and government.

---

[2] *Cyberspace Solarium Commission Report,* CYBERSOLARIUM.ORG, *https://cybersolarium.org/march-2020-csc-report/march-2020-csc-report/* (March 2020).

[3] *Harmonization 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).

[4] *Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements Proposed Rule,* GOVINFO.GOV, *https://www.govinfo.gov/content/pkg/FR-2024-04-04/pdf/2024-06526.pdf* (April 4, 2024). Accounting for and leveraging these existing incident reporting requirements should be a priority for CISA.

DOE's Office of Cybersecurity, Energy Security, and Emergency Response also requires certain energy sector entities to report certain cybersecurity incidents to DOE pursuant to 15 U.S.C. 772(b). As the energy sector's sector risk management agency (SRMA), DOE uses Form OE–417 to collect information from the electricity subsector relevant to DOE's overall national security and National Response Framework responsibilities.

In July 2023, the Securities and Exchange Commission (SEC) adopted rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies. In addition to cyber incident reporting through NERC, DOE, and the SEC, EEI member companies now also will be subject to CIRCIA's reporting requirements once implemented through CISA's final rule. EEI has expressed concerns with the public disclosure of a cyber incident through the SEC rules, especially before the incident is mitigated, and we value Chairman Garbarino's leadership on this issue. Public reporting provides details on vulnerabilities and attack vectors that may become a useful roadmap for malicious actors. This may make the entity, and others, a target for on-going or similar attacks.

The SEC, CISA, and all other Federal regulators must recognize the inherent sensitivity of and the need for protection of information regarding cybersecurity, including the risks associated with cybersecurity incident disclosure, and must allow reasonable flexibility regarding the governance of cybersecurity.[5] EEI appreciates the SEC's willingness to include a national security or public safety delay for disclosure, but more must be done to harmonize Federal reporting requirements and to limit disclosure of sensitive cyber incidents that may provide insights to adversaries. While the introduction of public reporting through the SEC rules following the passage of CIRCIA runs counter to the CIRC harmonization report's recommendations and the National Cybersecurity Strategy's intent, EEI remains committed to working with Government partners to streamline and to harmonize Federal cyber incident reporting.

In addition to these mandatory incident reporting requirements, the industry also uses voluntary cybersecurity standards, including the National Institute of Standards and Technology (NIST) Cybersecurity Framework, DOE's Cybersecurity Capability Maturity Model (C2M2), and, most recently, DOE's Cybersecurity Baselines for Electric Distribution Systems and Distributed Energy Resources (DER) that are being developed in partnership with State regulatory bodies through the National Association of Regulatory Utility Commissioners (NARUC).

Through these standards and voluntary regimes, the U.S. energy grid benefits from a baseline level of security. While these standards are important, regulations alone are insufficient given the dynamic threat environment, and they must be supplemented by industry-Government partnerships and coordinated response and recovery efforts. The electric power industry appreciated the chance to contribute to the drafting of the proposed rule through sector-specific listening sessions and through comments to CISA's request for information. The industry aims to continue this collaborative partnership to harmonize reporting requirements and to reduce the burden on covered entities in the energy sector.

AREAS FOR IMPROVEMENT IN THE PROPOSED RULE

This committee left the definitions of a covered entity, cyber incident, covered cyber incident, and substantial cyber incident up to the rulemaking process to allow for industry input on the definitions included in the proposed rule. The electric power sector is grateful for the chance to partner with CISA and DOE as our SRMA to focus the scope and scale of these definitions in a way that prioritizes both security and operational continuity, as well as transparency for the public, policy makers, and other sectors.

EEI joined several other critical infrastructure organizations in requesting an additional 30 days to analyze the lengthy proposal sufficiently, to determine the potential impacts to the energy sector, and to ensure harmonization between existing and other developing reporting requirements.[6] Additional time will allow our industry to develop thoughts on areas for improvement in the proposed rule. EEI is presently working closely with its member companies in this regard, but we preliminarily have identified the following opportunities for enhancement:

1. Scope of substantial cyber incident definition;

---

[5] *Edison Electric Institute Comments on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure,* SEC.GOV, *https://www.sec.gov/comments/s7-09-22/s70922-20128366-291140.pdf* (May 9, 2022).

[6] *Joint Trades Letter Requesting an Extension on CIRCIA Comments,* USCHAMBER.COM, *https://www.uschamber.com/security/cybersecurity/joint-trades-letter-requesting-an-extension-on-cisa-comments* (April 5, 2024).

2. Volume of information requested;
3. Workforce burden;
4. Data preservation requirements;
5. Protection of information.

1. Scope of Substantial Cyber Incident Definition

CISA is proposing to define the term "covered cyber incident" to mean a "substantial cyber incident." Under CIRCIA, covered entities would be required to report a substantial cyber incident, including "unauthorized access to a covered entities' information system or network, or any nonpublic information contained therein, that is facilitated through or caused by either a compromise of a cloud service provider, managed service provider, other third-party data hosting provider, or a supply chain compromise."[7] The inclusion of "any nonpublic information" and "third-party data hosting provider or a supply chain compromise" in this definition is very broad, which may result in CISA receiving far more incident reports than it is capable of triaging.

Unfortunately, the unauthorized access to any nonpublic information is a common occurrence in the United States. In 2023 alone, there were 3,205 known compromises, more than 1,400 public data breach notices, and more than 353 million total victims.[8] In addition, the exploitation of the MOVEit vulnerability in 2023 exemplified the impact a supply chain compromise can have. During this event, 102 entities were impacted directly, however, "1,271 organizations were indirectly affected when information stored in or accessed by a MOVEit product or service was compromised via a vendor."[9] Therefore, it may be more appropriate for CISA to require reports from third-party service providers who disclose non-public information, rather than require reports from the companies themselves that are the victims of the disclosure of non-public information. As CISA has championed in its Secure by Design initiative, the onus should be on the producers and developers of products, rather than on consumers and end-users.[10] EEI recommends that CISA consider scaling back this definition to cover only the most risky and impactful incidents. This also may help CISA prioritize resources and mitigations for those incidents that rise to a higher threshold.

2. Volume of Information Requested

The proposed rule estimates CISA will receive 210,525 CIRCIA reports through 2033, at a cost of $1.2 billion for the Government and $1.4 billion for industry. Given the total number and cost of reports expected, EEI recommends that CISA reconsider the volume of information it is requesting from covered entities.

As mentioned, the electricity subsector already is required to report cyber incidents through NERC, DOE, and the SEC. As the sector's statutorily designated Electric Reliability Organization and SRMA, respectively, NERC and DOE have the sector-specific expertise necessary to process the content of energy sector cyber incident reports. In contrast, a recent report by the U.S. Government Accountability Office found that CISA has insufficient staff with the requisite operational technology skills, including a lack of threat hunting and incident response expertise in the energy sector.[11] Both CISA and industry would benefit from the development and implementation of reporting requirements that would result in the production of a manageable amount of information for all affected parties. To this end, it may be advisable for CISA to consider reviewing the type of information requested by NERC CIP–008–6 and OE–417, respectively, to help it formulate reporting requirements that are not unduly burdensome for either CISA or industry but that comply with CIRCIA's information-reporting requirements.

EEI also has concerns with CISA's ability to obtain the resources necessary to triage the volume of information it proposes to request. The DHS fiscal year 2024

---

[7] *Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements Proposed Rule,* GOVINFO.GOV, *https://www.govinfo.gov/content/pkg/FR-2024-04-04/pdf/2024-06526.pdf* (April 4, 2024).

[8] *2023 Was the Worst Year Yet for Data Breaches in Every Way—Except One,* PCMAG.COM, *https://www.pcmag.com/articles/2023-was-the-worst-year-yet-for-data-breaches* (February 26, 2024).

[9] *2023 Data Breach Report,* IDTHEFTCENTER.ORG, *https://www.idtheftcenter.org/post/2023-annual-data-breach-report-reveals-record-number-of-compromises-72-percent-increase-over-previous-high/* (January 25, 2024).

[10] *Secure by Design,* CISA.GOV, *https://www.cisa.gov/securebydesign* (April 2024).

[11] *Cybersecurity Improvements Needed in Addressing Risks to Operational Technology,* GAO.GOV, *https://www.gao.gov/assets/d24106576.pdf* (March 2024).

budget request included $98 million[12] for CIRCIA for the staffing, processes, and technology necessary for successful implementation; however, the final fiscal year 2024 appropriations package included just $73.9 million, $23 million below the request.[13] Despite the $116 million requested for CIRCIA in fiscal year 2025, EEI remains concerned with CISA's ability to have the mechanisms in place to handle the information it is requesting from covered entities appropriately.[14]

3. Workforce Burden

As this subcommittee has explored, the national cybersecurity workforce shortage is a major challenge across all critical infrastructure sectors. With more than 448,000 cybersecurity job openings in the United States, the energy sector is no exception to this challenge.[15] The volume and content of the required CIRCIA reports will create a significant burden for the energy sector's cybersecurity workforce. EEI recommends CISA consider reducing this burden by prioritizing the implementation of interagency information-sharing agreements and by ensuring submission requirements are similar to the industry's submission requirements for NERC CIP–008 and OE–417. A 2018 DOE Multiyear Plan for Energy Sector Cybersecurity found that Federal incident reporting guidelines were driven by compliance more than process improvement and that coordination among reporting mechanisms could be valuable.[16] The need to focus on requirements that are outcome-based rather than compliance-based remains necessary to reduce the workforce burden of reporting multiple times to the Federal Government.

4. Data Preservation Requirements

The proposed rule requires that, regardless of whether a covered entity submits a CIRCIA Report or is eligible for an exception from reporting, it must preserve data and records related to the covered incident or ransom payment for no less than 2 years from the date of submission or the date the submission would have been required. The proposed rule estimates data preservation costs to total more than $306 million, which is the largest category of costs following the initial familiarization costs of implementation. EEI recommends that CISA consider reducing the proposed data-retention threshold to help ease costs and, instead, should allow those resources to be leveraged for security mitigation measures.

5. Protection of Information

The current cyber threat landscape proves that no entity, public or private, is immune to cyber risk. In fact, CISA itself recently identified a threat actor's exploitation of two of its key systems, the Infrastructure Protection Gateway and Chemical Security Assessment Tool.[17] Upon finalization and implementation of CISA's CIRCIA regulations, the cyber incident reporting information for all 16 critical infrastructure sectors will be in the possession of one Federal agency, CISA, thereby making it an extremely attractive, high-value target. Given this reality, it is imperative that any information entrusted to CISA be protected sufficiently from cyber threat actors.

CONCLUSION

Thank you again for holding this hearing. The electricity subsector and EEI's member companies are committed to advancing our strong cybersecurity posture and remain committed to working with both public and private partners across all sectors to comply with incident reporting requirements in a way that prioritizes and enhances critical infrastructure security. We appreciate the bipartisan support that cybersecurity legislation historically has enjoyed in this committee and the work that you have done to enhance the energy sector's cybersecurity posture. We look

---

[12] *Fiscal Year 2024 Budget in Brief,* DHS.GOV, *https://www.dhs.gov/sites/default/files/2023-03/DHS%20FY%202024%20BUDGET%20IN%20BRIEF%20%28BIB%29__Remediated.pdf* (April 2023).

[13] *Division C—Department of Homeland Security Appropriations Act, 2024,* HOUSE.GOV, *https://docs.house.gov/billsthisweek/20240318/Division%20C%20Homeland.pdf* (March 2024).

[14] *Fiscal Year 2025 Budget in Brief,* DHS.GOV, *https://www.dhs.gov/sites/default/files/2024-03/2024__0311__fy__2025__budget__in__brief.pdf* (April 2024).

[15] *Cybersecurity Supply/Demand Heat Map,* CYBERSEEK.ORG, *https://www.cyberseek.org/heatmap.html* (April 2024).

[16] *Multiyear Plan for Energy Sector Cybersecurity,* ENERGY.GOV, *https://www.energy.gov/ceser/articles/doe-multiyear-plan-energy-cybersecurity* (March 2018).

[17] Kapko, Matt, *CISA Attacked in Ivanti Vulnerabilities Exploit Rush,* CYBERSECURITYDIVE.COM, *https://www.cybersecuritydive.com/news/cisa-attacked-ivanti-cve-exploits/709893/* (March 11, 2024).

forward to working together to continue to bolster critical infrastructure security and resilience for 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, TECHNOLOGY AND RISK STRATEGY FOR BITS, BANK POLICY INSTITUTE

Ms. HOGSETT. Thank you.

Chairman Garborino, Ranking Member Swalwell, Chairman Green, honorable Members of the subcommittee, thank you for inviting me to testify.

I'm Heather Hogsett, senior vice president of technology and risk strategy for BITS, the technology division of the Bank Policy Institute, or BPI.

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

On behalf of BPI members, we greatly appreciate this committee's leadership and the opportunity to provide perspective on CISA's proposed rule to implement CIRCIA.

The financial industry has been a strong supporter of sharing cyber threat and incident information for more than two decades and has experienced the value it provides.

We were pleased to support CIRCIA as it was being considered by Congress because it sought to develop a uniform incident reporting standard across all major sectors of the economy and would provide CISA with information it needs to better understand cyber threats.

While we continue to believe that CIRCIA will play an important role in our collective defense against nation-state attacks and cyber criminals, we urge CISA to substantially revise the proposed rule in several areas to ensure its requirements are simple, directly support CISA's ability to have awareness of significant cyber incident and to quickly share useful information with industry, and to allow cyber personnel to focus on response and recovery, rather than Government reporting.

As currently drafted, this proposal will require extensive efforts by critical personnel during the most critical phase of an incident. When combined with a low threshold for reporting, this will add significant burden and compliance obligations.

As CISA and this committee move forward, we offer several recommendations. CISA should refine its broad interpretation of the CIRCIA statute including definitions and data requirements. The definition of substantial cyber incident should be revised to ensure a higher threshold for reporting and avoid overreporting of incidents that cause minimal harm or impact.

For instance, the requirement to report a disruption of a covered entity's ability to engage in business or industrial operations or deliver goods or services lacks an impact threshold and could lead to

a large number of immaterial or less significant incidents being reported.

CISA should also reduce the reporting requirements to those that support the goal of CIRCIA to quickly identify and assess risks across sectors and provide useful information to critical infrastructure entities to defend against attacks.

When CIRCIA was enacted, Congress was careful to note that legislation sought to strike a balance between getting information quickly and letting victims respond to an attack without imposing burdensome requirements. The proposed rule would disrupt that balance by requiring entities to share sweeping investigative findings and details that are typically not available until weeks or months after an incident.

For example, entities should not be required to report a time line of compromised system communications with other systems or an assessment of the effectiveness of response efforts.

CISA should also focus on building the capability to leverage reported information for actionable purposes. CISA should ensure it is adequately equipped to intake incident reports and has the capabilities and subject-matter expertise to provide timely and actionable information back out to industry, along with tools, to help minimize or avoid threats.

CISA should also clarify how it will protect this very sensitive information and how it will provide sector risk management agencies with information they need to fulfill their responsibilities and coordinate with entities in their respective sectors.

Finally, we encourage Congress to continue to focus on regulatory harmonization. While we have seen progress in coordination on cyber incident notification by the prudential banking regulators, other independent regulators such as the Securities and Exchange Commission and the Commodity Futures Trading Commission have continued to issue rules that duplicate or conflict with CIRCIA.

In particular, the SEC's cyber incident disclosure rule adds unnecessary complexity to incident response and undermines the purpose of CIRCIA by publicizing that a company has been attacked while CISA is still working to confidentially warn other potential victims and prevent further harm.

We encourage Congress to explore legislative solutions to better facilitate harmonization efforts as this may be the most effective forcing function to achieve increased streamlining moving forward.

In closing, we are committed to continuing to work with CISA and this committee to refine the proposed rule and ensure its successful implementation. If its requirements are balanced appropriately, CIRCIA will help reduce attacks and the disruption they cause to individuals, businesses, our economy, and our way of life.

Thank you for opportunity to speak today, and I'm happy to answer any questions.

[The prepared statement of Ms. Hogsett follows:]

PREPARED STATEMENT OF HEATHER HOGSETT

MAY 1, 2024

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 of technology and risk strategy for 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 and 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 feedback today on CISA's notice of proposed rulemaking to implement the Cyber Incident Reporting for Critical Infrastructure Act of 2022. We were pleased to support CIRCIA as it was being considered by Congress because it sought to develop a uniform incident reporting standard across all major sectors of the economy and would provide CISA with information it needs to better defend against attacks.

While we continue to believe that CIRCIA will play an important role in our collective defense against nation-state attacks and malicious criminals, we urge CISA to substantially revise the proposed rule in several key areas to ensure its requirements are simple and directly support CISA's ability to have better awareness of significant cyber incidents; to quickly provide useful information to critical infrastructure; and to allow cyber personnel to focus on response and recovery rather than Government reporting.

As currently drafted, this proposal will require extensive efforts by critical personnel during the most critical phase of an incident and includes expectations for on-going updates. When combined with a low threshold for reporting and other existing regulatory reporting requirements, this will add significant burden and compliance obligations.

BPI is working with our member companies and several other financial trade associations to provide a detailed response that I will be happy to share with this committee once it is complete. In the interim, I would highlight that we believe CISA took an overly broad approach and expanded certain areas well beyond the statute. We offer the following concerns and recommendations:

(1) CISA should refine its broad interpretation of the CIRCIA statute. CISA should apply a higher threshold for incidents that must be reported to better focus on significant cyber threats. It should also reduce the reporting elements to those that support CIRCIA's goal to quickly identify and assess risks across sectors and disseminate early alerts and mitigation measures where possible.

(2) CISA should focus on building the capability to leverage reported information for actionable purposes. CISA should ensure it is adequately equipped to intake incident reports and has the capabilities and subject-matter expertise to provide timely and actionable information back out to industry along with tools to help minimize or avoid threats. CISA should also clarify how it will protect this information and provide Sector Risk Management Agencies with information they need to fulfill their responsibilities and coordinate with entities in their sector.

(3) Congress should continue to focus on regulatory harmonization. While we have seen progress in coordination on cyber incident notification by the prudential banking regulators, other independent regulators continue to issue rules that duplicate or conflict with CIRCIA. In particular, the SEC's cyber incident disclosure rule adds unnecessary complexity to incident response and undermines the purpose of CIRCIA by publicizing that a company has been attacked while CISA is still working to warn other potential victims and prevent further harm.

CYBER INCIDENT INFORMATION SHARING IN THE FINANCIAL SECTOR

Financial institutions are often targeted by hostile nation-state cyber actors and criminal organizations seeking to disrupt the financial system and overall functioning of the U.S. economy. As a critical infrastructure sector, the financial services industry has acknowledged the severity of these risks and invested significant resources over more than 2 decades to enhance or otherwise support cyber information-sharing efforts and incident response coordination.

The formation of the FSSCC and Financial Services Information Sharing and Analysis Center were both key elements in these efforts. The FSSCC strengthens

the resiliency of the financial services sector by proactively identifying cyber threats, driving preparedness and coordinating crisis response.[1] The FS–ISAC shares cyber threat information and best practices with roughly 5,000 members in 70 different countries.[2] Each organization strengthens public-private cooperation through trusted, confidential forums that enable detailed information sharing and serve as a model other critical infrastructure sectors have sought to emulate.

In addition to these 2 settings, BPI members supported regulatory efforts to ensure timely awareness of significant cybersecurity threats facing financial institutions or critical infrastructure more broadly. The prudential banking regulators' Computer-Security Incident Notification Rule[3] is an example of this. That rule allows institutions that have suffered a potentially significant incident to satisfy their compliance obligations by notifying their primary regulator—either the Federal Reserve Board, the Office of the Comptroller of the Currency or the Federal Deposit Insurance Corporation—via a simple email or telephone call within 36 hours. This requirement balances regulators' need for early awareness of significant cyber threats without diverting critical resources at affected entities who need to effectively respond.

BPI members were also broadly supportive of CIRCIA while it was being negotiated in Congress and leading up to its enactment in March 2022.[4] As a regularly-targeted critical infrastructure sector, we shared policy makers' view that the proliferation of cyber incidents represents a critical economic and national security threat. To that end, banks and other financial institutions believed CIRCIA was a unique opportunity to expand visibility, awareness, and coordinated sharing of incident information across all critical infrastructure sectors to combat sophisticated and persistent cyber threats.

FINANCIAL SERVICES REGULATORY LANDSCAPE

For CIRCIA to be effective, however, it is important that CISA acknowledges existing regulatory requirements and harmonizes those with CIRCIA wherever possible. As the Cyber Incident Reporting Council's report commissioned by CIRCIA identified, there are 8 distinct cyber incident reporting requirements applicable to the financial sector alone.[5] Financial institutions are also subject to rigorous supervision and examinations to determine whether they operate in a safe and sound manner. This includes on-site examiners evaluating compliance with relevant statutory requirements and whether firms implement appropriate security controls, including third-party risk management, operational risk and resiliency programs, and oversight by the board of directors.

The recent adoption of the SEC's public company disclosure[6] rule adds to this already complex regulatory landscape. As BPI and many industry stakeholders have pointed out,[7] the SEC's rule conflicts with the primary purpose of confidential reporting requirements like CIRCIA, creates confusion and diverts resources from critical response and recovery activities. Requiring public disclosure—particularly of ongoing incidents—puts sensitive information into the hands of hostile threat actors while shortening the time frame agencies like CISA will have to warn other potential victims. In the first few months since the rule went into effect, we've seen mali-

---

[1] *About FSSCC,* FSSCC, *https://fsscc.org/about-fsscc/*.

[2] *Who we are,* FS–ISAC, *https://www.fsisac.com/who-we-are.*

[3] Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers, 86 Fed. Reg. 66424 (Nov. 23, 2021).

[4] Press Release, Bank Policy Institute, President Signs Omnibus, Includes BPI-Supported LIBOR and Cyber Incident Reporting Solutions (Mar. 15, 2022), *https://bpi.com/president-signs-omnibus-includes-bpi-supported-libor-and-cyber-incident-reporting-solutions/;* Press Release, Bank Policy Institute, Incident Reporting Law Moves Toward Finish Line as Senate Seeks to Advance Sensible Solution (Oct. 6, 2021), *https://bpi.com/incident-reporting-law-moves-toward-finish-line-as-senate-seeks-to-advance-sensible-solution/*.

[5] DEP'T OF HOMELAND SEC., HARMONIZATION OF CYBER INCIDENT REPORTING TO THE FEDERAL GOVERNMENT 9 (2023).

[6] Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, 88 Fed. Reg. 51896, 51944 (Aug. 4, 2023).

[7] Press Release, Bank Policy Institute, SEC Rule on Cyber Disclosure Risks Harming Investors, Exacerbates Security Risks (Jul. 26, 2023), *https://bpi.com/sec-rule-on-cyber-disclosure-risks-harming-investors-exacerbates-security-risks/;* Heather Hogsett, *Fool's Gold: Why the Exceptions to the SEC's Cyber Disclosure Rule Cannot and Will Not Work, and the Damage that Will Ensue,* BANK POLICY INST. (Dec. 18, 2023), *https://bpi.com/fools-gold-why-the-exceptions-to-the-secs-cyber-disclosure-rule-cannot-and-will-not-work-and-the-damage-that-will-ensue/*.

cious actors even turn the disclosure requirement into an additional extortion method used against victim companies.[8]

IMPLEMENTING CIRCIA

Successful implementation of CIRCIA will provide several important benefits to our national cyber defense. If calibrated and implemented appropriately, CIRCIA will provide CISA with more information from across critical infrastructure sectors to enhance its analysis and assessment of emerging cyber threats. This in turn will improve the quality of the alerts and security services offered by CISA and other government partners and provide earlier warning to potentially affected companies so they can better protect themselves.

CIRCIA will also provide greater insight into the threats facing third parties and other service providers. Like financial institutions, threat actors have frequently targeted these entities in recent years and the proposed rule acknowledges how the compromise of a third-party service provider can "cause significant cascading impacts to tens, hundreds, or even thousands of other entities." Consistent incident reporting from those entities will provide CISA with a more complete picture of the cyber threat landscape and will also help third-party providers enhance their own incident management processes.

Benefits notwithstanding, implementing CIRCIA will be a challenge. As noted in the CIRC Report, there are 45 in-effect reporting requirements administered by 22 Federal agencies—many of which have different definitions and thresholds for reporting.[9] Rather than implementing the CIRC report's recommendation to adopt a more uniform definition and threshold for a reportable cyber incident, CISA's proposed substantial cyber incident definition adds another broad term with a reporting threshold well below many other existing requirements. Streamlining those requirements is no trivial task given the divergent missions and authorities of those Federal agencies—however, CISA's narrow interpretation of the "substantially similar" exemption under CIRCIA will render it unusable. As a result, entities will likely have to continue to simultaneously assess compliance with multiple notification, reporting, and disclosure obligations.

There is also the challenge of getting some independent regulatory agencies to engage and support broader harmonization efforts. For example, the SEC first proposed its public company disclosure rule just 8 days after the Senate passed CIRCIA. Since then, the SEC rule has created uncertainties around what cyber threat and incident information can be shared between private-sector entities and has been used as an additional extortion method by ransomware criminals—all for the attenuated benefit of informing investor decision making. This past January, the Commodity Futures Trading Commission also proposed a new rule on operational resilience that would require reporting of cyber incidents within 24 hours.[10]

CISA's 447-page NPRM is in many ways a reflection of how challenging it is to bring coherence to the fragmented cyber regulatory landscape. Articulating a definition for covered entity across 16 critical infrastructure sectors is not a straightforward exercise. At the same time though, the required data elements CISA proposes for CIRCIA reporting are expansive and, in several instances, well beyond what was contemplated by the underlying statute. For example, the rule proposes to require firms to report detailed investigative findings such as the "time line of compromised system communications with other systems"[11] as well as "a description of any unauthorized access, regardless of whether the covered cyber incident involved an attributed or unattributed cyber intrusion, identification of any informational impacts or information compromise, and any network location where activity was observed."[12] The NPRM also proposes that reports include the "direct economic impacts to operations"[13] and even an "assessment of the effectiveness of response efforts in mitigating and responding to the covered cyber incident."[14] These requirements are broader than those contained in the CIRCIA statute and, as discussed

---

[8] *Ransomware gangs are now reporting to the SEC, says CrowdStrike CEO,* CNBC (Dec. 21, 2023), *https://www.cnbc.com/video/2023/12/21/ransomware-gangs-are-now-reporting-to-the-sec-says-crowdstrike-ceo.html.*

[9] Id. at 4–5.

[10] Operational Resilience Framework for Futures Commission Merchants, Swap Dealers, and Major Swap Participants, 89 Fed. Reg. 4,709, 4758–59 (Jan. 24, 2024).

[11] CIRCIA NPRM § 226.8(a)(3)(iv).

[12] Id. at § 226.8(a)(2).

[13] Id. at § 226.8(a)(4).

[14] Id. at § 226.8(a)(4)(i)(2).

above, will make it difficult if not impossible to leverage a report provided to another Federal agency under the "substantially similar" reporting exemption.

Given the breadth and detail of the proposed reporting elements—several of which are typically unknown prior to the 72-hour reporting deadline—CIRCIA's supplemental reporting requirements would likewise become more burdensome than Congress intended. Because CISA interprets "substantial new or different information" as anything responsive to a required data field in a CIRCIA report, it is likely that an impacted entity will have to provide numerous supplemental reports during a single incident response. If not balanced appropriately, outsized compliance demands can create operational risks by consuming the time of front-line cyber personnel on reporting requirements instead of on network and enterprise security operations.

The proposed data elements are also relevant for another important aspect of CIRCIA's implementation—CISA's capability to intake reported information and provide timely and useful alerts back out to potentially impacted entities. This includes providing clarity for how CISA will share reported information with Sector Risk Management Agencies and other law enforcement partners. Equally important will be how CISA protects this very sensitive information once submitted as it will quickly become a target for attackers and could put covered entities at risk if breached. In the final rule, CISA should carefully calibrate the information required in CIRCIA reports with its own ability to leverage that information in furtherance of some actionable purpose. As currently constructed, the proposed rule requires information beyond CISA's direct statutory mandate and above what is necessary "to enhance situational awareness of cyber threats across critical infrastructure sectors."1515 6 U.S.C. § 681a(a).

RECOMMENDATIONS

As noted above, BPI is working on a comprehensive response to the CIRCIA NPRM. Based on our discussions with banks and other financial institutions thus far, we offer 3 recommendations for CISA and the committee's consideration:

(1) CISA should refine its broad interpretation of the CIRCIA statute.—CISA should revise the definition of "substantial cyber incident" to ensure a higher threshold for reporting and avoid over-reporting of incidents that cause minimal harm or impact. For instance, the requirement to report a "disruption of a covered entity's ability to engage in business or industrial operations, or deliver goods or services" lacks an impact threshold and could lead to a large number of immaterial or less significant incidents being reported. The CIRCIA statute had additional language for this prong referencing disruptions to business or industrial operations "including due to a denial of service attack, ransomware attack, or exploitation of a zero day vulnerability."[16] While Congress may not have intended to limit this threshold exclusively to those 3 scenarios, it does indicate a specific operational disruption much narrower than the one outlined in the proposed rule.

CISA should also reduce the reporting requirements to information that supports CIRCIA's goal to allow CISA to quickly identify and assess risks across sectors and provide early alerts and mitigation measures where possible. Covered entities should not be required to share sweeping investigative findings or details that are often not available until weeks or months after an incident.

In its proposed rule, CISA interprets the CIRCIA statute well beyond Congress's intent that CIRCIA promote "shared awareness of the cyber threats across the public and private sectors"[17] and not become a large-scale data collection exercise. For example, CISA acknowledges that the data elements proposed for CIRCIA reports exceed those specified by Congress in the statute. In fact, CISA's proposal outlines a level of granularity never seen before in incident reporting regimes and will make harmonizing cyber incident reports across Federal agencies even more challenging.

To fulfill its goal of better awareness of cyber threats across critical infrastructure sectors, Congress recognized CISA would need to be notified of substantial incidents within a relatively short time frame—hence the 72-hour reporting requirement. Nevertheless, when CIRCIA was enacted, Congress was careful to note the legislation sought to strike "a balance between getting information quickly and letting victims respond to an attack without imposing burdensome

[16] 6 U.S.C. § 681b(c)(2)(ii).

[17] S. REP. NO. 117–249, at 2 (2022), *https://www.Congress.gov/117/crpt/srpt249/CRPT-117srpt249.pdf.*

requirements."[18] CISA's proposed rule would disrupt that balance by requiring information that is often unknown within 72 hours and as a result significantly increasing supplemental reporting demands.

(2) CISA should focus on building the capability to leverage reported information for actionable purposes.—CISA estimates that over 316,000 companies will be considered covered entities under the final rule. When combined with the breadth of the proposed substantial cyber incident definition, CISA is likely to receive far more than the 15,000 annual incident reports it now anticipates. If CISA is to preserve its productive and collaborative relationship with the private sector, it is critical to assemble the necessary infrastructure, staff, and communication channels to analyze and disseminate actionable cyber threat information to potentially impacted entities.

It is also vital that CISA clearly articulate a process that will allow SRMAs, including the U.S. Treasury Department, to quickly be notified of an incident and to access information the SRMA may need to coordinate response efforts within their respective sectors. The financial services sector has a strong and collaborative relationship with Treasury that includes incident response playbooks and a communication plan. Both of these include coordination with regulators and interconnect with other national response mechanisms. The sector has experienced several ransomware attacks in the last year that impacted the sector to varying degrees. In each instance, Treasury played a vital role in the early stages by working with firms and regulators to assess impacts and potential downstream effects. Critical in this coordination is Treasury's ability to quickly access incident information while avoiding the need for various Government agencies to contact the affected entity. CISA should clarify how this process will work once CIRCIA reporting is in place and how it will preserve and support the role of SRMAs.

(3) Congress should continue to focus on regulatory harmonization.—With CIRCIA, Congress took an important step toward establishing a harmonized cyber incident reporting standard across critical infrastructure. In 2023, the Biden administration similarly identified harmonizing and streamlining existing regulation as a strategic priority in its National Cybersecurity Strategy,[19] and the CIRC issued its report on harmonization with several recommendations for Congressional action.[20]

Despite these efforts, independent regulators like the SEC and CFTC continue to offer their own disparate standards for incident reporting which will contribute to growing burnout and attrition among key cybersecurity personnel. According to a recent survey of large financial institutions, Chief Information Security Officers report spending between 30 to upwards of 50 percent of their time on regulatory compliance, with several firms noting that their security teams spend more than 70 percent of their time on compliance activities. As regulations continue to expand in number and scope, cybersecurity teams will have less time to adjust to rapid technological change. This presents considerable operational risk—particularly as hostile actors move to weaponize emerging technologies like artificial intelligence and quantum computing.

With that being the case, we encourage Congress to explore legislative solutions to further harmonization efforts. The CIRC report's recommendation that Congress remove any barriers to harmonization and drive adoption of model definitions, time lines, and thresholds for cyber incident reporting[21] could be beneficial if applied across all Federal agencies to include independent regulatory agencies. It is vital that Congress make clear to regulators that they must recognize existing Federal requirements and leverage the CIRCIA reports, rather than continue to issue new incident reporting requirements. This may be the most effective forcing function to achieve increased streamlining moving forward.

---

[18] Press Release, U.S. Sen. Homeland Sec. Comm., Peters & Portman Landmark Provision Requiring Critical Infrastructure to Report Cyber-Attacks Signed into Law as Part of the Funding Bill (Mar. 15, 2022), *https://www.hsgac.senate.gov/media/dems/peters-and-portman-landmark-provision-requiring-critical-infrastructure-to-report-cyber-attacks-signed-into-law-as-part-of-funding-bill/*.

[19] WHITE HOUSE, NATIONAL CYBERSECURITY STRATEGY 1, 9 (2023), *https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf*.

[20] DEP'T OF HOMELAND SEC., HARMONIZATION OF CYBER INCIDENT REPORTING TO THE FEDERAL GOVERNMENT 34 (2023).

[21] Id.

CONCLUSION

The financial services sector has long supported the early and confidential sharing of cyber threat and incident information. Early awareness of threats helps firms respond and calibrate additional security measures that can prevent malicious activity or minimize its impact. CIRCIA represents an important step toward expanding this type of awareness and information sharing across all critical infrastructure sectors. If its requirements are appropriately balanced, CIRCIA will help reduce attacks and the disruption they cause to individuals, businesses, our economy, and our way of life.

It is imperative that we work together to ensure the final reporting requirements of CIRCIA balance CISA's needs for early incident information while not disrupting critical incident response and remediation activities. As currently drafted, CIRCIA would add significant requirements to an already challenging and complex set of Government reporting requirements. It will also overwhelm CISA with information that is not needed or useful to fulfill the goals of better situational awareness and timely information sharing with critical infrastructure.

We are committed to continuing to work with CISA and this committee to refine the proposed rule and ensure its successful implementation.

Mr. GARBARINO. Thank you, Ms. Hogsett.

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

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

Mr. MAYER. Chairman Garbarino, Ranking Member Swalwell, honorable Members of the subcommittee, thank you for convening this hearing on implementation of the CISA Cyber Incident Reporting for Critical Infrastructure Act, CIRCIA, perhaps the most important of the foundational cybersecurity-related statutes Congress has passed.

My name is Robert Mayer. I'm senior vice president of cybersecurity and innovation at USTelecom. Our members include broadband providers, suppliers, and technology innovators, all providing advanced and secure communication services to markets urban and rural and everywhere in between.

In addition to my role at USTelecom, I serve as the chair of the Communications Sector Coordinating Council and co-chair of the DHS ICT Supply Chain Risk Management Task Force, the two principal organizations that serve as the Government's industry partners for developing cybersecurity and supply chain security policies.

Thank you for holding this hearing today. It is absolutely crucial to our national security that CISA critical infrastructure entities and other Government agencies work collaboratively with this subcommittee to implement Congress' vision for this law.

Our members have a long history of successful collaboration with U.S. Government partners, dating back the Cuban Missile Crisis when the U.S. Government formed a critical alliance with the telecommunications industry to ensure its survival in the event of a nuclear attack. That collaboration continues today as USTelecom works regularly with Government partners like NIST, CISA, the intelligence community, DOD, and other valued partners.

Unfortunately, parts of our Government risk undermining this collaboration as we increasingly see a regulatory mindset focused on prescriptive compliance rather than dynamic teamwork. This manifested last week in the FCC's misguided order that will im-

pose 20th-Century utility-based prescriptive regulations on internet service providers including in the realm of cybersecurity where other agencies such as CISA are the ones with the appropriate expertise.

To be clear, CIRCIA implementation is an enormous task. CISA estimates that 300,000 entities will be covered by its requirements and it will take years of multiple iterative exchanges between Government and critical infrastructure entities to fully mature.

There are several areas in particular that we believe need our collective attention. For one, we need clarity on the terms and definitions in the rule. The proposed scope of covered entities and covered cyber incidents are expansive and currently lack key guidance that cybersecurity practitioners and the attorneys will need.

Without more precise definitions and clear reporting thresholds, overreporting will occur and could overwhelm Government resources and undermine the effectiveness of CIRCIA. We should avoid unproductive and disproportionate focus on routine events in favor of reporting cyber incidents that pertain directly to CISA's mission.

Moreover, it is imperative for our Government partners to recognize the substantial cyber resources that will be allocated to assess whether an event meets the reporting criteria and fulfill the expansive set of reporting requirements.

It's also important to underscore that CIRCIA partnership implies reciprocity. To fulfill CIRCIA's purpose, CISA needs to establish mechanisms of rapidly disseminating valuable defensive advisories to critical infrastructure entities while also supporting victims as they respond to highly debilitating attacks.

It is also vital that we achieve harmonization and efficiency in reporting. Our members from the smallest to the largest have expressed concern about the substantial resources they will need to dedicate to complying with a rapidly growing patchwork of incident reporting requirements.

Our ask from the Federal Government partners is this. Providers need to be able to submit reports through a single agency. It will be essential to streamline the contents of reports as much as possible, by developing a common format, while allowing a variety of flexible reporting mechanisms that could ideally be tailored to the unique needs of organizations.

Finally, we call on CISA to establish ex parte communications for the CIRCIA rulemaking. This is a critical step in the spirit of collaboration toward ensuring a robust framework that reflects the intricate realities of cybersecurity and critical infrastructure sectors.

Agency adoption of a transparent and open process akin to that employed by other Government agencies will facilitate continuous and meaningful input from industry stakeholders whose expertise and first-hand experience are invaluable for crafting policies that are not only effective but also practical.

Deep and persistent collaboration is the key to achieving Congressional intent in implementing CIRCIA. USTelecom and its members will continue to work closely with CISA through the Comm Sector Coordinating Council and other fora and by actively participating in the CIRCIA rulemaking process. We look forward

to continued successful collaborations to combat the ever-evolving cyber threats we face.

I look forward to your questions.

Mr. GARBARINO. Thank——

Mr. MAYER. Thank you.

[The prepared statement of Mr. Mayer follows:]

PREPARED STATEMENT OF ROBERT MAYER

MAY 1, 2024

Chairman Andrew Garbarino, Ranking Member Eric Swalwell, Members of the subcommittee, thank you for convening this hearing on implementation of the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA), perhaps the most important of the foundational cybersecurity-related statutes Congress has passed. My name is Robert Mayer, and I am the senior vice president, cybersecurity and innovation at USTelecom and serve as the chair of the Communications Sector Coordinating Council and co-chair of the DHS ICT Supply Chain Risk Management Task Force.

It is absolutely crucial to our national security that CISA, critical infrastructure entities, and other Government agencies work collaboratively to implement Congress's vision for this law—to deepen and operationalize the partnership between Government and industry that is indispensable to our defense against cyber threats.

As this subcommittee is well aware, the United States' adversaries—China, Russia, Iran, North Korea—are increasingly becoming an aggressive military alliance, and those governments and their criminal proxies have extremely sophisticated cyber capabilities. We need close and well-coordinated teamwork between Government and industry to ensure our defense.

CIRCIA can be a profoundly powerful tool in deepening this collaboration and teamwork, and I implore the subcommittee to push this principle relentlessly in the years to come.

Unfortunately, parts of our Government risk undermining this principle, as we increasingly see a rigid regulatory mindset focused on prescriptive compliance rather than dynamic teamwork. This manifested last week in the FCC's misguided order that will impose 20th Century utility-based prescriptive regulations on Internet Service Providers—including even in the realm of cybersecurity—which are investing billions of dollars to innovate for the 21st Century.

As the most dynamic and innovative nation in history, we need to recognize that our defense against these threats requires us to deepen our collaboration. We need to double down on, not undermine, the Government-industry partnership. At this very moment, and literally every moment, experts in Government and private industry are working shoulder to shoulder to outwit and outpace highly-organized efforts to infiltrate our Nation's critical infrastructure. That is the only approach that will work.

Thankfully, the launch of CIRCIA can help get this right, because CIRCIA—if properly implemented—is fundamentally about collaboration and holistic situational awareness. Now, it is incumbent on Government and industry partners to roll up our sleeves and collectively begin the work of translating Congress's directions into operational reality.

To be clear, CIRCIA implementation is an enormous task—CISA estimates that 300,000 entities will be covered by its requirements—and it will take years and multiple iterative exchanges between Government and critical infrastructure entities to fully mature. Here again, the more collaboration and partnership we practice, the more we can develop mutual understanding and expectations of what is needed and how to achieve it.

There are several areas in particular that we believe need our collective attention.

For one, we need clarity on the terms and definitions in the rule. Without sufficient specificity, this is difficult to accomplish. The proposed scope of "covered entities" and "covered cyber incident" are expansive and currently lack key guidance that cybersecurity practitioners will need, as they seek to provide CISA with information that is responsive to the agency's mission.

Moreover, it is imperative for our Government partners to recognize the substantial cyber resources that will be allocated to assess whether an event meets the reporting criteria. The industry requires more precise definitions and clear reporting thresholds. Without these, there is a real risk that, in an effort to comply with the law, the industry will report numerous events that could easily overwhelm CISA's

capacity to act on the information. Such overreporting could unnecessarily burden Government resources and undermine the effectiveness of CIRCIA. It is crucial to establish definitions that are not excessively broad, as overly inclusive terms could divert essential resources away from cyber defense and toward regulatory compliance for its own sake.

Critically, we believe that covered cyber incidents should only be those pertaining directly to the mission of CISA and avoid unproductive and disproportionate focus on routine events.

It is also important to underscore that partnership implies reciprocity. To fulfill CIRCIA's purpose, CISA needs to establish mechanisms of rapidly disseminating valuable defensive advisories to critical infrastructure entities while also supporting victims as they respond to highly debilitating attacks.

The estimated cost to industry of these new requirements is $1.4 billion over 11 years, and it is estimated the Federal Government will incur costs of $1.2 billion over the same time frame. Collectively, our Nation needs a return on this investment and for the law to achieve its aims. We will work with CISA to ensure that meaningful incident reports lead to broader situational awareness and to increased operational preparedness and response capabilities.

It is also vital that we achieve harmonization and efficiency in reporting. Our members, from the smallest to the largest, have expressed concern about the substantial resources they will need to dedicate to complying with a rapidly-growing patchwork of incident reporting requirements. Our ask from Federal Government partners is this: Providers need to be able to submit reports to a single agency. It will be essential to streamline the contents of reports as much as possible—by developing a common format—while allowing a variety of flexible reporting mechanisms that could ideally be tailored to the unique needs of organizations.

Finally, we call on CISA to establish ex parte communications for the CIRCIA rulemaking. This is a critical step toward ensuring a robust regulatory framework that reflects the intricate realities of cybersecurity in critical infrastructure sectors. As CISA now possesses enhanced regulatory powers, it is imperative that the agency adopts a transparent and open process akin to that employed by other regulatory bodies. This approach will facilitate continuous and meaningful input from industry stakeholders, whose expertise and first-hand experience are invaluable for creating regulations that are not only effective but also practical.

Such a process would not only enhance the quality and applicability of the regulatory outcomes but also bolster the credibility and trustworthiness of CISA as a regulatory authority in the eyes of the industries it regulates.

Deep and persistent collaboration is the key to achieving Congress's intent in implementing CIRCIA, and USTelecom and its members will continue to work closely with CISA, our sector risk management agency, through the Communications Sector Coordinating Council and other fora, and by actively participating in the CIRCIA rulemaking process. For decades, we have engaged consistently with CISA, its predecessors, and other Government agencies to provide information about cyber threats and to advance law enforcement investigations, and we will continue to deepen and evolve that practice.

We seek the Government's continuing partnership in making that a reality. I look forward to your questions.

Mr. GARBARINO. Thank you, Mr. Mayer.

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

STATEMENT OF AMIT ELAZARI, CO-FOUNDER AND CEO, OPEN POLICY GROUP

Ms. ELAZARI. Chairman Green, Chairman Garbarino, Ranking Member Swalwell, Members of the subcommittee, on behalf of OpenPolicy and our community of innovative companies, thank you for the opportunity to testify today on the implementation of CIRCIA.

My name is Dr. Amit Elazari, and I'm the CEO and cofounder of OpenPolicy. We are the world's first technology platform for policy intelligence and engagement, making Government affairs and policy more accessible to entities of all sizes.

OpenPolicy represents leading entrepreneurial companies, innovators that create cutting-edge security solutions that protect critical infrastructure and Federal agencies. OpenPolicy itself is a small business, a startup, and perhaps the smallest among the IT Sector Coordinating Council members.

Members of the subcommittee, at the time when threats to our Nation have never been more profound and the consequences have never been higher, many businesses and organizations still stand defenseless against persistent and advanced attacks. These threats advanced with AI. We are in an arms race against the adversaries, and they have an asymmetric advantage. They already have the information.

Winning in this race or merely keeping ahead, keeping pace requires more than just information. It requires reducing our collective risk. It requires achieving cyber resilience. This is one of the key goals of CIRCIA.

CIRCIA is one of the most comprehensive cyber laws passed in decades. It holds a great promise to reduce risk if implemented properly. If not, we risk a lot. Our colleagues have already spoken about this.

For small businesses, we actually risk increasing the cyber risk. This is because we have a small amount of firefighters, defenders, and we can overwhelm them with these requests. With billions in potential costs for both Government agencies and critical infrastructure entities, we need to get this right.

The communicative cost of this expanded scope we talked about, covered entities, covered incidents, needs to be met with a broader value-for-risk reduction. This entails action within CIRCIA and beyond it. Significant infrastructure investments, we talked about common architecture, common technologies, common forms.

We need to be giving back to those entities. We need to make sure that we take all those reports in and use the state-of-the-art technology to really get those insights and move from prevention to mitigation.

In the context of the CIRCIA rule, we are focusing on a few more recommendations. First of all, I talked about technology and infrastructure. The common framework to work between agencies needs to rely on the cutting elementary solutions. This is because only with AI we will be able to deduct the most important insights from all this information coming in and actually move toward resilience and mitigation.

We need to align the findings that we're getting from the indicators with other programs that are investing within agencies and critical infrastructures like CDM. If the threats are coming from OT, from OT infrastructure, this needs to be a priority across the board.

This type of reflection must also look at harmonization, and my colleagues already talked extensively about that. I'm going to bring forth one concrete recommendation.

The DOD, the DIB has a large population of small entities. We estimate about 20 percent of all impacted entities with the current scope within DOD. The CIRCIA agreement with DOD, getting that aligned with the different clients, this must be a priority. We will need Congress' support and oversight with this priority.

My colleague, he already talked about ex parte. In the next 15 months after the comment period extension, the landscape will change. An ex parte process would ensure we get feedback from all stakeholders involved as the threat landscape evolves in a way that is transparent. CISA can bring a model that is building on the FCC or the copyright office there to ensure ex parte communication.

We have an opportunity to lead in this race. Proper implementation of CIRCIA can yield significant progress. Your support and oversight is essential. There could be additional measures. We must focus on technology solutions and infrastructure.

We appreciate the time and the ability to share comments with you and stand ready to collaborate with you.

Thank you for the opportunity to testify, and I welcome your questions.

[The prepared statement of Ms. Elazari follows:]

PREPARED STATEMENT OF AMIT ELAZARI

APRIL 29, 2024

Chairman Garbarino, Ranking Member Swalwell, and distinguished Members of the subcommittee, on behalf of OpenPolicy and our community of innovative companies, thank you for the opportunity to testify today on the Cyber Incident Reporting for Critical Infrastructure Act or (CIRCIA).[1] We appreciate your leadership in supporting the passage of CIRCIA, and commend your critical role in conducting oversight of the law's implementation process. We very much welcome the opportunity to continue working with this subcommittee.

At a time when threats to our Nation have never been more profound, and the consequences for human lives, critical infrastructure, and the foundational institutions on which we rely, have never been more prominent, the majority of businesses and critical infrastructure providers still stand defenseless against persistent and existential cyber threats. These threats have only expanded with the advancement of AI; the convergence of operational technology (OT), IoT, and IT systems; and the growing sophistication of adversaries.

CIRCIA, perhaps the most comprehensive legislative action on cybersecurity in decades, presents a critical opportunity to increase the Government's situational awareness, reduce cyber risk, and move us collectively forward in the endless asymmetric fight against adversaries seeking to undermine U.S. national and economic security.

But, as I must emphasize—only if implemented properly.

My name is Amit Elazari, and I am the CEO and co-founder of OpenPolicy, a small business and technology company (otherwise known as a "startup"). I'm also the former head of cybersecurity policy at Intel Corporation, served as chair of the Cyber Committee of the Information Technology Industry Council (ITI), and was a member of the IT-Sector Coordinating Council (SCC) executive committee.

In addition to my current role, I teach at the University of California at Berkeley in the Master in Information and Cybersecurity Program and serve as an advisor to the UC Berkeley Center for Long-Term Cybersecurity. I also co-founded Disclose.io, whose body of work related to establishing authorization for third-party "good faith" security research (ethical, or "friendly" hacking) is referred to in the CIRCIA proposed implementing rule ("Rule" or NPRM").

In my capacity as a cyber policy expert, I engaged extensively in the stakeholder process as CIRCIA was drafted, and am now actively engaged in the rulemaking process. Today, I'm honored to share my views, and the view of the OpenPolicy community, on the progress made regarding CIRCIA implementation and the proposed rule.

By way of background, OpenPolicy[2] is the world's first policy intelligence and engagement technology platform, aiming to democratize access to the policy-making process for entities of all sizes by leveraging AI. OpenPolicy is a small business and perhaps the smallest member of the IT Sector Coordinating Council.

---

[1] 6 U.S.C. 681–681; Public Law 117–103, as amended by Public Law 117–263 (Dec. 23, 2022).
[2] *www.openpolicygroup.com.*

OpenPolicy collaborates with and represents leading innovators that develop cutting-edge technologies to enhance cybersecurity and protect critical infrastructure. OpenPolicy members include some of the world's leading AI, IoT, and botnet prevention security companies such as Armis, Human Security, FiniteState, HiddenLayer, Kiteworks, Cranium AI, and more. Our members' solutions are used extensively by the critical infrastructure community and among Federal agencies to protect against malicious attacks.

My testimony identifies concrete policy recommendations that seek to align the Rule and CISA's implementation process with Congressional intent. I also want to highlight the Rule's impact on small businesses. This committee is right to reflect on the implementation of CIRCIA, given its mandate, and also because of changes in the policy landscape, technology itself, and the threat landscape since both CIRCIA's enactment and the RFI release. OpenPolicy applauds you for facilitating this discussion.[3]

BACKGROUND

Recent events underscore the urgent need to strengthen national security and defense, and the opportunity CIRCIA has to advance Government situational cyber awareness.

The promise CIRCIA holds relies on the ability of CISA to quickly intake reports, allocate resources, and provide support to entities affected by cyber incidents. CISA seeks to identify trends and swiftly disseminate this information to network defenders. Such proactive sharing will help alert other potential targets about emerging and existing threats and ideally prevent them from succumbing to similar attacks.

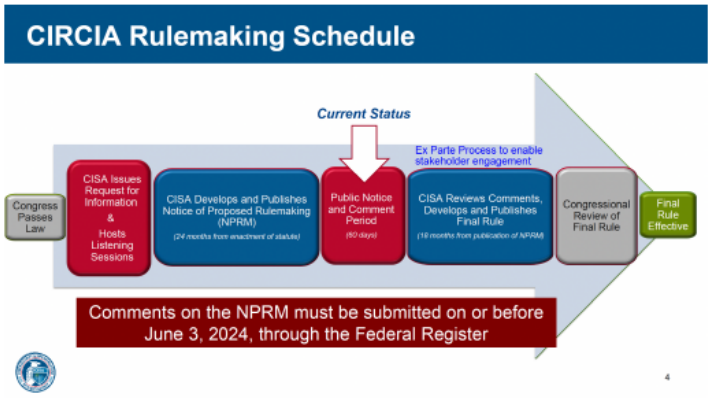
This use of information from the time an incident is reported, in support of immediate remediation but also to further longer-term prevention—is what CIRCIA aims to achieve and is meant to enhance our collective security. Congress intended for CIRCIA to not only improve Government awareness of cyber incidents but also to enhance security resilience throughout the entire ecosystem and ultimately advance risk reduction.

The effectiveness of CIRCIA and its underlying regulations should be measured not only by how efficiently information from reported cyber incidents is examined, enriched, and transferred, but also by how that information is leveraged to improve the security of the entire ecosystem, i.e., in a manner proportional to the cost (estimated in $U.S. billions). Achieving this goal will entail a unified Federal policy for leveraging the reported information to increase cyber resilience. This will require actions that extend beyond CIRCIA and the Rule. But the Rule, implemented correctly, presents a critical opportunity to advance this goal.

[3] CIRCIA requires covered entities to report to CISA-covered cyber incidents within 72 hours after the covered entity reasonably believes that the covered cyber incident has occurred and ransom payments made in response to a ransomware attack within 24 hours after the ransom payment has been made. See 6 U.S.C. 681b(a).

On the matter of Rulemaking process:

> *The landscape will continue to change—The Rulemaking process on CIRCIA should enable "ex parte" filings and engagements in the 15 months that follow the comment period.*



[ex parte comment process added, source: CISA]

CISA's 450-page NPRM on CIRCIA was released on April 4, 2024. Indeed, CISA's comprehensive and diligent work has resulted in an extensive Rule that will have a significant impact on our Nation, its security posture, and definitions that will have a profound impact on small businesses and the startup/innovation community. The majority of impacted entities may not be able to bring their unique point of view forward during this time frame, and most lack the resources and access to Government affairs professionals.

CISA has engaged extensively with stakeholders via the RFI, and various listening sessions, yet the critical phase of the regulatory development process begins now—with the release of the Proposed Rule, the Comments Consideration and adjudication process, and preparation for Final Rule release. Thus, we encourage CISA not only to extend the comment period and continue with the stakeholder engagement process but to also create a process that will allow for additional "ex parte" meetings and filings on the Rule. This should be accompanied by a transparent process for ex parte filings publication, similar to the proposed rules processes conducted and operated by the Federal Communications Commission or the Copyright Office.[4]

Such a process would ensure that perspectives could be provided in a transparent and inclusive manner to CISA as the policy, technology, and threat landscape evolves in the 15-month period that follows the NPRM release and after the comment period has ended. This would enable additional engagement and better alignment on the Rule, following the formal comment period.[5]

---

[4] See, for the FCC, 47 CFR §§ 1.1200–1.1216, and Federal Communication Commission, "Ex Parte Resources", *https://www.fcc.gov/proceedings-actions/ex-parte/general/ex-parte-resources.* See, for the Copyright Office, 37 CFR §§ 201, 205, U.S. Copyright Office, Ex Parte Communications, *https://www.copyright.gov/rulemaking/ex-parte-communications/*.

[5] OpenPolicy conducted meetings and led "ex parte" comments on a recent Cybersecurity policy related Rule and Order released by the FCC, which were ultimately cited in the Final Order. We find this process to be very useful and essential in a case where the evolving landscape merits continued, transparent engagement during the long period of comments adjudication, and particularly beneficial for small businesses who may not be able to engage on NPRM by the end of the comment period. We acknowledge the robust engagement processes already done by CISA, and further encourage CISA to continue and expand its engagement processes with innovative companies and small businesses, especially for sectors where they serve a large proportion of the impacted community, such as the DIB.

On matters of policy:

The cumulative cost of compliance burden, due to the proposed scope and expansion of liability, should be balanced and reciprocated with increased cyber resilience and risk reduction value

The record on stakeholder engagement reflects consensus on underlying concerns associated with definitions and issues proposed to be addressed in the Rule:

- Complexity and Regulatory Duplicity (among Federal agencies and regulators, States and Federal laws, and other applicable global regimes, such as E.U. NIS 2.0 directive) that will result in duplicative reporting, information and data overload, "noise", and extensive compliance burden on entities, including on small businesses, during the critical, "fire-fighting" period of incident response, when resources are limited. There is an urgent need for "harmonization" and streamlining of requirements.
- Concerns related to the definition of "covered cyber incident" capturing "too much" and in a manner that does not advance CISA's situational awareness, but rather overwhelms CISA.
- Concerns related to the chilling effect of expanded liability, which may hinder the public-private partnership model that undergirds information sharing and threat mitigation practices today with the U.S. Government and CISA, in particular.
- Concerns related to the scope of covered entities and impact on smaller businesses.
- Concerns related to the adverse impact to privacy and security due to increased information sharing, in certain cases, and the case of sharing sensitive "vulnerability" information in particular.

The Rule proposes a broad scope on many of these issues, notably the definitions of covered entities, incidents, and required fields. It notes however CISA's goal is to "achieve the proper balance among the number of reports being submitted, the benefits resulting from their submission . . . ". Our overarching recommendation is to ensure that the cumulative impact and increased costs associated with such expansion, will in fact, result in additional value to risk reduction and enahnced cyber resilience.

To that end, OpenPolicy proposes the following policy recommendations:

To ensure enhanced situational awareness of cyber threats across critical infrastructure sectors "translates" into enhanced cyber resilience and risk reduction, CISA should consider:

- Additional reports, support functions, and public-private partnership structures focused on impacted under-resourced entities for information sharing and cyber resilience resources.
- Robust consideration to ensure that state-of-the-art secure and diverse sets of technology solutions, including AI capabilities, are used to intake incident reports,[6] review them, respond, and enable real-time mitigation in a way that supports entities' ability to transition from "remediation" to "prevention".[7]
- Alignment of other CISA, and other Government-supported, resources (including programs such as CDM) to the nexus of threats, indicators, and compromises "spotted" via the reporting.
- Increased funding and resources to support the intake of remediation solutions and overall resilience of critical infrastructure, including Federal infrastructure, to attacks—embodying the zero trust and secure by design culture.

Our continued focus should be preventing attacks, not only remediating them. The volume of reports should be calibrated in service of this cause. Achieving this goal

---

[6] One method of technology adoption could be adopting standardized reporting forms supported by advanced programmatic and technological capabilities, whereby CISA can quickly operationalize, anonymize, and share data with the industry in a way that is not attributed to specific entities. This approach ensures that incident information, rather than being relegated to solely routine threat reports, is transformed into actionable intelligence that can be immediately utilized to protect entities and enhance industry awareness and preparedness. The primary purpose of this reporting requirement should be to deliver critical and practical information in real time, enabling front-line cyber defenders to thwart attacks. Clarifying this goal will significantly aid in addressing the tactical details of the final rule. It would not only ensure that it meets its intended objectives effectively but also foster the overall resilience and awareness of the entire cyber ecosystem.

[7] CISA notes, the concern from "noise" increased scope (as illustrated by a broader set of "entities", "incidents", and "reporting fields"), "can be mitigated through technological and procedural strategies." [Rule, at 23652–3]. More attention and resources should be provided in support of such technological and procedural strategies, to achieve the desired "translation" effect. CISA also recognizes further the breadth of duplicity and also that agencies may have different motivations in requesting such information.

will entail a broader technical and programmatic collaboration between all Federal agencies involved, as well as the adoption of technology solutions.

To summarize, CISA was tasked with regulatory development and proposed definitions seeking to balance these inquiries with the underlying congressional intent of CIRCIA. The NPRM reflects a cumulative extended scope of proposed definitions with respect to covered entities, the scope of incidents to be reported, the application on small businesses, and the potential (and actual risk) for duplicative burden for reporting.

Overall this approach reflects a higher "cost" and "burden" that needs to be accompanied by a balanced "value", and progress in situational awareness and risk reduction—thereby enabling a significant "giving back" component.

Further action is needed to reduce the potential cost associated with regulatory duplicity and the potential for liability

CISA has acknowledged both the concerns of stakeholders associated with a complex reporting landscape and the need for further action on this matter.[8]

We recommend the following:

- CIRCIA Agreements, geared to enable information-sharing mechanisms and the underlying technology architecture to support such sharing in a secure manner, should be prioritized, resourced, and achieved. The Rule clarifies that good-faith efforts to reach such agreements would be made. However and as demonstrated by policy actions in the last 2 years, achieving this goal requires a more holistic and deliberate effort from all agencies involved and Congress. As the Congressional Research Report on CIRCIA puts it: "It seems unlikely that Federal regulators will relinquish their specific reporting requirements in deference to CISA because existing regulations and the proposed CIRCIA rule *serve different purposes.*"[9] (emphasis added).
- One of the focal points of the CIRCIA agreements should be addressing the potential overlap with reporting requirements applicable to the Defense Industrial Base (DIB), under DFARS clause 252.204–7012. This path will reduce the considerable burden on a sector that is largely composed of small businesses (see below). This approach could be enabled by 2 related policy actions that recently matured. First, The DoD DFAR is soon to be revised,[10] thereby enabling further harmonization, despite the difference in scope of the "incident" definition.[11] Second, the DoD recently announced supporting infrastructure that can potentially enable a CIRCIA Agreement.[12]
- Congress should conduct oversight and perhaps even act in service of achieving additional CIRCIA agreements and reducing duplicity, when practical and desired, to achieve agency alignment.
- The need for harmonization and reducing duplicity is clear.[13] The path toward reducing regulatory duplication, including with globally applicable regimes, should move away from aspirational and exploratory, toward actionable and

---

[8] "In an attempt to minimize the burden on covered entities potentially subject to both CIRCIA and other Federal cyber incident reporting requirements, CISA is committed to exploring ways to harmonize this regulation with other existing Federal reporting regimes, where practicable and seeks comment from the public on how it can further achieve this goal." Id. at 23653.

[9] Congressional Research Service, CIRCIA: Notice of Proposed Rule Making: In Brief, April 11, 2024.

[10] The Defense Acquisition Regulations Council Director has recently tasked a team with rule development, exploring a revision for DFARS clause 252.204–7012, DFARS clause 252.204–7012, Safeguarding Covered Defense Information and Cyber Incident Reporting (See DFARS Case 2023–D 024, has described, on the DFARS Open Cases Report, *https://www.acq.osd.mil/dpap/dars/opencases/dfarscasenum/dfars.pdf.*

[11] Compared to the CIRCIA proposed rule definition, covered entities in the Defense Industrial Base (DIB) Sector are already obligated to report cybersecurity incidents in a substantially similar time frame (72 hours) pursuant to DFARS clause 252.204–7012, see Safeguarding Covered Defense Information and Cyber Incident Reporting. In contrast, the current scope of the DIB sector reportable incidents is narrower, and focuses on compromises of Controlled Unclassified Information while the CIRCIA proposed rule outlines a broader scope for "covered incident".

[12] On March 12, 2024, DoD published the Defense Industrial Base Cybersecurity Activities (DIB CS) final rule, which expands eligibility to DoD's voluntary incident reporting and cyber threat intelligence sharing program to all DIB entities (rather than just cleared defense contractors). These revisions will allow all defense contractors who own or operate an unclassified information system that processes, stores, or transmits covered defense information to benefit from bilateral information sharing.

[13] See also the National Cybersecurity Strategy, at p. 11, "The Federal Government must coordinate the authorities and capabilities of the departments and agencies that are collectively responsible for supporting the defense of critical infrastructure".

practical—and such efforts will likely require a common technology architecture, where additional resources may be needed.

- On legal liability, we recommend enhanced "due process" mechanisms for covered entities. We are concerned about liability protection erosion in the case of good-faith disagreements between CISA and the covered entity. As drafted, liability protection measures are "abandoned" once a subpoena is issued but without intervening process. While CIRCIA provides CISA the ability to use its subpoena power, the current NPRM does not include further consideration, or a "curing" process, an arbitration process, or other procedures to deliberate with CISA, in good-faith, the amount of information requested prior to CISA leveraging its subpoena power, while enabling the entity to maintain liability protection (see § 226.14(d)(1), and ps. 23735). We recommend further consideration and Congressional oversight to ensure a measured approach in the Final Rule implementation on this topic.

Small Businesses First "Mindset"

Although the CIRCIA proposed rule affects many small entities across all critical infrastructure sectors, its impact on the DIB Sector small business community is profound. Defense security compliance Industry Expert Jacob Horne provided some striking analysis:[14]

- Nearly a quarter of all affected entities are in the Defense Industrial Base Sector.
  - Of the 316,244 affected entities, CISA estimates 72,000 of them are in the DIB.
- 17% of entities affected by the CIRCIA proposed rule are DIB SMBs.
  - DoD has stated that roughly 75% of the DIB is made from small and medium-sized businesses.

  That amounts to 54,000 of the 72,000 DIB entities in Table 1 Affected Population, by Criteria (see NPRM, at 23742).
- 98% of affected entities are SMBs, 17% of affected SMBs are in the DIB.
  - Of the 316,244 covered entities, CISA estimates that 310,855 would be considered small entities (See, Id. at 23763).

	DIB Sector	Wire/ Radio Comms	Critical Manufacturing	Financial Services
Percent Total Affected Entities	23%	20%	12%	12%
Percent Total Costs	16%	14%	9%	9%

See Table 1 and Table 10 of the NPRM, Id.

We, therefore, recommend prioritizing "scoping" activities (such as achieving CIRCIA agreements) impacting small businesses that are profoundly impacted by the Rule, such as the DIB small business community.

SUMMARY

The Congressional intent for CIRCIA is "preserv[ing] national security, economic security, and public health and safety", and assisting the Federal Government with increasing situational awareness and visibility to cyber threats in support of a broader mission to achieve systemic risk reduction for the United States and its underlying critical infrastructure. This ultimate value, of increasing cyber resilience merits additional proportionality between the cost, and value of and processes CISA and the Federal Government will exercise to "give back" to impacted communities who bear the implementation cost. This balance may require more resources and additional infrastructure to "rapidly deploy resources" and better diverse, state-of-the-art solutions to stay ahead of malicious actors and deploy alerting systems. It will further require those who need to alert the Government—to have solutions, and "alert systems", to spot issues, and to intake alerts and process them into action. To achieve cyber resilience we must approach CIRCIA implementation in the context of the broader common fabric of cybersecurity policy efforts, implemented in the United States and globally.

[14] See also Jacob Horne, Sum IT Up Podcast: CIRCIA Rulemaking and Double Incident Reporting for the DIB, available at: *https://www.summit7.us/blog/circia-rulemaking-?hs__amp=true.*

Creating the architecture, technically, procedurally, and programmatically, and the culture, that truly achieves the underlying risk reduction goal of CIRCIA will require action from CISA, and other agencies, that may extend beyond the Rule, but proper implementation of CIRCIA can result in considerable progress. Much progress has been made—we will continue to rely on Congress's relentless attention to this matter, as we move forward with CIRCIA's implementation.

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

Mr. GARBARINO. Thank you, Ms. Elazari.

Members will be recognized by order of seniority for their 5 minutes of questioning. An additional round of questioning may be called after all Members have been recognized.

I now recognize the gentleman from Mississippi, Mr. Ezell, for 5 minutes of questioning.

Mr. EZELL. Thank you, Mr. Chairman.

Thank you all for being here today, and I'll just tell you I can't hear as fast as you talk. So just be a little patient with me. I may talk a little slower than the rest of these folks around here, but I'll do my best.

As CISA introduces new proposed rules around cybersecurity, I want to ensure that our industry partners are being heard.

Ms. Hogsett, CISA estimates that implementing the CIRCIA will cost $2.8 billion, cover 314,000 entities, and result in over 200,000 reports over the next 11 years.

Do you agree with CISA's analysis about the cost and this impact?

Ms. HOGSETT. Thank you for the question, sir.

So we are still going through the estimates and how CISA put those together. I will say, based on our conversations with financial institutions, that from what we can tell, the estimates for both number of companies and entities that would have to report, the number of reports they would likely receive, but also the cost to retain certain information is underestimated by quite a significant margin.

This is not an insignificant Government reporting burden that would be imposed on covered entities.

Mr. EZELL. To give us perspective, how many reports do you estimate that entities in your sector generate in a year? Can you describe current existing compliance costs for your sector?

Ms. HOGSETT. For my sector?

Mr. EZELL. Yes.

Ms. HOGSETT. So I'd have to get back to you with more specifics for the purpose of CIRCIA.

What I can tell you is that financial services is one of the most heavily-regulated sectors out there.

Mr. EZELL. Right.

Ms. HOGSETT. We recently did a survey of our member institutions to look at the compliance burden and the amount time that they spend on regulations and compliance, as opposed to improving their programs and defending against attackers.

Chief information security officers who are often the lead point for this within firms report spending anywhere from 30 to 50 percent of their time on compliance, and their teams collectively have reported spending about 70 percent of their time.

Mr. EZELL. OK. One of the stated goals of CIRCIA is to use information gathered about cyber incidents and to, "enhance the quality and effectiveness of information sharing in coordination of efforts with the appropriate entities".

Are you confident in CISA's ability to analyze this massive amount of data and use it to produce actionable information in some sort of a timely fashion?

Ms. HOGSETT. Again, thank you for the question.

We think that CISA has some work to do to scale back the requirements of this to ensure they are getting useful information and we're not just getting a lot of signal because we want CISA to be able to pinpoint those incident and those threat vectors that are really of most significance and then have the capability to very quickly turn that back around so that if a financial institution is facing something that might come to face an electric company or a telecom, that that gets out very quickly and we can prevent that from spreading further.

That requires a speed with which we have not yet seen Government be able to move. So we do encourage narrowing the threshold for incidents that would need to be reported, narrowing the elements that would need to be reported, and then also ensuring that CISA has the necessary capabilities and staff expertise.

You need some level of subject-matter expertise to also kind-of know what to look for to really make this successful. We think it can be successful and it would be very valuable, but we do need to narrow it a little bit.

Mr. EZELL. Well, anytime you get the Government involved, it's going to slow down. We all know that. So, you know, coming from police world, we get a lot of information, and sometimes it's not that easy to gather it and use it and get it done in a timely manner.

So, Dr. Elazari, can you highlight some areas where Federal agencies could improve regulatory reporting requirements to help small businesses?

Ms. ELAZARI. Thank you, sir.

So it is really striking to see the largest amount, significant amount of impacted entities are actually smaller. The threshold that is now proposed is building on the small to medium business size. So actually a start-up with a 50 million ARR, annual revenue, I understand from the estimates could be in scope. So this is a very large community.

Out of it, interestingly, a lot of it from the defense. The defense industrial base, these are innovators. They are working to protect us. So this is an area we must pay attention to.

So we are aware of a lot of duplicity, and actually it's striking. The Congressional reports, research itself says it's unlikely that some agencies would resist urge to continue with their reporting requirements because they think it's served—it's serving other goals.

Mr. EZELL. Right.

Ms. ELAZARI. So this is an area where we would need Congress support with.

I want to be very actionable. The duplicity issue is serious, and it's discussed. There is a National Cyber Director report on it. It requires additional action.

In the context of the CIRCIA agreement framework that CISA has put out in the proposed rule, the use of the terminology is somewhat aspirational. We would study the potential duplicity. There is desire and good-faith desire to work with agencies, but we really need to be doubling down on those sectors where the duplicity is not just harmful for the businesses, it's harmful for the Nation.

In those areas where we have a lot of burden on small businesses like the DIB which some common architecture formats, where we can, where we can achieve common goals—and I understand that two recent changes in the default rules for the DOD have opened the door on—for this issue. I've elaborated on this in the written testimony. So we think this should be a priority.

Mr. EZELL. Thank you very much.

Mr. Chairman, I yield back.

Mr. GARBARINO. The gentleman yields back.

I now recognize the former Chair of this committee, the gentlelady from New York, Ms. Clarke.

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

I thank our Ranking Member for allowing me to waive on this afternoon.

Good afternoon. First, let me thank our panel of witnesses for joining us today to share their views on CISA's recent NPRM on cyber incident reporting.

Let me also once again thank the Chair and Ranking Member for permitting me to participate in today's hearing.

CIRCIA was one of the subcommittee's most significant accomplishments during the 116th Congress, and I'm committed to ensuring its success.

I'm also glad to see some familiar faces at the witness table. Both Ms. Hogsett and Mr. Mayer testified at the subcommittee's legislative hearing on CIRCIA in September 2021 and offered critical input that improved the bill.

So I appreciate your continued commitment to CIRCIA's success.

Implementation of CIRCIA will be an enormous undertaking for both the Government and the private sector, and so I congratulate CISA on publishing the NPRM.

Having reviewed sections of the proposed rule, I want to clarify a few points. When I began working with my colleagues on the subcommittee and in the private-sector draft CIRCIA, our consensus was that the Federal Government would benefit from a well-scoped incident reporting framework.

Notably, on September 2021—at a September 2021 hearing, I said that we do not expect all critical infrastructure owners and operators to be subject to this reporting requirement. Rather we expected to apply only to a subset.

Additionally, our intent was that reporting requirements would be appropriately tailored to limit overreporting and ensure that CIRCIA ultimately yields the security benefits we intended. In short, we wanted reporting from more than the 120 entities the Solarium Commission recommended and a greater range of incident

than just those that would trigger a unified coordination group. But we did not intend to subject everyone or every incident to reporting.

To that end, I hope that CISA will continue to further engage with stakeholders to refine the parameters for incident reporting.

Another priority was streamlining reporting and reducing the cost of compliance, which brings me to my first question directed to all of our witnesses.

What can CISA do—be doing right now to streamline incident reporting and what can it do to ensure that cyber incident intake forms are accessible and easy to use?

Mr. AARONSON. We'll go in order.

So, first of all, let me just thank you, Representative Clarke, for everything you just said about your intent with CIRCIA. I think all of us, I'll certainly speak for EEI, agree with that intent.

I think, most importantly—and I mentioned it both in my written and verbal testimony today—is to leverage sector risk management agencies as areas where they are already collecting data through mandatory reporting requirements that are sector-specific and meaningful.

Leveraging the substantially similar reporting requirement definition that you put in the act but that doesn't seem to really be as prominent in the proposed rule is probably the most important recommendation I can give.

Mr. MAYER. Thank you, Congresswoman Clarke, and also thank you for the work you've done to put—promote this work with CIRCIA and other efforts in cybersecurity.

I think the two points you mentioned are critical here, and here's where there's opportunities for improvement.

One is a subset of the covered entities. I have no way of providing any assurance, as I read the rules as they are proposed, that we're not going to require all of the companies within our sector to be responsive to this. That will absolutely guarantee that the CISA will be overwhelmed with information that's submitted.

The question was asked about the 200,000 potential reports between now and 2033. That's light years away, 11 years, when it comes to cybersecurity. We'll be in a completely different environment in 11 years. We'll have 6G. We have AI. We'll probably have quantum computing at that point.

So trying to speculate about what that environment looks like in terms of threats and reporting is very challenging.

I do think it's very important that we get clarity around what is a reportable event because the way it reads right now, I have no way of knowing what a company would be responsible for submitting, given the current types of attacks that we're facing.

One company alone in our industry talked yesterday about having 6,000 attacks a month. We could be at 200,000 reports in 1 year or less just from a narrow subset of companies.

So we really need work together with CISA and other stakeholders to figure out how do we get to the intention of the legislators, Congress, and CISA which is to provide rapid response in times of triage—we're talking about really significant incident—so that we can help victims, so that we can forewarn other folks in the ecosystem, that we can integrate the information, assemble it,

study it, analyze it, and produce mitigating communications, what can we mitigate.

If we do that, we have a much higher likelihood that we're going to be successful. If we don't do that, I think we're looking at a big problem. Hopefully over time it will evolve. We'll get better at it.

Ms. ELAZARI. I will just add——

Mr. GARBARINO. We'll let—you can continue, please. You can answer the question.

Ms. ELAZARI. OK.

First of all, Ms. Clarke, thank you so much for your leadership in support of passage of the law.

I will just add very briefly. Common architecture, the NPRM is very lean on except the web form and some API. Colleagues have already discussed the issue of the definition, the scope, the reporting.

If there is not going to be a very sophisticated technology system to take all this intake forms with one format and APIs or at least where we can harmonize, we won't be able to leverage the same cutting-edge solutions that the adversaries are already using.

That is technology that is also going to help us move again from prevention, from the firefighting, to understanding the systematic risk, to moving to cyber resilience which is prevention.

Ms. CLARKE. Thank you.

I thank you, Mr. Chairman.

I thank you, Ranking Member.

I appreciate the indulgence. Thank you.

Mr. GARBARINO. Thank you. Thank you for coming.

I now recognize the gentlelady from Florida, Ms. Lee, for 5 minutes.

Ms. LEE. Thank, Mr. Chairman.

Thank you to all of our witnesses for being here today for this hearing.

Mr. Aaronson, I would like to start with you.

You identified in your testimony 5 specific areas you thought were in need of further consideration related to our process here, and one in particular was data preservation requirements.

I recognize your concern about the cost and logistics of maintaining the current data preservation that is proposed, but CISA suggests that maintaining data in this way helps them to analyze information and come up with better long-term strategies to help prevent attacks.

Would you share with us how long and in what way you recommend data be preserved?

Mr. AARONSON. Thank you so much for the question, Congresswoman Lee.

So I would say the importance of data retention, that's a—that's resource-intensive. We were talking about some of the statistics that you've heard. Mr. Mayer just mentioned a number. I mentioned a company that will remain nameless but that thinks they could have as many as 600 a month, and that would—that would evolve out to more than 65,000 over the next 9 years.

That is a significant burden of retention. That's a significant burden on the resources that would be needed from a digital perspec-

tive. That's a significant burden from a work force perspective, having to manage all that.

So I think maybe a little bit more philosophically, juxtaposing incident reporting, which is mandatory, and information sharing, which is voluntary, the idea here is we're trying to glean signal from noise.

I don't disagree with CISA's interpretation that more data could yield more information, but that's within reason. If we're talking about one company generating 65,000 reports over the course of the next 9 years, extrapolated over 300,000 potentially covered entities, how do you glean signal from that noise? How do you get or manage 2 years worth of that data? How do you manipulate it? How do you resource it? How do you have staff that deals with it? How do you have the digital infrastructure that can actually maintain all of that?

Those are really serious questions and really resource-intensive challenges.

Ms. LEE. Is there a time line that you think would be more appropriate?

Mr. AARONSON. So I think it's less the time line and more the amount of data that would be requested. So if we can start to narrow down the number of reports that would be required to those things that are truly impactful and truly impacting truly critical infrastructure, then a 2-year time horizon is not untenable.

But if you're talking about throwing everything against the wall, that's when it becomes a more resource-intensive challenge.

Ms. LEE. You just mentioned something that is—was my next question because several of you have touched on this subject and that is the idea that the threshold for the reporting requirement itself you perceive to be overly broad and that it's going to capture too many things, too much information.

I think Ms. Hogsett referred to it as, you know, what is a reportable event and whether the definition there should be narrowed.

Mr. Aaronson, I'll start with you since we're already discussing it. Do you have any specific thoughts on how that definition should be narrowed? What should be a reportable event?

Mr. AARONSON. So in particular, the—so it's the four prongs. Right? Any one of them could trigger a reportable event.

The phrasing "loss of integrity" and some of the supply chain aspects, that's a lot of things. You know, without getting technical but things like password spraying, things like any sort of impact on a cloud provider could impact integrity, could impact availability. That becomes a reportable event.

Does that really matter? That's the question that we need to ask ourselves. What are those types of incidents that we truly need to be collecting?

Ms. LEE. Ms. Hogsett, let me hear from you on that same question.

Ms. HOGSETT. Yes, thank you for the question.

So we referred to it in our past comments to CISA as it should be with malicious intent. So if you think about an event that is having an impact and causing harm and it's not just a technical glitch or a system mis-configuration that took things off-line, I don't think those are the things that CISA should be collecting on.

But the way the definitions are currently crafted, it would capture that. We think that that should be narrowed to accommodate that letter.

Ms. LEE. Mr. Mayer, do you have any additional thoughts on that threshold of reporting requirement?

Mr. MAYER. I do think we have to get to the—when you are talking about confidentiality and integrating availability. You know, we're providing services that—we're providing services at 99.99 percent availability over the course of the year, what threshold would you lower that to, to make that reasonable?

I don't know the answer to that. But it's not, you know, what could conceivably be every single type of outage that occurs because all networks have issues. The question is: Have you built in the resiliency, the redundancy to respond quickly and survive that? How resilient are the networks?

I'm going to talk very briefly about supply chain because it's something I'm very familiar with through the task force. When you look at the supply chain and you talk about compromises, if we have to report events in the supply chain, we're not just talking about a static event. We're talking about everything from the design, to the development to the production, to the distribution, to the operations, to the maintenance, and ultimately to the end of the life cycle.

What is—what we have to look at is: Where is the most critical event that's going to occur? What's going to be the immediate impact? What is the potential for some cascading impact? How big a part of the ecosystem can potentially be impacted? That's going to be an iterative and evolving process.

So we have to get to the place where we can refine the analysis and thinking here and maybe have a life span of 6 months. We may decide after 6 months this is no longer a legitimate threshold because there's a new attack vector.

That's the kind of iteration. That's where the collaboration with industry comes in. That's where the shared expertise and, you know, perspective between Government and industry comes to play.

Ms. LEE. Thank you, Mr. Chairman.

I yield back.

Mr. GARBARINO. The gentlelady yields back.

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

Mr. SWALWELL. Ms. Hogsett, just to follow up on your point about not having to spend time and resources reporting a glitch, which I agree with, how would you be able to tell that early on, though, if it wasn't malicious? I don't know the answer to that, but that would just be my follow-along on that issue.

Ms. HOGSETT. Yes, it does take time. I think there's room, and we have this in other areas where the entity is allowed to take time to actually assess what happened. You can fairly early on figure out, OK, well, we had a major upgrade going in and it went awry versus we don't know what this is. It potentially looks bad. Then our firms would err on the side of, like, that's a bad thing.

It reaches we would refer to a materiality, like, has a significant material impact on a material part of your operations. That's a significant threshold.

That's kind-of how we think about it and would encourage an opportunity to talk to CISA a bit further about how we could capture that.

Mr. SWALWELL. Great. Thank you.

Ms. Elazari, you noted in your opening and alluded to the risk of being overly broad, especially for small businesses, and that if you do that, you risk them actually becoming more vulnerable to an attack.

I think I understand what you are saying but just want to give you a little more time to articulate what that looks like.

Ms. ELAZARI. Thank you, and I appreciate the question.

So there are a couple of points here. Certainly the thresholds are really broad in the rule, both in terms of the definitions of the small businesses. They actually refer to the specific sectors in certain cases.

I think we risk two main elements. When it comes to the small businesses, they really don't have the ability to divert the resource in order, you know, to make those type of assessments. So there is a strong, you know, concern they're going to be overreporting. They really cannot be seeping through those definitions, and they don't have the legal teams that could do that.

The other perhaps, you know, striking problems is for the small businesses, if you're devoting the resource there, they're not firefighting. This is real risk.

The final point is that those small communities are also the ones that really need our assistance not just in the prevention but into moving into remediation, not just the immediate attack but that Secure By Design, so multifactor, patching, the basic tools.

So that should be a big focus, giving back. That may require some more resource, some more infrastructure.

Very quickly, Congressman, with your permission, I will say most of the incidents we have seen out there, including some software supply chain issues, have nothing to do with malicious intent.

So the common frameworks today for incident report do not hinge on the concept of malicious intent, but I do believe there is a lot of value in reflecting on what Europe is doing. NIS directive is already being implemented.

It seems that the thresholds here in CIRCIA in the proposed NPRM are actually going beyond some of definitions there. So perhaps there is some learning to be held.

Mr. SWALWELL. Thank you. I think that also goes to what Ms. Hogsett was saying, that distinguishing between a software upgrade that goes south, and a malicious actor is really important, and we want to make sure you have clear guidance on that.

To all witnesses—maybe Mr. Aaronson, I'll start with you—and if you could just limit it to about 20 to 30 seconds so each could answer.

As you engage with other regulators, what do you see as a willingness to harmonize with CISA?

Mr. AARONSON. So, I think they're willing—I mean, it's probably a better question for the regulators themselves, but I think they would welcome that, right?

So the electric power sector has the Department of Energy's OE–417 forms. Those are pretty interesting. They're very limited in what they're asking for, but when they are asked, it's because of an impactful incident.

NERC has been around since 2005, and has been asking for some very specific information about incidents. That feeds very nicely into what CIRCIA is trying to do. I think it's just about not reinventing the wheel on the CISA side.

I think on the sector risk management side, on the sector-specific side, we've already got pretty good reporting regimes. Let's leverage those.

Mr. SWALWELL. Great.

Ms. Hogsett.

Ms. HOGSETT. So some—we have a large number of regulators. Some of them are very willing to participate and sort-of recognize that you need to be aligned. We have others that are independent regulators who continue to do their own thing.

The SEC is one I would point to in particular that we see as particularly harmful, but we've also seen the Commodity Futures Trading Commission just earlier this year propose a new rule. As part of that, it would require instant reporting as well.

So we continue to see a proliferation of additional requirements rather than a centralization, as I think Congress intended to make this occur through CISA.

Mr. SWALWELL. Great. Thanks.

Mr. MAYER. So for the cons, I don't suffer the situation where we have, I don't know, 15, 20 different regulators. But we have one regulator who is very determined to impose cybersecurity requirements on our sector, and we would hope that as part of what the CIRC is recommending——

Mr. SWALWELL. Yes.

Mr. MAYER [continuing]. There would be a dialog between CISA and our regulators to make sure that we're not having competing requirements, that a single set of information can be shared as appropriate.

Any other agencies that get involved in this should begin to think about what that harmonization picture looks like broadly for the sectors, all of the critical infrastructure sectors.

Ms. ELAZARI. Perhaps I can just provide one point of view. I think even if we had more cohesive—cohesive kind of landscape and we have more parallels, we still wouldn't have common architecture.

So if the different regulators and agencies are not feeling like they're getting that visibility, sometimes their goal is different. We know from the SEC, the goal is, they're, you know, educating the investors, right, where the goal of CIRCIA is very different.

If we want to have that common architecture to gain insights, of course with the state-of-the-art technology and with the secure elements that we need to maintain that information in confidence, even with that streamlining, it will be hard to get from that information everything we need to give back.

So I think that's a common area of focus for the agencies as they're considering the duplicity.

Mr. SWALWELL. Great. Thank you. Yield back.

Mr. GARBARINO. The gentleman yields back.

I now recognize myself for 5 minutes of questioning.

I want to, in my second round, I'm going to focus on harmonization, but really on this first round, I want to talk about the specific rule, and really hear from industry as to what—you know, the comment period is open. We think it's going to be extended—what really needs to be done, because as I said in my opening statement, this needs to be done right. We don't want to do it and then have to change it. This needs to be done right. That is why we're doing this.

You know, I was looking at some things, you know, for example, there's a—under the proposed rule, there's a covered entity would have to submit a supplemental report. They don't have all the information required within 72 hours of having a reasonable belief that there's an incident has occurred.

You know, they're looking at, they want information such as technical details, physical locations of networks, devices, information systems, the impact of covered cyber incident, and the covered entity's operations, you know, et cetera.

That seems just one of the many things that they're looking for. You know, I want to hear from you, do you think this information is feasible to provide, you know, within 72 hours, or, you know, how much longer after that will a supplemental report be filed? Are there going to be multiple—is there concerns of multiple supplemental reports?

You know, I want to hear specifically from everyone, all of you, just really the concerns about what's under the current rule, what's proposed, and what needs to be done to fix it. So we'll start with Mr. Aaronson.

Mr. AARONSON. So there's a lot there. I would say the rule itself—I think Ms. Clarke hit it really well—the intent of the committee always was to create a subset of reports that actually glean—you know, again, create meaningful insights, and I fear that by asking for all of these things in such a short amount of time—yes, there's the supplemental and all that.

But as everybody has said, that fog of war in those early days, that is not a good time to be spending on compliance burdens; it's a good time to be responding and recovering and then understanding what the impact is.

I'll keep going back to the value of the OE–417. There was an impact. Great. We told somebody there was an impact. Now there's knowledge that was an impact, and we can all talk to each other.

The other value of that construct is, it creates a signal that something happened, now let's dig deeper.

This idea that we are going to generate so much information in a short amount of time, in the interest of creating insights for other sectors, is just flawed. This goes back to my juxtaposing information sharing versus incident reporting. Incident reporting is about compliance. Incident reporting is about mandatory knowledge.

As Dr. Elazari said, incident reporting in the SEC's case is about transparency to investors.

If what we're trying to solve here is to create cross-sector awareness, voluntary information sharing is what we need to be prioritizing, and to the extent that CIRCIA needs to find those truly impactful, truly critical incidents that happened, then having that first step of, this happened, like an OE–417, as opposed to trying to dig deep and create all of this, you know, kind-of long-term record, it's just not the right approach.

Mr. GARBARINO. Ms. Hogsett.

Ms. HOGSETT. To build on Scott's point, so this is frankly the most expansive data-reporting regime we've seen. We've got companies that have to comply globally with hundreds of different regulatory reporting requirements. This is the most, I think, of any of those, quite frankly.

The data elements, as Scott noted, are well beyond what would initially be known. So, you know, a better approach, what I think we would propose is, narrow that to really critical information that you can do something with, and then send that back out to a wider audience.

There is value in CISA being able to follow up with the entity, and I think on our part, you know, our firms would far prefer to get the information in quickly to CISA, and then have an on-going dialog if CISA would like more information, as opposed to making it a foregone conclusion that you must submit all of these data elements.

If you actually read the full rule, the requirement is sort of an allowance to provide, if you don't have the information right away at 72 hours, you can provide the supplemental reports.

The assumption, as its written, is that you will, at some point in time, provide all of that data, or at least say, don't have it, won't provide, and then you're sort-of like, Are you going to take it? Is that good? Or is CISA going to come back at you and say you didn't comply.

So I think there's a lot of questions that firms still have around how often, like, when—what would trigger a supplemental report. You might have multiple of those before the incident is closed.

It's just creating an on-going reporting requirement that we think could be balanced better to make it effective for everybody.

Mr. MAYER. I think there's a theme here that runs across a lot of these issues, and that is a lack of specificity and clarity. So the rule talks about providing new and different information. I don't know what "new and different information" means and how significantly new it is, and how different it is from what was originally provided.

It's also not time-bound. So I could be in this situation or a company could be in this situation where they're into perpetuity, you know, providing supplemental information that may not have any impact on improving security in the ecosystem.

So we need to tighten this up, get some clarity around what type of supplemental information is going to contribute to a better understanding, allowing CISA to more immediately respond and help victims and forewarn victims.

If it doesn't meet that criteria, we're going to be taking resources away from CISA's people, and we're going to take resources away from front-line practitioners, who are going to be more concerned

about complying with the supplemental requirements out of fear of some enforcement action potentially. I don't think that improves security at all.

Mr. GARBARINO. Doctor.

Ms. ELAZARI. I think it's worth underlying what was the goal with the supplementing reporting clause in the beginning. The concern was—and it's right—that in the 72 hours, there isn't enough information.

So the goal was to report something and not fear from liability as we come toward the potentially, and often needed, supplemental reporting, but the problem is, we have all these fields, and instead of thinking about it as a voluntary measure as needing and allowing CISA to use their RFI, right, process, in order to ask more information, it's flipped backward.

So that, combined with the potential for liability protections being removed once, you know, CISA exercises their subpoena power, creates a very big risk that people—entities will just be over-reporting at scale, essentially what we call in security DDOSing, creating a denial of service, overloading of information.

Mr. GARBARINO. Thank you, Doctor.

I'm so happy my friend from New Jersey, Mr. Menendez, could join us. This is wonderful. I now recognize Mr. Menendez for 5 minutes of questioning.

Mr. MENENDEZ. It's a pleasure to be here. Mr. Chairman, Mr. Ranking Member, thank you for convening today's hearing. To our witnesses, thank you for being here. I'd like to discuss possible solutions to building out CISA's analytical capabilities.

Dr. Elazari, in your testimony you mentioned that CISA should be using state-of-the-art technology to collect incident reports, including leveraging artificial intelligence.

Can you expand on how leveraging AI could improve the process of incidents reports?

Ms. ELAZARI. Thank you, Congressman. So, I'm not the technology expert here, but our community does include some of the most innovative AI companies in the world. In security right now, the cutting—the leading-edge companies are leveraging AI in order to study information on scale, use generative AI models as well to be ahead of the attacker, to predict where the attacker would be, leveraging knowledge from, you know, the dark web and knowledge about the adversaries, and really, you know, being ahead of even the—of the incident.

I think there is a lot of new technologies out there, but what is striking, in the context of the proposed rule, is CISA's comfort about getting all these reports. They actually say it—we're not concerned about not getting not enough reports—sorry—too much reports. We are concerned about not getting enough. We're going to solve it with today's technology and strategic approaches.

But the funding is $100 million annually, I believe, so there is no proportion between how do we think that all this reporting is coming in, and actually we will be using cutting-edge solutions like the solutions to give back.

I must emphasize, give back, it's not just an immediate remediation. It's what are the patterns, where do we need prioritize more cyber resilience measures, right, those secure by designs, those

measures that we need to give to the critical infrastructure entities that don't have resource.

So we have to be leveraging those cutting-edge solutions and they're going to be changing in the next 15 months, and this is where the ex parte process will allow us to have that dialog with the right parties in place with CISA.

Mr. MENENDEZ. So you're confident in the technology and that it will assist CISA. You're just concerned, it seems like, that the funding mechanisms to ensure that CISA has the ability to procure and use and have the work force to use the technology that's state-of-the-art, cutting-edge, that will enable them to do their job better?

Ms. ELAZARI. So I think, sir, there are also very legitimate concerns being raised on the scope itself. There are two prongs here. There is everything that is being reported in the overload, but then at the minimum at the other side, we should be using cutting-edge solutions because that's the way to make sure that the asymmetric advantage that the attackers have, they have—they go after the weakest link—is met with the best solutions to get the insights.

I do believe that—and we need to study this more—but there is an underestimate on how much it's going to be costing to not just create that common architecture to get all the reports in one place and secure them, but also, use those solutions in order to make sure that we are actually having—getting the best indicators. There is a lot of information right now we are asking for entities. We need to give back risk-reduction value.

Mr. MENENDEZ. Understood. On the flip side, is there any risk that in using AI, CISA's processing of these reports might include hallucinations, and could the use of AI end up reducing the accuracy for the sake of processing speed? Anybody that wants to answer that question.

Ms. ELAZARI. I would just say very quickly, sir, that I think our—this administration, this Congress, recognizes both the benefits and the need to use AI, and both the potential risks. So I think there are processes under way. We are, in fact, taking part in many of them, to make sure that as we are deploying AI solutions, we are also making—make sure it's deploying solutions to make it trusted and secure.

Mr. MENENDEZ. Great.

Mr. MAYER. We also want humans in the loop so that there's a way to make sure that the AI is not hallucinating and telling you to shut down, you know, parts of the global network when that may not be necessary, so.

I mean, we're all going to be learning how to use AI and how to not use it and how to evolve it over time, how to make sure we have assurances that it's not, as you said, hallucinating. That's a process. It's a new technology that we're going to be looking at.

Mr. MENENDEZ. Keeping people in the room and part of the process, do you believe that we are—that the technology that we're developing, that's being developed in the AI space, or state-of-the-art technology that we could use for CISA, do you believe that our training of the work force is being developed as quickly, and will we have the people that we need to ensure that we keep—excuse

me—people in the room to take advantage of the technology and have that sort of parallel track?

Mr. MAYER. It's a race.

Mr. MENENDEZ. Yes.

Mr. MAYER. We're going to have to do a lot to prepare the work force for the introduction of AI on so many different levels. The displacement that's going to occur as a result of AI is going to be significant.

I will tell you that AI has advantages, both in terms of improving our defensive capabilities, but it also provides advantages to the adversaries in terms of their offensive capabilities.

We know the adversaries are going to use every advantage they can get, and AI is going to be a big vector for accelerating that. So we have to have the same capabilities in terms of defending our networks and the ecosystem.

Mr. MENENDEZ. Absolutely.

Ms. HOGSETT. I would just add, I agree with Robert and the previous comments. The human capital element and the subject-matter expertise is the key piece, that technology will get you so far. But not just keeping a human in the loop, but also CISA currently has challenges with having specific subject-matter expertise to, again, weed through the noise that they're getting in, to pick out key pieces and how to connect those.

Machines can't currently do that, and it's actually something we've heard from security experts at the firms we work with, is that, if you've got someone who's watching networks all day long, they know when something is an anomaly. They automatically instinctively have that, and they know what to look for. So technology can amplify that, but it's not 100 percent solution.

Mr. AARONSON. I know we're over time, but I am professionally obligated, when talking about AI, as a representative of the electric power sector, to say a couple of things.

So first of all, artificial intelligence, as has been said, is, first of all, an incredible opportunity with all sorts of efficiencies.

It also represents an attack vector, for sure, and so from a national security perspective, it is an imperative that United States win at artificial intelligence.

AI needs data centers, data centers need extraordinary amounts of electricity, and electricity needs infrastructure. So, we need to be making sure that we're building out infrastructure that can support this AI revolution, support the data centers that will support this digital opportunity.

So there is a very clear through-line between the AI/national security imperative and infrastructure development to support it.

Mr. MENENDEZ. Appreciate that, and yield back, Chairman.

Mr. GARBARINO. Come late and you go over.

Now, for our second—I'm going to start a second round, and I'm going to recognize the gentlelady from Florida, Ms. Lee, for another round of questions.

Ms. LEE. Mr. Aaronson, I'd like follow up on another one of the concerns that you identified. So overall, of course, we're here trying to find ways to streamline our processes, promote efficiency, eliminate duplication, but you highlighted a particular concern related to all 16 critical infrastructure sectors reporting to CISA, and

therefore, all of this sensitive information residing at CISA as a potential protection of information becoming a vulnerability in and of itself.

Tell us, though, how would you reconcile those two goals of, let's have a single reporting system, let's streamline this for our private-sector partners, but also, being concerned about housing that kind of information all in one single location?

Mr. AARONSON. Yes. So it's sort-of a two-fold question. There is the malicious side of it which is—and I don't have some, you know, magic-wand answer. I would simply say, we have to recognize that that is going to be a target.

That—you know, sophisticated adversaries watch incident reporting. They like to know: did their attack have the impact that they intended? They like to use that information to hone new attacks.

So, a treasure trove, as I said earlier, of information is 100 percent going to be a target. We simply need to protect it accordingly. I think this goes to some of the CISA resourcing issues.

Let's go into this with eyes wide open. This isn't just about collecting data and putting it in a data warehouse somewhere. This is about protecting it as the critical, sensitive information that it is.

The second part is protection from things like FOIA, and using, again, public policy protections, like in the electric power sector, we have CEII—critical electric infrastructure information—making sure that this does not become open-source information, that well-meaning public citizens and reporters and whomever else want access to. We just need to make sure that we put belts and suspenders around protecting it as the sensitive information that it is.

Ms. LEE. You just mentioned something that I think is very interesting and important and not always recognized about artificial intelligence and the data centers and the necessity—the type of power and infrastructure that's going to be required to support these data centers.

Would you elaborate a bit on what you see coming on the horizon in that regard?

Mr. AARONSON. So extraordinary growth, and I think we always look at past performance as indicator of future need, and that's just not where we are right now. This is exponential growth that we are about to see.

I see this as an opportunity for everybody involved. I think there are a lot of opportunities with respect to infrastructure build-out. There are a lot of opportunities with respect to things like small modular reactors. I think the more storage, battery, utility scale storage we can get out there, we have to build more infrastructure to support this demand. Full stop.

I also view it as a supply chain challenge. The Chinese have used their industrial policy for the last 30-plus years as a weapon.

Much as we hear the Director of National Intelligence say that near-peer nation-states are using cyber threats to hold the United States at risk at a time of their choosing, I think Chinese industrial policy is doing the same thing.

When I talk about this, I like to use actually a Chinese proverb. The best time to plant a tree was 30 years ago. The second best

time is today. The best time to combat Chinese industrial policy was 30 years ago. The second best time is today.

So in addition to the build-out of the grid and infrastructure to support the AI revolution, we also need to be thinking about near-shoring, friend-shoring, onshoring, manufacturing capacity so that we can meet the demand growth that we're about to see.

Ms. LEE. Then turning back to your earlier point about efficiencies, you touched on sector risk management agencies earlier, and suggested that we might be better—we might be better able to utilize them. Tell us more about your thoughts on the sector risk management agencies.

Mr. AARONSON. Yes. So the electric power sector enjoys a really constructive relationship with our SRMA, the Department of Energy. There's a couple reasons for that. The Department of Energy is nonregulatory. So when we work with them, it is not with sort-of this regulatory sword of Damocles hanging over us. It is really this operational collaboration that happens between and among.

Leveraging SRMAs as this existing entry point for information sharing and for existing incident reporting allows for, again, a more efficient way to then inform—and I want to be careful here—CIRCIA and CISA play a really important cross-sector role.

That said, inputs from sector-specific agencies to then inform the cross-sector, in the electric power sector's opinion, that's the value of CISA, that's the value of CIRCIA, and so we want to see that leveraged.

Ms. LEE. Thank you, Mr. Chairman. I yield back.

Mr. GARBARINO. The gentlelady yields back.

Even though he came late, I'm going to recognize him again. Mr. Menendez, from New Jersey, you're recognized for 5 minutes of questions.

Mr. MENENDEZ. That's why I love showing up, Mr. Chairman.

An important part of improving cyber incident reporting requirements is to increase regulatory harmonization. Currently, not only have numerous Federal agencies imposed cyber incident reporting requirements, but many international governments have also mandated cyber incident reporting.

In March, Secretary Mayorkas announced a new effort to align incident reporting requirements with E.U. regulations where feasible.

For any of the witnesses, how important is international reporting harmonization to your sectors, and how can CISA and the NPRM help facilitate that kind of international harmonization?

Ms. HOGSETT. I'm happy to start. So for the financial services sector, we have a number of firms that operate globally and so I think one of the largest ones has I think the count is something like 115 different regulators that have a requirement to report incidents.

So that international dynamic is very valuable if for no other reason than to help ensure that a victim company can focus on getting themselves back on their feet and protecting any of their customers, et cetera, and not focusing on having to tick the box on multiple different requirements.

In our sector we actually have a G7 cyber experts group so of the global 7 countries that are our allies we have a work stream to help align some of these requirements.

The Financial Stability Board for us has already put out a proposed incident reporting template that we're working to try to get alignment globally on those common data elements.

The Cyber Incident Reporting Council that was created under CIRCIA actually highlighted some of this. There's a great value in helping streamline this so that we can all coordinate as we might need to globally.

Like if China is targeting critical infrastructure here, they might be targeting it at our allies at the same point in time. We want to make sure they can get information and that's shared as well.

The challenge right now with the way the CIRCIA rule has been put together is, it goes well beyond other requirements. So if you can narrow that, it will get us that much closer to having harmonization, having a streamlined reporting so that we can get information where it needs to go without disrupting a response.

Mr. MENENDEZ. Appreciate that.

Mr. MAYER. I think the more that CISA can do to help facilitate a dialog, either bilateral or multinational dialog, around some level of consistency is going to be very important. It's not just international, we also have to worry about States and localities getting involved in fragmented reporting requirements.

The more requirements there are that are not aligned and inconsistent, the much more challenging it's going to be for an enterprise to effectively address those reporting requirements in a way that's efficient for them and efficient for Government.

So I think CISA has a role to play on that international dialog, along with other agencies of Government, including the State Department.

Ms. ELAZARI. So to put this in context, I think actually the IT sector has, perhaps, the most multinationals, but it's not just multinationals with large departments of cybersecurity and lawyers.

If we have those small business entities with some software that is focusing on a critical function—we're talking about start-ups with $50 million, you know, in revenue, these—software is going anywhere, right? These companies often rely on operating globally often with Five Eye, with Europe.

So, I think actually not only it is essential, there is big opportunity in this international alignment, and I want to speak about two things in particular. We saw this in action with the IoT Cyber Trust Mark and the important work with the FCC to look into the E.U.-cyber intersect.

I believe the NAS 2 directive has actually more confined proposed definitions for some of the things we have seen in this proposed rule. So I think opting in, allowing companies that want to actually mutually report to a common architecture, at least when it comes to the NAS directive, where we have a lot of that critical sector and a lot of the IT companies already covered.

That is one very particular implementation that would not only bolster cyber resilience and the ability to work with our allies for remediation but really help companies.

So I think not only this is a priority. We need to be pragmatic and focus on these areas where we have the same covered entities, the same agreements, right, on the covered issues to ensure not just common definitions, but common architecture.

Mr. MENENDEZ. Appreciate that. One quick follow-up. The important work of regulatory harmonization requires not just the cooperation of CISA, but also the regulatory agencies that may have inconsistent reporting requirements.

As you engage with other regulators, what do you see as a willingness to harmonize with CISA, and how can Congress and CISA better support efforts at regulatory harmonization? I went over last time, so these have to be quick answers.

Mr. AARONSON. I'll try to give a quick answer. It's also responsive to Ms. Lee's question a minute ago, and I want to pick up on something Ms. Hogsett said.

Common architecture, common definitions, the problem right now is CISA's requests are so much different than every other regulatory agency. They've kind-of gone above and beyond. There isn't anything that's substantially similar.

So, I think there's got to be a, let's meet each other halfway. I think there are some regulatory agencies—I can't speak for any of them, but I think some would like more information. So maybe it is rising that tide a little bit. But CISA's got to come back down a little as opposed to asking for the kitchen sink.

Mr. MENENDEZ. I appreciate that, and I yield back.

Mr. GARBARINO. The gentleman yields back. I now recognize myself for 5 minutes of my second round of 5 minutes. That's good English.

Mr. Mayer, CISA expects entities will be able to self-identify as a covered entity, and they think it's going to be easy. Do you agree that most entities will be able to easily self-determine whether they are a covered entity under the rule?

Mr. MAYER. Well, I think in our sector's case, I think—and I alluded to this earlier—I would start with the assumption that you're a covered entity just by virtue of the fact that you're providing communication services, you're a part of the critical infrastructure 16 sectors.

I don't think, you know, the exemptions under the small business is going to necessarily be persuasive in getting you the exemption. So the assumption has to be that, assume you're covered.

Mr. GARBARINO. Better to be safe than sorry, I guess, right?

Mr. MAYER. Sorry?

Mr. GARBARINO. Better be safe than sorry?

Mr. MAYER. Correct.

Mr. GARBARINO. OK. The sector-specific plans referenced in the Notice of Proposed Rulemaking were last published in 2015. Is your sector still accurately represented by its specific plan?

Mr. MAYER. I believe it is. I think when we look at what we identified as risks and the performance plan, many of that—much of that is still relevant.

I will say yesterday that the National Security Memo that came out will set in motion the requirement for a new sector's risk assessment, and a sector-specific plan. So we will put resources to evaluate what's changed, what's most impactful, and what stretch

should we be thinking about and perhaps that we were not fully cognizant of over the, you know, years ago when we did the performance plan.

I think, for example, AI is going to be a factor, and in the DHS ICT task force, we're looking at the threat analysis we did 3 years ago, and we're now going through with the lens of AI and trying to understand what changes about that threaten landscape.

So yes, it's going to have to be updated, but a lot of it is still relevant.

Mr. GARBARINO. Thank you. I said I was going to talk a little bit about harmonization, and I can't do that without talking about the SEC rule which I hate. We've heard a lot of anecdotal concerns about the chilling effect that this rule, the SEC cybersecurity rule, is having on cyber information.

Ms. Hogsett, can you explain from the bank—BPI'S perspective, I'll say, negative impacts, but I'll let you talk about potential impacts of the SEC's rule on cyber information sharing.

Ms. HOGSETT. Sure. Thank you for the question, and thank you for your leadership on this point. We really appreciate it.

So our concern with the SEC disclosure rule is that literally the rule requires that 4 days after you've determined that you have a significant event, you are publicly disclosing that.

If we look at CIRCIA, that means that basically CISA has about 24 hours, perhaps, to leverage the confidential reporting, and then turn that back around into useful information to help prevent attacks or further harm.

That in today's day and age is an extraordinarily short period of time. So you're really cutting short and undercutting the purpose and the effectiveness of CIRCIA itself.

Publicly disclosing gives attackers information they might not otherwise have. We have seen it being automated using bots to then start to automatically scan other companies to detect if they have a certain vulnerability.

It also prioritizes the desire of investors to have transparency over the need for critical infrastructure to protect themselves. So we believe that this is very harmful.

In the short 4 months that it has been in effect, we've already seen it interfere with long-standing collective defense efforts because it's caused confusion about what information can and cannot be shared.

We've also seen attackers use it as an additional extortion method. So, if you don't file with the SEC, your ransomware actor will then threaten to report you to the SEC, and it is now the third prong of an attack that they have started to use.

Mr. GARBARINO. Thank you. Hopefully, our efforts—we're still working on a CRA—hopefully our efforts are successful. Last thing, I have time for probably one more question, and we're going to be submitting a lot of questions for you to answer, because I could go on for another hour, I think.

Mr. Aaronson, just yesterday, Biden administration released an NSM–22 update and PPD–21, and you talked about how EEI enjoys a positive relationship with DOE, your sector risk management agency.

Can you elaborate a little more on what's working well with the energy sector and the SRMA relationship and what could be improved as the administration works to implement both CIRCIA and NSM–22?

Mr. AARONSON. These things just roll off the tongue, don't they?

Mr. GARBARINO. Yes.

Mr. AARONSON. I miss PPD. That was a lot easier to talk about. So I mentioned before, I think part of the reason that we enjoy a good relationship with the Department of Energy is, they are non-regulatory. So, it's a much more trusted, kind-of open relationship.

I think another aspect of our partnership is the Sector Coordinating Council. We have a CEO-led Sector Coordinating Council. I serve as part of the secretariat for that, represents all segments of the sector all across not just the United States but North America. It is a North American grid.

Bringing chief executive officers together with senior Government officials really does help us to prioritize the things that are important and then work collaboratively to buy down risk.

The last thing I think I would say is, a focus not just on trying to protect everything from everything all of the time, but instead, acknowledging that resilience is probably the most important avenue of defense. We call it defense in depth, right? The attack does not have the intended impact or when it comes to natural hazards, like storms and fires and earthquakes and what have you, that ability to make sure bad days do not become catastrophic.

So, working collaboratively with Government to restore power as quickly as possible when something bad happens, having spare equipment programs working collaboratively with the Department of Energy on policies that enable resilience, that's really the crux of the fruitful relationship that we have.

The last thing I'll say is operational collaboration. We talk a lot about information sharing—we talked about it a lot today—yes, information sharing is important, but industry and Government working hand-in-glove, side by side, to share actionable intelligence, to inform intelligence, through organizations like the Energy Threat Analysis Center, or ETAC, have been really fruitful ways to leverage Government resources and industry resources to buy down risk and to understand attacks and socialize mitigation as quickly as possible.

Mr. GARBARINO. Thank you.

I now recognize the gentleman from California, Mr. Swalwell, for another round of questions. Do you have——

Mr. SWALWELL. Yes, please.

Would you all agree that the SEC rule is affecting our ability to recruit talented CISOs to help us protect critical infrastructure? I'll start with Ms. Elazari. If that's the case, why is that the case, and is it driving folks out of the profession as well?

Ms. ELAZARI. So I think it is the case. As a matter of fact, we've seen an amicus brief filed on litigation related to SolarWinds, *SEC* v. *Tim Brown and SolarWinds*. We have seen an amicus brief on behalf of the CISO community with about, I believe, 50 leading cybersecurity professionals, by the way, former, you know, S&P 500—very large organizations as well as a different amicus brief from Government—former Government officials, noting that one of

the potential consequences of that particular litigation, but also the overarching, right, the overarching SEC cyber rule, is creating that chilling effect on the professional community.

We must understand that is not a community we have many of. The gentleman here talked already about the issue of skilled work force.

So this is a big priority, and we need to look at the CIRCIA rule and the scope of what's covered, but also, the issue of the liability protections being stripped away if there is a disagreement after the RFI and the first subpoena and to—and really think about those professionals.

So I think all of this is very important context because we do have a crisis around the skilled work force in cybersecurity, especially in the top layer. We have heard from the community there is impact, both with the rule and both to litigation around it.

Mr. SWALWELL. Great. Thank you.

Anyone else want to weigh in on that?

Ms. HOGSETT. We've definitely heard a rise in concern among the CISO community with the SEC rule, particularly, as Dr. Elazari noted, the enforcement measure by the SEC with personal liability against the SolarWinds CISO.

Cybersecurity is a team sport. The CISO is, quite frankly, sort-of the conductor——

Mr. SWALWELL. Yes.

Ms. HOGSETT [continuing]. And they can do many things, but they can't control all of it. So I think for CISOs who have not previously had that sort of a personal liability, it is deeply concerning for them, and I've actually heard of one who basically decided to retire because the risk was just too great after a really successful decades'-long career.

Given the threat environment especially that we face, it is deeply concerning to many.

Mr. SWALWELL. As one recently told me who was a Fortune 100 CISO, he said, when an attack happens now, rather than respond to the attack, the first thing that you do is, you huddle all of the lawyers, and you're losing precious response time because you're worried about, like, your personal liability on any action that you take, which means that consumer data and, you know, consumer information and then potentially critical infrastructure could be seriously jeopardized as that's taking place, so.

Ms. HOGSETT. Yes.

Mr. SWALWELL. I'll yield back.

Mr. GARBARINO. The gentleman yields back.

I'd like to thank the witnesses for their valuable testimony and the Members for their questions.

The Members of the subcommittee may have some additional questions for witnesses, I know I do, and we would ask that the witnesses respond to these in writing.

Pursuant to committee rule VII(D), the hearing record will be held open for 10 days.

Without objection, this subcommittee stands adjourned.

[Whereupon, at 3:43 p.m., the subcommittee was adjourned.]

○