S. Hrg. 118–353

STREAMLINING THE FEDERAL CYBERSECURITY REGULATORY PROCESS: THE PATH TO HARMONIZATION

HEARING

BEFORE THE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS UNITED STATES SENATE

ONE HUNDRED EIGHTEENTH CONGRESS

SECOND SESSION

JUNE 5, 2024

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

Printed for the use of the
Committee on Homeland Security and Governmental Affairs

U.S. GOVERNMENT PUBLISHING OFFICE
56–046 PDF WASHINGTON : 2024

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

GARY C. PETERS, Michigan, *Chairman*

THOMAS R. CARPER, Delaware
MAGGIE HASSAN, New Hampshire
KYRSTEN SINEMA, Arizona
JACKY ROSEN, Nevada
JON OSSOFF, Georgia
RICHARD BLUMENTHAL, Connecticut
LAPHONZA BUTLER, California

RAND PAUL, Kentucky
RON JOHNSON, Wisconsin
JAMES LANKFORD, Oklahoma
MITT ROMNEY, Utah
RICK SCOTT, Florida
JOSH HAWLEY, Missouri
ROGER MARSHALL, Kansas

DAVID M. WEINBERG, *Staff Director*
CHRISTOPHER J. MULKINS, *Director of Homeland Security*
EMILY A, FERGUSON, *Professional Staff Member*
WILLIAM E. HENDERSON III, *Minority Staff Director*
CHRISTINA N. SALAZAR, *Minority Chief Counsel*
KENDAL B. TIGNER, *Minority Professional Staff Member*
LAURA W. KILBRIDE, *Chief Clerk*
ASHLEY A. GONZALEZ, *Hearing Clerk*

CONTENTS

WITNESSES

WEDNESDAY, JUNE 5, 2024

ALPHABETICAL LIST OF WITNESSES

APPENDIX

STREAMLINING THE FEDERAL CYBERSECURITY REGULATORY PROCESS: THE PATH TO HARMONIZATION

WEDNESDAY, JUNE 5, 2024

U.S. SENATE,
COMMITTEE ON HOMELAND SECURITY
AND GOVERNMENTAL AFFAIRS,
Washington, DC.

The Committee met, pursuant to notice, at 10 a.m., in room SD–342, Dirksen Senate Office Building, Hon. Gary Peters, Chair of the Committee, presiding.

Present: Senators Peters [presiding], Hassan, Rosen, Blumenthal, and Lankford.

OPENING STATEMENT OF SENATOR PETERS[1]

Chairman PETERS. The Committee will come to order.

Cybersecurity remains one of the greatest challenges facing our Nation. As we have become more reliant on technology and digital infrastructure, the threat of cyberattacks has dramatically increased. Every day, our citizens, our critical infrastructure operators, and our Federal, State, and local governments have to defend against hundreds of thousands of potential cyberattacks.

These come from criminals who take advantage of our vulnerable people, foreign actors who threaten our critical infrastructure, and hackers who try to destabilize American businesses. Cyberattacks are more coordinated and more dangerous than ever.

In response to this threat, American regulators have begun to set new standards for cybersecurity and digital safety. They have moved quickly in that work. In the last four years alone, Federal regulators have passed 48 rules on cybersecurity, more than 10 per year. That does not include new policies at the State as well as the local level.

This surge of regulations comes from a good place. It represents our government's response to a new and growing threat and has helped give American businesses some important guidance on how to keep safe from these cyber threats.

The challenge is that even though all aspects of our society are vulnerable to cyberattacks from electric grids to water systems to gas pipelines—no one, no one is coordinating this effort. This is a patchwork of new guidelines set by separate agencies. Regulators are working to respond to the unique challenges their sectors certainly face, and they are often not looking at the bigger picture of

[1] The prepared statement of Senator Peters appears in the Appendix on page 23.

how all of these different rules interact with each other. Without that higher level coordination, there is no way to ensure that these guidelines do not overlap, duplicate, or, quite simply, contradict each other.

The results are often confusing and inefficient. Businesses are scrambling to follow a web of new standards, ones that can change quickly with new technological innovations. Airlines have to adhere to three different regulators on cybersecurity. Railroads have six. A bank could have 16 different oversight bodies, all of whom are passing their own standards and expecting those standards to be followed. This is not necessarily a case where more is better. We must be smart in these regulations to ensure the higher level of cybersecurity.

In short, businesses and their employees are spending too many resources trying to understand these new guidelines. Companies are taking their cybersecurity professionals off the line to fill out paperwork, leaving their defenses undermanned and vulnerable.

We need effective regulations on cybersecurity, no question about that. But we need them to be efficient, adaptable, and coordinated all across different agencies. Harmonization and harmonizing these guidelines will make our government more efficient, help businesses compete on the global stage, and ensure that we are addressing cybersecurity threats in the most effective way. That is why I am working on legislation to establish a Harmonization Committee at Office of the National Cyber Director (ONCD) that would require all agencies and regulators to come together, talk about cybersecurity regulations, and work on harmonization.

Passing legislation is the only solution. We have to bring independent agencies together and start harmonizing this effort. Only Congress has the power to do so. If we fail at this mission, we will not be able to build the most effective response to cyber threats.

It is the practice of the Homeland Security and Governmental Affairs Committee (HSGAC) to swear in witnesses, so if each of you would please stand and raise your right hand.

Do you swear that the testimony that you will give before this Committee will be the truth, the whole truth, and nothing but the truth, so help you, God?

Mr. LEISERSON. I do.

Mr. HINCHMAN. I do.

Chairman PETERS. You may be seated. Thank you.

Our first witness, Nicholas Leiserson, is an Assistant National Cyber Director for Cyber Policy and Programs. He previously served as ONCD's Deputy Chief of Staff, and prior to joining ONCD, Nicholas spent more than a decade on the staff of Congressman James R. Langevin, principal author of the National Cyber Director Act.

Mr. Leiserson, you are now recognized for your opening comments.

TESTIMONY OF NICHOLAS LEISERSON,[1] ASSISTANT NATIONAL CYBER DIRECTOR FOR CYBER POLICY AND PROGRAMS, OFFICE OF THE NATIONAL CYBER DIRECTOR, EXECUTIVE OFFICE OF THE PRESIDENT

Mr. LEISERSON. Good morning, Chairman Peters and distinguished Senators of the Committee. Thank you for the opportunity to testify before you today.

Today's hearing is about a complex topic, how to set baseline cybersecurity requirements across critical infrastructure in a harmonized manner. It involves coordinating dozens of agencies, each implementing its own unique authorities. Yet, despite the complexity, our value proposition is simple. In a harmonized regulatory environment we will see better cybersecurity outcomes as we reduce the dollars that are going into regulatory compliance.

Pursuant to the National Cybersecurity Strategy (NCS) Implementation Plan, the Office of the National Cyber Director released a request for information last year about cybersecurity regulatory harmonization and reciprocity. ONCD received 86 unique responses to the request for information (RFI), covering 11 of 16 critical infrastructure sectors. In all, the respondents represent over 15,000 businesses, States, and other organizations.

We have analyzed the responses, and yesterday we released our summary of the more than 2,000 pages of comments we received. There are three key findings. First, the lack of harmonization and reciprocity harms cybersecurity outcomes while increasing compliance costs. Second, challenges with harmonization extend to businesses of all sectors and all sizes, and cross jurisdictional boundaries. Third, the United States government is positioned to act to address these challenges.

Let me share some of what we heard.

The Business Roundtable, a group of Chief Executive Officers (CEOs) whose companies support one in four American jobs, noted that, "Duplicative, conflicting, or unnecessary regulations require companies to devote more resources to fulfilling technical compliance requirements without improving cybersecurity outcomes."

The National Defense Industry Association (NDIA), whose more than 65,000 corporate and individual members comprise much of our defense industrial base, wrote, "Inconsistencies also pose barriers to entry, especially for small and midsized businesses that often have limited resources."

In some cases, respondents noted that Chief Information Security Officers (CISO) were spending 30 to 50 percent of their time not on security but on compliance activities.

ONCD leads the coordination of implementation of national cyber policy and strategy. In alignment with our mission, both the National Cybersecurity Strategy and the recent National Security Memorandum (NSM) on Critical Infrastructure assign ONCD the responsibility for coordinating cybersecurity regulatory harmonization across the government. Improving Federal coherence, in partnership with our interagency and private sector stakeholders, is at the core of our mission. Based on feedback from the RFI, ONCD has begun to build a pilot reciprocity framework. We antici-

[1] The prepared statement of Mr. Leiserson appears in the Appendix on page 25.

pate that this pilot will give us valuable insights as to how best achieve reciprocity when designing a cybersecurity regulatory approach from the ground up.

However, our vision cannot be fully achieved without help from Congress. As the United States Chamber of Commerce noted in its filing, "A significant challenge to U.S. regulatory harmonization efforts are independent regulatory agencies," and further, "The U.S. Chamber urges Congress to consider legislation to address this challenge."

The Administration supports Chair Peters' bill, consistent with the views previously provided to the Committee, that would allow ONCD to better carry out our mission by bringing independent regulatory commissions to the table together, with the interagency, in a policymaking process. This would act as a catalyst to develop a cross-sector framework for harmonization and reciprocity.

Such a framework is foundational to our desired end state, which would do three things: first, strengthen cybersecurity readiness and resilience across all sectors; second, simplify responsibilities of cyber regulators while enabling them to focus on their areas of expertise; and finally, substantially reduce the administrative burden and cost on regulated entities.

Mr. Chair, Members of the Committee, in closing, regulatory harmonization is a hard problem. It is a problem that has existed for decades. The trend line is generally heading toward more fragmentation, not more harmonization. It is a problem that requires leadership from ONCD and Congress, informed by the private sector. We have the opportunity to set the stage for a more harmonized future, and I hope we will do so together.

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

Chairman PETERS. Thank you. Thank you for your testimony.

Our next witness is David Hinchman. He is the Director of Information Technology and Cybersecurity at the U.S. Government Accountability Office (GAO). In that role, he oversees audits on critical infrastructure, the information technology (IT) and cybersecurity workforce, cloud computing, and the IT modernization efforts at the Internal Revenue Service (IRS). Prior to joining GAO in 2002, Mr. Hinchman worked as a business consultant for several private sector firms and served as a Surface Warfare officer in the United States Navy.

Mr. Hinchman, you are now recognized for your opening remarks.

TESTIMONY OF DAVID HINCHMAN,[1] DIRECTOR, INFORMATION TECHNOLOGY AND CYBERSECURITY, U.S. GOVERNMENT ACCOUNTABILITY OFFICE

Mr. HINCHMAN. Thank you. Chair Peters, Members of the Committee, thank you for inviting GAO to discuss our work on the Federal Government's efforts to harmonize cybersecurity regulations. Our nation increasingly depends on computer-based information systems and electronic data to execute fundamental operations and to process and maintain crucial information.

[1] The prepared statement of Mr. Hinchman appears in the Appendix on page 32.

Cyber-based intrusions and attacks on both Federal and non-Federal systems by malicious actors are becoming more common and more disruptive. These attacks threaten the continuity, confidence, and integrity of these essential systems, including those that support our nation's critical infrastructure. Never has there been a greater need to ensure that these vital systems have the appropriate direction and guidance needed to ensure their security.

Because the private sector owns the majority of this infrastructure, it is crucial that the public and private sectors work together to protect these assets and systems. However, when critical infrastructure sectors are subject to multiple regulations that grow and evolve in a decentralized manner, this can result in conflicting, inconsistent, or redundant requirements.

In recent years, interest in harmonizing these regulations has gained momentum, with several actions taken both by Congress and the Executive Branch. Today I would like to briefly summarize the findings of GAO's work in this area as well as share our current observations on ongoing efforts.

In legislation sponsored by this Committee, the 2022 Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA), addressed the need for standardized cyber incident reporting, in addition to incident reporting requirements that both deconflicted and harmonized. Additionally, the Administration specifically addressed harmonization as a core strategic objective in the 2023 National Cybersecurity Strategy. The Administration also addresses important information in a request for information published by the Office of the National Cyber Director, the organization that leads the Administration's harmonization efforts. This request for information sought to gather public comments on opportunities for and obstacles to harmonizing cyber regulations. Further, the April 2024 National Security Memorandum on Critical Infrastructure Security and Resilience called for an approach to harmonizing cyber regulations as part of a national plan for infrastructure risk management.

Taken together, these congressional executive actions provide an important starting point for the harmonization effort. However, GAO's past work and ongoing observations offer cautionary notes on the challenges that will be faced on this journey.

In February 2024, GAO reported that the ONCD's National Cyber Strategy did not define outcome-oriented performance measures. Our past work has consistently found, across the government, that well-defined performance measures allow for more accurate assessment of the extent to which an initiative, such as those found in the National Cyber Strategy, are achieving their stated objectives.

Without identifying appropriate outcome-oriented performance measures, ONCD may be limited in its ability to deliver the effectiveness of the national strategy and meeting its goals of better securing cyberspace and the nation's critical infrastructure.

Further, a 2023 Department of Homeland Security (DHS) report, required by CIRCIA, found 45 existing incident cyber reporting requirements across our nation's critical infrastructures. Among these 45 requirements, DHS found substantive differences such as varying definitions, differing report timelines, and inconsistent reporting mechanisms. Notably, this report looked at only one aspect of cyber regulations and still found these 45 applicable requirements. This serves as a stark reminder of how many regulations likely exist in the broader realm of general infrastructure cybersecurity and how much work will be required to harmonize those numerous requirements once they are identified.

In summary, given the increasing need for harmonized cyber regulations, it will be important for stakeholders in this vital process, representing both the Legislative and Executive Branches, to continue to work toward a common goal. It will also be crucial to develop definitive goals for this process based on both realistic timeframes as well as measurable performance.

This whole-of-government effort will require two things: one, a continued focus to ensure that performance goals are well defined and outcome oriented; and two, that the appropriate groundwork is laid to fully understand the universe of regulations to be harmonized. By taking these actions we can better position our nation's critical infrastructure to successfully defend itself against the growing and ever-present cybersecurity threat.

Mr. Chairman, this concludes my statement. Thank you.

Chairman PETERS. Thank you.

As both of you mentioned in your opening comments, and I mentioned in mine, we know that regulations are used by Federal agencies in multiple ways. I mentioned in my opening about making sure we have clean water to drink, protecting investors from predatory practices, and the list goes on.

Cybersecurity regulations have received a greater amount of attention given the growing threat of cyberattacks, which is not going down, and probably would argue exponentially going up, and on our critical infrastructure and Federal IT systems, which are a particular target.

Mr. Leiserson, why do cybersecurity regulations lend themselves generally to be a good candidate for harmonization all across these agencies? We need to do a lot of harmonization in a lot of fields, but why cybersecurity, in particular?

Mr. LEISERSON. Thank you, Mr. Chair. It is a great question. From our standpoint, the reason that we are particularly interested in looking at baseline cybersecurity requirements across critical infrastructure sectors is that the information and communications technology (ICT) That is used, whether you are in a bank, a nuclear power plant, a water treatment facility, the information and communications technology is largely the same, and the first thing that adversaries are trying to do when they get access, whether they are trying to steal money, drop ransomware, or potentially affect our ability to mobilize militarily, the first thing they are going after is these enterprise IT systems.

For that reason, because the enterprise IT systems are common across sectors, we really feel strongly that having a harmonized approach with reciprocity across different regulators will help ensure that we get both better cybersecurity outcomes and less money spent on compliance.

Chairman PETERS. Very good. Several public comments at ONCD's request for information on harmonization discuss the difficulties of understanding and implementing cybersecurity requirements, which I think leads to a compliance culture as opposed to dedicating resources to actually protecting our systems from cyberattacks.

Mr. Hinchman, this question is for you. How can regulators better tailor their requirements to promote cybersecurity rather than just a check-the-box exercise that only incrementally increases security but unfortunately does not move us forward, and in the process significantly increases the compliance burden while now moving us forward?

Mr. HINCHMAN. Thank you, Senator. I think one way to think of this, it is not a lot different from our duplication overlap and fragmentation work that we do for the Committee, which the Comptroller General (CG) was up here several weeks ago talking about. The idea of redundant, conflicting requirements is not different. It is on a much greater scale, and it is something that is national, and something that we are still struggling to understand the real breadth of.

But I think the general idea that because regulations have run patchwork here and there, specific sectors will pass rules because it is important to them, they are dealing with a certain threat, and then when you have organizations that work across sectors or across State lines or across international boundaries you run into a lot of things that they have to do in addition to what they may do with what I will call their home set of rules and regulations.

That compliance issue becomes a real cost burden, and some of the work that we have done, we did a job in 2020, looking at States, and dealing with four agencies—Federal Bureau of Investigation (FBI), IRS, Social Security Administration (SSA), and Centers for Medicare and Medicaid Services (CMS). Thirty five of the States reported a moderate to significant increase in costs related to the compliance that they had to do to meet the different regulations of each of those four agencies.

To remove that I think you need to look for a common framework. People have talked about whether the National Institute of Standards and Technology's (NIST) Cybersecurity Framework offers that possibility. But a common set of minimum standards that stretch across the government that can then be customized to meet the needs of individual sectors.

Chairman PETERS. Very good. As noted, Mr. Leiserson, in your opening statement, the Office of the National Cyber Director is designated as the Federal lead for addressing cybersecurity regulatory harmonization. My question for you, you have raised some of this, but to clarify for the Committee, what are the biggest challenges ONCD is now facing in harmonizing cyber regulations?

Mr. LEISERSON. Certainly, Mr. Chair. Thanks for the question. There are two things that I would highlight as the challenges. One is the breadth that we have here, where you see dozens of regulators who have dozens more regulations—you mentioned the 48 that we have seen just in the past four years—which means that from our perspective you really need a strategic approach, a top-down approach that says this is the framework that we are aiming at and gives that guidance to regulators.

But that gets into the second challenge. So the first challenge is the breadth of the problem and getting our hands around it, the second challenge is getting all of the relevant parties to the table. As I mentioned, from our perspective, the most important part of ensuring that we have a framework, that is applicable across sectors and does appropriately address the concerns that different regulators have, is to ensure all of them are participants in a policymaking process to design such a framework. But doing so at the moment we are limited in our ability to do so with respect to independent regulatory commissions, which is something that we truly need Congress' help with.

Chairman PETERS. Mr. Leiserson, again, you stated in your testimony that the Administration supports legislation that would require all agencies, including our independent regulatory agencies, to come up to the table, basically, and work on harmonizing their regulations with everybody else. My specific question for you, sir, is how would having this convening authority help the ONCD actually address this issue? What are going to be the strengths of getting this done?

Mr. LEISERSON. Thank you, Mr. Chair. It would help enormously, frankly, and it would help because right now when we want to talk to our independent regulatory commission partners, which we do as much as we can, we basically have a coalition of the wiling. We have the folks who want to come to the table, who believe that this is an important problem, and have a conversation about it. But having a clear mandate from Congress to bring everyone to the table will let us do what we do best at ONCD, which is listen to our partners, work with them to address the challenges, and as I say, design a comprehensive framework that allows for harmonization, yes, but just as importantly, reciprocity, the idea that once I have proven, as an entity, that I have met the requirements once, I do not need to do so, no matter how many other regulators are asking the same questions. That is what will allow us to both get better cybersecurity outcomes and, at the same time, reduce the burden on businesses.

Chairman PETERS. Great. Thank you.

Senator Hassan, you are recognized for your questions.

OPENING STATEMENT OF SENATOR HASSAN

Senator HASSAN. Thank you very much, Mr. Chair, and I appreciate you and the Ranking Member holding this hearing. I appreciate not only our witnesses being here today, but thank you and the teams you work with for the work you do.

Mr. Leiserson, I wanted to start with some questions about kind of where we are on certain issues. Recent cyberattacks, like the attack on Change Healthcare just a few months ago, have highlighted the impact that a cyberattack can have on critical services. In the Change Healthcare attack, we saw that an attack on a single major service provider could result in a really major disruption to the whole national health network.

What steps have your office, Cybersecurity and Infrastructure Security Agency (CISA), and the agencies overseeing different infrastructure sectors taken to identify potential single points of failure in critical infrastructure?

Mr. LEISERSON. Thank you, ma'am, for that question. It is one that actually is very important to our work in the Administration.

When I was on the Hill, I actually worked with the Cyberspace Solarium Commission (CSC), where we talked about systemically important critical infrastructure. if you look at the President's letter to Congress, delivering CISA's report on Section 9002 of the fiscal year (FY) 2021 National Defense Authorization Act (NDAA), in response to Congress' request, he specifically highlighted the fact that we need more policy on systemically important entities as a key goal of the policy process that we kicked off in November 2022.

That has produced this new National Security Memorandum, and right now sector risk management agencies are working to, within their sectors, identify exactly, as you describe, these critical points of failure, and then working with CISA as the national coordinator to help ensure that once we have them identified we can provision resources appropriately and ensure that we are appropriately managing that risk.

Senator HASSAN. Thank you for that. Another question for you. Effective implementation of cybersecurity laws requires a Federal workforce with the appropriate expertise and skills. What is the National Cyber Director doing to expand the Federal workforce of cybersecurity professionals so that government agencies have the expertise needed to safeguard our country's cybersecurity?

Mr. LEISERSON. Thank you, Senator. There are two things that I think I will highlight for this, something that is a key priority of National Cyber Director Harry Coker, Jr. The first is that we recognize that our regulatory partners need capacity building for cybersecurity regulations. We are talking about how we need harmonization. We also need to ensure they have the appropriate expertise. That is something that we, at the Office of the National Cyber Director, with our partners and the Office of Management and Budget (OMB), in our annual budget guidance that we provide to agencies, have specifically highlighted for the fiscal year 2025 budget as a key priority, that they are making investments in the personnel that they need in order to do their jobs effectively.

More broadly, one of the key goals of implementing the National Cyber Workforce and Education Strategy we released last year is both removing barriers and broadening pathways to entry. A key initiative we are focused on right now is skills-based hiring. It is removing the barrier of saying "if you have the appropriate skills to do a cybersecurity job, but you do not have a four-year college degree that should not be a barrier, in terms of your being able to join the Federal Government." At the end of April we announced that next year the 2210 Series, which is the largest series of Federal IT positions, the Office of Personnel Management (OPM) is working to ensure that all 2210's you can hire using a skills-based process, which we believe is incredibly important to getting the talent that we need into Federal jobs.

Senator HASSAN. That is really helpful, and please stay in touch if there are additional strategies that we can employ to help bring people in from the private sector to work for the Federal Government.

Mr. Hinchman, your written testimony discusses the need to harmonize cybersecurity requirements with national infrastructure risk management planning. Last year, I introduced bipartisan legislation with Senator Romney to codify the Department of Homeland Security's national risk management process. I am pleased to see that the White House's recent National Security Memorandum includes a requirement to implement part of our bill. The memorandum requires the Department of Homeland Security to develop a National Infrastructure Risk Management Plan and to update it periodically.

How could this plan improve cybersecurity across U.S. critical infrastructure, and how could the plan help harmonize current cybersecurity regulations?

Mr. HINCHMAN. I think that this plan is going to go a long way toward all of those things. The National Infrastructure Protection Plan (NIPP) was last updated in 2013. An update is desperately needed. The world has changed so much in the last 11 years, both in terms of technology, how it is used, as well as the threat we face on a daily basis. I think that the National Cyber Strategy's approach of building up from a risk management plan that starts at the sectors, very sector specific, makes them go out, understand what does their threat landscape look like, which then all come in to DHS, which then inform the development of the national plan, which is then submitted to the White House, is a very important first step for understanding what it is that we are facing and what we need to have out there so that we can ensure that individual sectors have the customized cybersecurity standards that they need, in addition to the national framework that is developed.

Senator HASSAN. As they have the customized cybersecurity infrastructure that they need, you are also able to identify things that they have in common, and as we are talking about harmonizing efforts, trying to make sure that the regulatory framework really is reflective of those specific needs.

Mr. HINCHMAN. Absolutely. I think the way I think of it right now is we do not yet understand what we do not know, and until that work is done and as these efforts, as Mr. Leiserson has been describing, that is all going to start to come together, and we are going to start to understand the landscape a lot better, and that is what is going to enable the really positive developments, like the framework, the customized specialties within sectors, as well as the commonalities that the sectors share, as you mentioned.

Senator HASSAN. OK. Thank you. One more question to you again, Mr. Hinchman. There are important reporting requirements for companies that are targeted by a cyberattack. For example, some companies must inform the Department of Homeland Security about cyberattacks on critical infrastructure. These reporting requirements provide the Federal Government with important information to prevent cyberattacks on other companies.

One way to improve reporting requirements is to streamline them across State and Federal levels which will help ensure that companies are aware of and able to fulfill their obligations. How is the Federal Government coordinating the efforts of various Federal agencies to streamline reporting requirements for cyberattacks?

Mr. HINCHMAN. I would argue that that effort is very much in its infancy. I think the press that you see every day about the U.S. Securities and Exchange Commission (SEC) rule that came out last year in addition to CISA's Notice of Proposed Rulemaking (NPR) has a lot of people very concerned about just what you mentioned. There is not that harmonization that is happening yet.

A lot of the small businesses are very scared that these reporting requirements will crush them under administrative burden. I think that there is some work still to be done to make sure that we are imposing the right requirements on the right organizations with the right threshold of burden.

There is going to be burden. We cannot get around that. But I think there needs to be sensitivity to what that burden is to different sized organizations.

Senator HASSAN. Thank you very much. Thank you, Mr. Chair.

Chairman PETERS. Thank you, Senator Hassan.

Mr. Leiserson, this next question will be for you. In July 2023, the Office of the National Cyber Director released a request for information on cybersecurity regulatory harmonization. The main theme of a lack of coordination amongst the regulators, particularly independent regulatory agencies such as the Securities and Exchange Commission, the Federal Communications Commission (FCC), the Federal Trade Commission (FTC) certainly stands out to me.

My question for you is how the ONCD incorporating the feedback from the RFI into their work?

Mr. LEISERSON. Thank you, Mr. Chair. The reason that we put out the RFI in the first place is absolutely that we rely on the input from all of our partners, both in the private sector and in the interagency, to inform our work.

There are a couple of things that I think really stood out to us in terms of the RFI and have crystallized how we are approaching our regulatory harmonization and reciprocity work going forward. One element, in particular, is the fact that reciprocity, which we had theorized should probably be part of the solution, was really highlighted in the RFI respondents as something that is absolutely critical to our getting this right. The focus on the compliance burden really points to the fact that, yes, you want a harmonized baseline because that gives you the simplicity, the clarity of understanding what specifically it is that you need to do. But you need the reciprocity to ensure that also translates into less compliance costs.

The other thing that I think I will highlight is the amount of focus on supply chain risk management and the fact that for a number of companies they are right now trying to figure out how do they manage risk in their supply chains, cyber risks that can come because there are either connections back into their networks or the fact that a disruption in their supply chain could materially impact their business. Having a harmonized framework would also help them do their own internal risk management processes, which I will admit was not something that we were really thinking through at the outset. Now we look and say, well, this actually could be a catalyst for businesses too. You may have regulation that actually helps them manage their own business risk by being able to look and say, oh, these folks have met the baseline standards. That helps us understand what their posture is for our own internal business focus supply chain risk management.

Chairman PETERS. Mr. Hinchman, in your testimony you highlighted that the Federal Government should adopt model definitions and consider setting minimum cybersecurity requirements. How do conflicting definitions and requirements contribute to the difficulties in overall compliance?

Mr. HINCHMAN. Any time that an organization is subject to multiple—the word of art is regime—reporting regime, you run into compliance burdens. We have done work in the financial sector where CISA, from financial services firms, has reported their folks spend 30 to 40 percent of their time on compliance rather than focusing on cybersecurity.

It gets back to the point I had initially made about duplication and overlap, that when you have multiple reporting regimes with multiple requirements that are not alike you spend a lot of time doing paperwork rather than focusing on your job, because you need to meet the requirements of both of these frameworks that you are subject to.

A single overarching framework, which is then customized as appropriate within a sector, ideally would remove a lot of that burden, so that there is a single point of reference that everyone starts from when thinking about cybersecurity in their organizations, and that includes reporting requirements, anything else.

Yet when we talk about reporting requirement there is a whole framework beyond that, identification management, protection of data, response recovery. I think it is really important that people be able to go to one place, know where that starts, and then figure out what they are required to do from there, so that you can streamline those compliance requirements. There will always be some compliance burden, as I mentioned a moment ago, but we can do a lot to streamline that and minimize it.

Chairman PETERS. Yes. Very good. Mr. Leiserson, to what extent has disharmonization of cyber regulations and compliance mechanisms actually impacted the ability of companies to compete internationally?

Mr. LEISERSON. Thank you, Mr. Chair. That has absolutely been something that we have heard, for a number of reasons, I would say. First and foremost, it can mean that companies need to invest in multiple systems. You are basically forcing them to duplicate some of their information and communications technology spend because they are subject to disharmonious regulatory regimes. When that is the case, if they are competing against a company in, say Europe, that is only operating under an European Union (EU) framework, they will be at a competitive disadvantage.

I think that really points to part of what we are hoping to get out of this effort. If we have a strong Federal framework for baseline cybersecurity requirements it is developed by all of the relevant parties in the interagency, including the independent regulatory commissions. That actually is very helpful for us in digital trade negotiations, in other export of American businesses, because we can then go forth and say, hey, now we are looking for mutual recognition with our international partners, and we can give folks an understanding of what exactly that means because we have a single framework to point to, whereas right now when you look at mutual recognition it is often challenging because we are pointing back to what we are doing, that is a kind of hodge-podge of different regulatory requirements.

Chairman PETERS. Thank you. Senator Lankford, you are recognized for your questions.

OPENING STATEMENT OF SENATOR LANKFORD

Senator LANKFORD. For my 19 minutes of questions?

Chairman PETERS. Your 19 minutes, yes. Senator Rosen is here. She will want you to be briefer.

Senator LANKFORD. It will be a little more brief than that. Thank you both. Thanks for the information and the background on it. I apologize I have had to run in and out through this hearing, as well.

You gave a stat earlier that I want to be able to drill down a little bit on it. You gave a stat that one of the business organizations said they spend 30 to 50 percent of their time not on security but on compliance.

Let's drill down on that a little bit. Do they give you information or do you have a sense of what that compliance is that could not be done so they could spend more time on security?

Mr. LEISERSON. Absolutely, Senator, and thanks very much for that question. That 30 to 50 percent number is for chief information security officers and their time. That was in response to our RFI last year. More recent testimony, actually, that was given in April, before the Committee on Homeland Security, said that when you look at CISA's teams' times, sometimes it is up to 70 percent. Seventy percent of the human capital that, in this case this is the financial services sector that had done this survey, 70 percent of their teams' time were spent on compliance activities.

The concern that I think we have is not that there should not be requirements. There absolutely must be. The financial services system, for instance, is absolutely vital to our economy, to our national security.

However, when you have time spent on developing reports, on responding to examiners' question, not in a standardized, harmonized way, that is a challenge. A further challenge is if another regulator then comes in, after you have just finished an examination with the first, the second regulator comes in and says, "Hey, yes, you have all of these reports that you have developed for the first, but we have a different opinion with respect to risk."

The Chair had asked earlier about why cybersecurity is particularly amenable to harmonization, and the reason is the risk that we are talking about here is the same. It is the same information systems.

That is really one of the challenges that we see out there any why we believe the approach here is so important.

Senator LANKFORD. What is the right percentage of time, do you think, to be able to do compliance? Because they are going to have to do some. You are right. But 70 percent is clearly not the right number on this, to try to get it down to that level. It is going to be just a ballpark. I get that.

Mr. LEISERSON. Yes. I am more of a cybersecurity guy, Senator, than a compliance guy, but I would be happy to take that back and get some sense. But 70 percent is not correct.

Senator LANKFORD. It is not correct. I will tell you, I met with some folks that were in rural health care yesterday, and nursing homes and skilled nursing. They are frustrated because their compliance requirements continue to go up. They are adding additional nurses, not to see patients but to fill out forms that are now being requested by CMS. It is the same issue here. They do not have the same issue of multiple regulators. They just have increased amount of compliance to be able to fill out forms. When you take nurses away from patients to be able to fill out forms you have got more forms but not more care.

We have the same situation, my fear is, and I know we have duplication, but we also have increased requirements to be able to do some of these completed forms to be able to turn in, for someone to be able to put in a drawer so that later, if there is a problem, they can show, yes, here is your problem. You did not fill out this form correctly, rather than helping them with compliance. That is my perspective on that, but that one I want to be able to push on.

I need to ask, though, why OMB does not already have the authority to do this? Obviously there is a lot of authority that OMB has, to be able to coordinate against all agencies. What is unique about this legislation that gives authority that OMB does not have right now?

Mr. LEISERSON. Senator, thanks very much for that question. I will say a couple of things. First of all, we are lockstep with the Office of Information and Regulatory Affairs (OIRA), at OMB. We work very closely with them.

Part of the challenge that they have is they do not have a gold standard that they can point to when it comes to Executive Branch regulators and say this is not harmonized with something, right. The challenge right now is you can come to a regulator and say, "This doesn't look like other regulations," but there is not a policy that says this is what good, baseline cybersecurity requirements, cross-sectorally for enterprise IT looks like. That is part of what we are trying to solve.

The other challenge, though, is the independent regulatory commissions, which we do not have the authority, neither OMB nor the Office of the National Cyber Director, to bring to the table to help design that framework. From our standpoint it needs to be an inclusive process. We need to hear from everyone in order to design something effectively, and that is something that, from the Administration's perspective, not just ONCD's, the Administration supports the approach that Chair Peters has laid out.

Senator LANKFORD. I am going to defer the time and actually be done earlier rather than later. That is shocking, I know, for everybody. But Chair Peters, this is an area we need to work on, the independent agencies, not just in this area but in a broader area. My perspective—and I am not going to force GAO to be able to make a comment about this—my perspective on this, there are independent agencies that feel like they are independent from everybody. They are not independent from everybody. They still need additional oversight. They still need to be able to go through the OIRA review. There are still some boundaries that need to be there when they are creating new regulations, that they are not a completely independent fourth branch of government, that they do need to have some kind of oversight.

This is something that I think we need to look at, not only in this area but in a broader area, in the days ahead, and the authority that this Committee has.

Chairman PETERS. I agree with you, and this is, I think, a very meaningful step. It will set an example of how we have to bring them together in a key area. But I am with you all the way, Senator, on that.

Senator Rosen, you are recognized for your questions early.

OPENING STATEMENT OF SENATOR ROSEN

Senator ROSEN. Thank you, and I am going to say, as a former software developer and systems analyst, I can tell you IT modernization can really help with compliance issues, it can streamline the process, and it can remove those duplicative reportings because it can see what you are doing. You should not have to, say, put this in this form. It should populate in all the forms, just like we use when we use our phone. I think there are a lot of things that can happen concurrently, not necessarily consecutively. There are a lot of ways that we can work on this, and I look forward to working on that, as well.

But I am going to talk about cyber incident trends, because implementing these Federal cybersecurity regulations, they really create large datasets of cyber incidents and information about the state of private sector cybersecurity. When this data is analyzed—like I said, I am a former analyst and software developer—the aggregated data, it can bolster the resilience of both the public and private sectors by identifying widespread vulnerabilities, malicious cyber campaigns, emerging threats, et cetera. It can also be used in other ways against people, as well, because you can de-aggregate the data, in some cases, so we have to be mindful of that.

But here, how are agencies collaborating, Mr. Leiserson, to leverage the cyber incident data to identify these trends and help us move forward faster to target the entities?

Mr. LEISERSON. Thank you, Senator, very much for that question. As a former programmer myself it is absolutely something that is of interest to us in conversations that we have been having as we work to implement the legislation that this Committee pushed forward, the Cyber Incident Reporting for Critical Infrastructure Act, to ensure that we are seeing exactly those gains in terms of an understanding of the cyber landscape.

One of the things that I remember General Alexander said from the beginning of his time at the National Security Agency (NSA), as the Director of NSA, was we need a common operating picture of what is going on in cyberspace. CIRCIA allows us to get there, but only if we are properly positioned to do the appropriate data analytics once we get there. I have had conversations with DHS's new Office of Statistics, Homeland Security Statistics, which has a cybersecurity program, about looking at exactly this challenge. I think it is one that as we move toward CIRCIA implementation in September 2025, we absolutely need to take advantage of what we can, from the broader analytics landscape, is also something we, at ONCD, in partnership with CISA and the Department of Treasury's Federal Insurance Office are working on for cyber insurance data, as well, because the insurers see a lot of these trends too.

Senator ROSEN. I think it is important that we share some of the data in smart ways so we are not in the silos, where maybe the insurance data sees one thing in some other ways electric companies see another, whatever that is. You are missing these common threads, as you know, if you are working as a programmer, as well.

Speaking of working as programmers, there is a workforce shortage—we know it—especially in the private sector, and there are currently nearly 470,000 cybersecurity jobs open in the United States, across the tech industry, even more. But compounding this challenge, cybersecurity teams, like I said, what James was saying, they really are spending too much time on compliance.

Do you want to add anything else about what he said about how we use our staff in smart ways, how we use artificial intelligence (AI), how we create easier reporting, and how do we populate data across to avoid those duplicative efforts? If there is any last thing you want to say about that, I would like that, and then what additional support you might need from us to help you do that.

Mr. LEISERSON. Thank you, Senator, for that question. It is a topic, the cyber workforce issue, is one that all of us at the Office of the National Cyber Director are passionate about and implementing the National Cyber Workforce and Education Strategy. I got into cyber policy personally because as a programmer, I did not get trained on secure software development whatsoever. I was in public policy classes and listening to my compatriots say, "Hey, we have all these concerns about cybersecurity." I looked at them and I was like, "I think I am the problem." [Laughter.]

It is absolutely a challenge that we see, I think. A lot of the work that we are doing on regulatory harmonization and reciprocity I would say is focused on actually reducing the demand side. As Senator Lankford mentioned, right, we are really interested in saying we want our cybersecurity personnel focused not on delivering reports to multiple regulators but instead focused on how are we going to actually secure systems. There are a lot of gains that we can see in terms of reduction on the demand side. That is still not going to deal with those 470,000 open jobs.

Senator ROSEN. That is right.

Mr. LEISERSON. The things that we are focused on right now at ONCD, in particular, are broadening pathways and removing barriers. I had mentioned earlier that we are doing a lot of work to ensure that skills-based hiring for the Federal Government is the way we look at things going forward. We are also looking to do that in contracts. That has been a major focus of ours is to say there should not be requirements in Federal contracts if you are going to provide IT support to the Federal Government, that you need to have any particular degree.

Senator ROSEN. That is right.

Mr. LEISERSON. That is a great way, from our perspective, to broaden the base that needs to come in.

Senator ROSEN. In addition to expanding the private sector workforce we know we have to implement the National Cybersecurity Strategy, like I said, adding trained personnel to so many agencies. Everybody needs it. Last Congress I was proud to lead, with Chair

Peters, the Federal Rotational Cybersecurity Workforce Program to help Federal agencies better enhance their cyber workforce.

Mr. Hinchman, which agencies that are required to oversee the implementation of Federal cybersecurity regulations themselves face significant cyber personnel shortages or training deficiencies, and what do you think we can help with?

Mr. HINCHMAN. Certainly. That is a big unknown right now, Senator. I do lead our IT and cyber workforce work at GAO. I will be doing the GAO mandate that is in your bill that was passed, that is due, I think, at the end of next year, after the program has had a time to get up and operate for a bit.

One of the things that the Federal Government really struggles with is not understanding what our cyber workforce looks like within Federal agencies. We have a job that we are doing under our broad Federal Information Security Modernization Act (FISMA) mandate for this Committee, that is looking at five of the largest consumers of cyber workforce and trying to understand how they are managing their workforce across the department, at the department level. We are finding that in terms of the general practices that need to be applied there is work that needs to be done.

There is also a job we are doing for Chairman Green at House Homeland Security, looking at the cost of the Federal cyber workforce, and that is going to be looking at all 24 Chief Financial Officers (CFO) Act agencies and comparing that cost versus how much is spent on cyber as a service, when you hire contractors to do your cybersecurity, as well as looking for initiatives that different agencies have to try to get Federal cyber workers into the workforce for us.

But overall, the government is really just now starting to try to understand what the Federal cyber workforce looks like. It is hard to answer where those holes are. I am looking forward to this work. It is exciting. I think it is going to be a body of work that is going to add a lot of value to this conversation the government is having because there is a lot that we need to be doing better to fill these cyber workforce gaps.

Senator ROSEN. If I had my way I would be down in every elementary school teaching all the fun things about robotics and computing and science, technology, engineering and mathematics (STEM) and logic, things I carry with me every single day, and show young folks the path forward and what great, exciting careers they are, and hopefully get them early and they get the bug—no pun intended—for software. But that would be my hope, to really invest in our young folks in bringing them along.

Thank you, Chair.

Chairman PETERS. Thank you, Senator Rosen. We appreciate your passion for that. Thank you so much.

Senator Blumenthal, you are recognized for your questions.

OPENING STATEMENT OF SENATOR BLUMENTHAL

Senator BLUMENTHAL. Thank you very much, Mr. Chair. Thank you both for your work. I think we are all becoming more and more aware of the need for standard setting and rules in this area of cyber. I think the general public is becoming more aware of it, as well, as we see the effects of ransomware throughout our economy and our society.

Just last February, as you well know, a ransomware group launched an attack on Change Healthcare, one of our nation's largest online health care claims and payments processors. We are still seeing the effects of it in Connecticut, and I think probably around the country.

Russia, China, Iran, and other foreign adversaries are targeting our critical infrastructure and probing for vulnerabilities for even more catastrophic attacks. Again, very recently, just this past Monday, the head of our cyber team, General Haugh, expressed his fears that China is, to use his word, "prepositioning" itself in our critical infrastructure. Essentially it is creating beachheads in case there is greater conflict between our countries. A really scary set of developments. We have already seen the immense costs and disruption of attacks not only change health care but Colonial Pipeline, Maersk, other major companies.

We have been warned. We need to treat this crisis like a national emergency. We need to give it the urgency that Americans should feel as a Nation, in effect, under attack. We should be ramping up our efforts to make sure that Russia and China cannot keep exploiting this critical infrastructure.

My question to both of you is, where are we falling behind on setting cybersecurity rules that counter these efforts by Russia and China, set the bar higher so that we are more invulnerable to their creating havoc?

Mr. LEISERSON. Senator, that is a very good point, and I really appreciate the question. Let me do a little bit of framing, I think, and then I will talk about some of the specific sectors and what we are up to and then why we think that regulatory harmonization will help.

On the framing side, I think we, at the Office of the National Cyber Director, could not agree more that this is something that the American people need to understand and know about. I have heard my boss, the National Cyber Director, Harry Coker, Jr., say he was so grateful for the opportunity to testify in January in front of the House about the Volt Typhoon activity. This is the People's Liberation Army and the People's Republic of China (PRC) targeting our critical infrastructure for exactly as General Haugh suggested, prepositioning, and the fact that that is putting America at unacceptable risk. It is unacceptable risk, and we need to take action as a government to address that risk.

One of the ways to do so is to put in place baseline cybersecurity requirements. I think what you have seen this Administration do leading on, in particular, the transportation sector, where we have emergency directives from the Transportation Security Administration (TSA). Those are turning into Notices of Proposed Rulemaking to solidify the significant gains that we have seen there. There was an Executive Order (EO) that the President signed out earlier this year giving the U.S. Coast Guard (USCG) additional authorities in the maritime sector. I think one of the areas that we are most interested in right now is seeing what we can do in the water and wastewater system sector, where there are still significant deficiencies and work that we need to do.

I think foundational to our approach at ONCD is knowing that we need to see better cybersecurity outcomes if we have a framework and we can say, across sectors, here is how you should be approaching securing your enterprise IT systems, which are what the adversaries are targeting to get that initial access, to set those beachheads, we will see better cybersecurity outcomes. In fact, you will be able to invest more in cybersecurity instead of in compliance. We will actually see better cybersecurity outcomes with a harmonized baseline.

That is why we are so focused on this at ONCD. We are a cyber office. Our concern is cybersecurity outcomes. When we see the amount of time and effort that is being spent on compliance from duplicative regulations that is not helping us get cybersecurity outcomes, and we need to have better ones.

Senator BLUMENTHAL. Thank you.

Mr. HINCHMAN. I would echo Mr. Leiserson's comments. The single cybersecurity framework is the important starting point, and I do not have much to add that he did not say. But I also think that Congress needs to consider expanding regulatory authority for some agencies in charge.

As I mentioned in my oral comments that the private and public sector have to work together in critical infrastructure, and in many cases we cannot compel private organizations to do certain things absent regulatory authority. That does not mean that we should be passing wholesale power out there, but very targeted specific, and the number of different plans have been put forward by the Administration talking about the need for those agencies to approach Congress with specific proposals for what they need to increase that.

I think to echo the water and wastewater thought, I have a review looking at cybersecurity in the water and wastewater sector that we are doing for two subcommittees on House Homeland Security. That is exactly the problem they ran into. This past fall there was a much publicized snafu that the Environmental Protection Agency (EPA) ran into trying to impose cybersecurity requirements through sort of a back door, because they did not want to go through the onerous rulemaking process. They were met with a lot of resistance, a number of lawsuits, both from States and organizations. They withdrew their requirements.

I think that there needs to be a different thinking about how we get the private sector to come along with these requirements once they are in place.

Senator BLUMENTHAL. Thank you. Thank you both for your work and your answers to those questions, and thank you, Mr. Chair, for having this hearing. There are a lot of multi-syllable words in the title to this hearing—harmonization, cybersecurity, regulatory—but it really is a matter of national security, and we need to pay attention more vigorously than we have done.

Thank you both. Thanks, Mr. Chair.

Chairman PETERS. Thank you, Senator Blumenthal.

A couple of final questions here for both of you. Federal agencies, as you know very well, are not the only agencies that have cybersecurity regulations. We have State regulations, local cities, other localities across the Nation have all sorts of requirements for businesses that operate in their areas.

I will give you a couple of examples. For example, Massachusetts State law requires all persons who own or license personal information about Massachusetts residents to develop, implement, and maintain a comprehensive information security program. The New York Department of Financial Services (DFS) has also adopted a robust set of cybersecurity rules with significant requirements for any company that provides a financial or credit service within the State of New York. I could just go on and on with that list.

Mr. Leiserson, how is the Federal Government working to coordinate with State, local, Tribal, territorial (SLTT) governments all across the government landscape to harmonize these regulations?

Mr. LEISERSON. Thank you, Mr. Chair. I will highlight a couple of points. First of all, both the New York Department of Financial Services and the State of New York responded to our RFI, our request for information, and one of the things that stood out to me was the fact that they really were asking for Federal leadership in this space. DFS and the State said having strong Federal guidelines, which a harmonized set of baseline requirements would do, would help them significantly in terms of how they would model their work. DFS, the Department of Financial Services, has worked with Federal regulators. It is something that we are concerned about. Again, like when we see duplicative requirements that are attempting to control the same risks, whether they are at the State level, at the Federal level, or the international level, that gives us pause.

But if we can get the Federal house in order, if we can set a strong Federal baseline requirement, if we can lead, we do have strong confidence that both our State governments will look at that as a gold standard and also start to move in that direction, and also our international partners.

One of the things that the National Cyber Director, Harry Coker, Jr., has consistently impressed upon me is in his conversations with international counterparts they bring up regulatory harmonization. They ask what is it that we are doing to help control risks to critical infrastructure, and they say, “Gee, it would be great to see Federal leadership here. We need the United States to help us understand. You have the most sophisticated tech sector. You have the most reliance on technology. If you can set a gold standard that would help us. That would give something for us to shoot for, as well.”

I think it really is incumbent upon us, in the Federal Government, partnering between the Administration and Congress, to set that standard.

Chairman PETERS. Mr. Hinchman, how does this contrasting Federal, State, local regulations, how does that impact businesses in our country?

Mr. HINCHMAN. I think very similar to the problems we have with just sort of Federal agencies. It is the multiple requirements and who do you need to do, and for what. I think the examples you drew are great.

I live in Texas. The Texas Department of Information Resources has an incident reporting rule that schools are required to follow in an attack. The CISA Notice of Proposed Rulemaking also includes schools. Now you are going to have schools that are trying to figure out how to do their local reporting as well as the national reporting, and these are organizations that traditionally do not have resources for this. They are already undermanned. IT is probably underfunded. In a small district you may have one person that does IT for the entire district, including the cyber side. I do not know that that is sustainable.

I think we really need to think about how those State and local rules are impacted by perhaps the Federal leadership that has been called for, so that they have more of a benchmark to follow. I think there are also things like privacy. States are increasingly passing privacy laws, which may be conflicting with guidance they are getting from the Federal level. How does a business operating manage both of those? It is similar to how sort the patchwork of Federal regulations has popped up, is the patchwork of State laws pop up, as well. That all needs to be managed and sort of brought into a common framework so that folks know who they are operating from and what the standards are.

Chairman PETERS. Very good. I want to thank both of our witnesses. Thank you for being here today and sharing your thoughts. Congress and the entire Federal Government must work together to harmonize our country's cybersecurity regulations. I think the testimony from both of you was very clear to that point, and it is, without question, a critical step in protecting both our citizens as well as our businesses from cyber threats.

I look forward to continuing to work together with both of you and others to strengthen cybersecurity standards and make sure that they are also coordinated, effective, and efficient and give our industries the guidance that they need.

The record for this hearing will remain open for 15 days, until 5 p.m. on June 20, 2024, for the submission of statements and questions for the record.

This hearing is now adjourned.

[Whereupon, at 11:05 a.m., the hearing was adjourned.]

APPENDIX

Chairman Peters Opening Statement As Prepared for Delivery
Full Committee Hearing: Cyber Regulatory Harmonization
June 5, 2024

The Committee will come to order.

Cybersecurity remains one of the greatest challenges facing our nation. As we have become more reliant on technology and digital infrastructure, the threat of cyberattacks has dramatically increased. Every day, our citizens, our critical infrastructure operators, and our federal, state, and local governments have to defend against hundreds of thousands of potential cyberattacks.

These come from criminals who take advantage of vulnerable people; foreign actors who threaten our critical infrastructure, and hackers who try to destabilize American businesses. Cyberattacks are more coordinated – and more dangerous – than ever.

In response to this threat, American regulators have begun to set new standards for cybersecurity and digital safety. They have moved quickly in that work. In the last four years alone, federal regulators have passed 48 rules on cybersecurity – more than 10 per year. And that doesn't include new policies at the state and local level.

This surge of regulations comes from a good place. It represents our government's response to a new and growing threat and has helped give American businesses some important guidance on how to keep safe from cyber threats.

The challenge is that even though all aspects of our society are vulnerable to cyberattacks – from electric grids to water systems to gas pipelines - no one is coordinating this effort. This is a patchwork of new guidelines set by separate agencies. Regulators are working to respond to the unique challenges their sectors face – and they are often not looking at the bigger picture of how all these rules interact. Without that higher level coordination, there is no way to ensure that these guidelines don't overlap, duplicate, or contradict each other.

The results are often confusing and inefficient. Businesses are scrambling to follow a web of new standards – ones that can change quickly with new technological innovations. Airlines have to adhere to three different regulators on cybersecurity. Railroads can have six. A bank could have *sixteen* different oversight bodies – all of whom are passing their own standards, expecting to be followed. This is not necessarily a case where more is better. We must be smart in these regulations to ensure the highest level of cybersecurity.

In short, businesses and their employees are spending too many resources trying to understand these new guidelines. Companies are taking their cybersecurity professionals off the line to fill out paperwork, leaving their defenses undermanned and vulnerable.

We need effective regulations on cybersecurity. But we need them to be efficient, adaptable, and coordinated across different agencies. Harmonizing these guidelines will make our government more efficient, help businesses compete on the global stage, and ensure that we're addressing cybersecurity threats in the most effective way. That is why I am working on legislation to establish a Harmonization Committee at O-N-C-D that would require all agencies and regulators to come together, talk about cybersecurity regulations, and work on harmonization.

Passing legislation is the only solution. We have to bring independent agencies together and start harmonizing this effort. Only Congress has the power to do so. If we fail at that mission, we won't be able to build the most effective response to cyber threats.

June 5, 2024

Testimony of Nick Leiserson

Assistant National Cyber Director for Cyber Policy and Programs

Office of the National Cyber Director

Executive Office of the President

10:00 A.M. EDT

United States Senate

Committee on Homeland Security and Governmental Affairs

Hearing on

"Streamlining the Federal Cybersecurity Regulatory Process: The Path to Harmonization"

Chairman Peters, Ranking Member Paul, and distinguished Senators of the Committee, thank you for the opportunity to testify before you today. The White House Office of the National Cyber Director (ONCD) is still a young organization. Thanks in part to the vision of this Committee, however, we are leaning in to tackle enduring cybersecurity challenges and better protect the nation.

One of these enduring challenges is the need to better harmonize Federal cybersecurity regulations. Since the Committee's last hearing on this topic in 2017, the digital interconnectedness of our society has only grown, as has the sophistication of threat actors in cyberspace. More regulators are stepping up to help manage the unacceptable level of risk that persists in many critical infrastructure sectors, and Congress has granted additional authorities to the government to impose minimum cybersecurity requirements. Yet, our efforts to confront cyber threats aggressively have not been anchored in a comprehensive policy framework for regulatory harmonization. In fact, many of the challenges raised in then-Chairman Johnson's hearing seven years ago continue to ring true.

The Administration is addressing these challenges. Both the National Cybersecurity Strategy (NCS) and the recently signed National Security Memorandum 22 (NSM-22) on "Critical Infrastructure Security and Resilience" prioritize cybersecurity regulatory harmonization. We have made this a priority – in fact, it is the first item in the inaugural National Cybersecurity Strategy Implementation Plan – because duplicative or contradictory cybersecurity regulations not only pose unnecessary costs on regulated entities, they also drain investment away from improvements in actual cybersecurity. By acting strategically, we can achieve better cybersecurity outcomes and lower costs to businesses and their customers.

As the Assistant National Cyber Director for Cyber Policy and Programs, I lead ONCD's regulatory harmonization work, in addition to our efforts to coordinate national cybersecurity policy related to implementation of the Strategy, critical infrastructure protection, cyber insurance, and other, similar topics. Today, I will describe for you ONCD's approach to this hard problem, which has been informed by the more than 80 responses to our request for information (RFI) last year. I will discuss the actions we are taking under the second version of the Implementation Plan, which we released last month. Most importantly, I will convey our hope that we can work closely with Congress to make meaningful progress on this important good government reform effort.

Cybersecurity Regulatory Harmonization & Reciprocity

When I talk about cybersecurity regulatory harmonization, I'm really talking about two concepts that go hand in hand: regulatory *harmonization* and regulatory *reciprocity*.

Cybersecurity regulatory *harmonization* refers to the use of a common set of requirements associated with cybersecurity or information security controls. Harmonization often occurs after efforts to *align* requirements, by ensuring that, when regulators are trying to control for the same type of risk, they are using a common taxonomy for risk management. For example, once there is *alignment* between regulations that certain systems require access controls, *harmonization* of those regulations would be agreeing on allowable forms of multi-factor authentication to access them.

A key focus of ONCD has also been the development of *reciprocity* or *mutual recognition* frameworks for regulations. *Reciprocity* would allow the findings of one regulator that an entity has met a harmonized requirement to meet the requirements of another. In other words, if one regulator found that a company's multifactor authentication was being appropriately used on an information system, another regulator would use the first regulator's finding – not their own, independent assessment – as the necessary proof that the company was complying. Reciprocity can drastically reduce the portion of compliance costs spent on administrative burdens[1] by allowing entities to demonstrate conformance to a regulation once and then reuse that finding for multiple regulators.

Congress has established numerous regulators, each with their own unique authorities, expertise, and responsibility to manage risk within their jurisdiction. Many companies are subject to multiple regulators, whether because parts of their business cross different regulatory authorities, or because they operate across jurisdictional lines (such as state, Federal, and international). While these regulations are rarely harmonized or have reciprocity between them, that is a result of the distinct equities each regulator is addressing. Banks and water treatment plants have different business, environmental, and national security regulations because the risks to each for those sectors are different.

But this all changes for cybersecurity regulations. Cybersecurity controls on information and communications technology (ICT) are unique in that, for many common enterprise ICTs, both the technology and the risk being managed are consistent across sectors. For both banks and water treatment plants, how we define and require access controls should be the same for each because the risk being addressed is the same: preventing unauthorized access. While there are certainly sector-specific technologies that need to be accounted for, business systems across sectors are more similar than different.

As I noted, both the NCS and NSM-22 highlight the importance of cybersecurity regulatory harmonization. This is driven, in part, by the Administration's recognition that we need minimum cybersecurity requirements for critical infrastructure. As National Cyber Director Harry Coker, Jr., testified in January:

> "Sharing situational awareness of [People's Republic of China (PRC)] threat actors – which itself is an objective of the Strategy – is necessary, but not sufficient to meet the magnitude of the threat posed by the PRC and other malicious actors. When it comes to matters of national security, there is a clear need for mandatory cybersecurity requirements to both mitigate risk and to level the playing field to ensure that companies that do make investments in cybersecurity are not disadvantaged in the marketplace."

The stakes are simply too high for us to maintain the regulatory status quo. At the same time, when setting requirements, we must be laser-focused on the outcomes we seek to achieve. Effective cybersecurity regulations minimize the cost and burden of compliance while

[1] Per the OECD: "Administrative burdens can be defined as the costs of complying with information obligations stemming from government regulation. Information obligations can be defined as regulatory obligations to provide information and data to the public sector or third parties." https://www.oecd-ilibrary.org/governance/oecd-regulatory-compliance-cost-assessment-guidance_9789264209657-en.

maximizing their cybersecurity risk reduction effect. Harmonization and reciprocity are key ways to do just that.

By statute, ONCD advises the President on cybersecurity policy and strategy related to the coordination of, among other things, programs and policies intended to improve the cybersecurity posture of the United States. ONCD leads the coordination of implementation of national cyber policy and strategy, including the NCS. Our statutory remit also extends to "the streamlining of Federal… regulations relating to cybersecurity."[2] In alignment with our mission, both the NCS and NSM-22 assign ONCD the responsibility for coordinating cybersecurity regulatory harmonization across the U.S. Government.[3]

ONCD's Efforts on Cybersecurity Regulatory Harmonization & Reciprocity

ONCD began addressing these challenges by developing a vision for regulatory harmonization and reciprocity to mitigate cyber risk. That vision was grounded in the National Cybersecurity Strategy, and included as principles:

1. Baseline cybersecurity requirements should be harmonized across sectors and regulators and should leverage existing cybersecurity frameworks, voluntary consensus standards, and guidance.
2. Proof of compliance with baseline requirements should be reciprocated across regulators.
3. Individual regulators should, when necessary, develop or retain and enforce sector-specific requirements that go beyond baseline requirements and are tailored to the unique risks within the sector that each regulator is charged with managing.

We posit that implementing these principles would produce an end-state that would: strengthen cybersecurity readiness and resilience across all sectors; simplify oversight and regulatory responsibilities of cyber regulators while enabling them to focus on areas of unique, sector-specific expertise; and substantially reduce the administrative burden and cost on regulated entities. These benefits would accrue to regulated companies, the broader public, and to regulators themselves:

- For regulated entities, harmonized and reciprocal cybersecurity oversight approaches would decrease the administrative burden tied to varying or redundant regulatory requirements for similar functions. Through eliminating differing requirements and duplicative examinations, regulated entities could instead devote those additional resources and effort to improving their cybersecurity posture.
- For the American people, the use of a common cybersecurity baseline with reciprocity would lead to the development of standardized tools or services, increasing compliance with the baseline while decreasing cybersecurity costs and helping drive the adoption of the baseline protections beyond regulated sectors. For instance, ICT services that were adapted to meet baseline cybersecurity requirements would be available in other contexts,

[2] Section 1752 of P.L. 116-283 (6 U.S.C. § 1500(c)(1)(C)).

[3] Pursuant to the *Cybersecurity Incident Reporting for Critical Infrastructure Act of 2022* (Division Y of P.L. 117-103), the Cyber Incident Reporting Council coordinates, deconflicts, and harmonizes Federal incident reporting requirements.

including to consumers or small and medium-sized businesses that are not in critical infrastructure sectors.

- For regulators, harmonization and reciprocity would reduce resources needed to perform oversight activities with respect to the common baseline (reciprocity would mean that regulators could divide the waterfront and not examine every control) and provide an opportunity to focus oversight on their key concerns and areas of greatest expertise. By avoiding duplication of effort, regulators would have more time and resources to devote to their individual oversight or supervisory responsibilities.

Pursuant to the National Cybersecurity Strategy Implementation Plan, ONCD began to explore a framework for reciprocity for baseline requirements in conjunction with interagency partners that participate in the Cybersecurity Forum for Independent and Executive Branch Regulators (Cybersecurity Forum). We also released an RFI intended to gather input from industry, civil society, academia, and other government partners about our approach.[4]

Analysis of the RFI Responses

ONCD received 86 unique responses to the RFI, representing 11 of the 16 critical infrastructure sectors, as well as trade associations, nonprofits, and research organizations. In all, the respondents, many of which are membership organizations, represent over 15,000 businesses, states, and other organizations.

Respondents overwhelmingly agreed that the lack of cybersecurity regulatory harmonization and reciprocity posed a challenge to both cybersecurity outcomes and to business competitiveness. For instance, the Business Roundtable, an association of more than 200 chief executive officers of America's leading companies, noted that: "Duplicative, conflicting, or unnecessary regulations require companies to **devote more resources to fulfilling technical compliance requirements without improving cybersecurity outcomes** [emphasis added]." These sentiments were shared across sectors and for businesses of all sizes. The National Defense Industry Association, representing nearly 1,750 corporate members as well as 65,000 individual members from small and mid-sized contractors, highlighted: "Inconsistencies also pose barriers to entry, **especially for small and mid-sized businesses** [emphasis added] that often have limited resources available to establish multiple compliance schemes."

Respondents raised concerns not only about a lack of harmonization and reciprocity across Federal agencies, but also between state and Federal regulators and across international borders. Many lamented a lack of reciprocity to date, noting that investments in compliance across multiple regulatory regimes intended to control the same risk resulted in a net reduction in actual programmatic cybersecurity spending. The Financial Services Sector Coordinating Council highlighted that many sector chief information security officers report spending 30 to upwards of 50 percent of their time on regulatory compliance.

In describing the characteristics of a more harmonized and reciprocal cybersecurity regulatory landscape, RFI respondents touched on themes very similar to ONCD's initial vision:

[4] https://www.federalregister.gov/documents/2023/08/16/2023-17424/request-for-information-on-cyber-regulatory-harmonization-request-for-information-opportunities-for.

- Regulators should continue to focus on aligning to risk management approaches like the National Institute of Standard and Technology (NIST) Cybersecurity Framework.
- Coordinating among regulators to decrease overlapping requirements and collaborating with key allies (such as the United Kingdom, European Union, Canada, and Australia) to drive international reciprocity would materially improve the status quo.
- Elevating the importance of supply chain security would help ensure ICT vendors are held to the same standards as critical infrastructure operators.
- Providing Federal leadership would be essential to achieve these goals and to guide state, local, Tribal, and territorial (SLTT) governments to streamline related regulations.

These themes are consistent with our approach, especially the focus on baseline Federal ICT requirements as a first step with the ultimate goal of reciprocity or mutual recognition with SLTT and international governments, led by the U.S. Government.

Next Steps

Based on feedback from the RFI, ONCD has begun to build a pilot reciprocity framework to be used in a critical infrastructure subsector.[5] We anticipate that this pilot, which we expect to complete early next year, will give us valuable insights as to how best to achieve reciprocity when designing a cybersecurity regulatory approach from the ground up. We are also working with the Cybersecurity Forum to move from alignment to harmonization with respect to certain common cybersecurity controls. These initiatives continue to lay the foundation for more comprehensive efforts to knit dozens of regulatory regimes together.

ONCD's current work is grounded in our vision for regulatory harmonization and reciprocity, and critically informed by the RFI responses. However, this vision, shared by many RFI respondents, cannot be fully achieved without congressional action. As the United States Chamber of Commerce recommended in its filing:

> "A significant challenge to U.S. regulatory harmonization efforts are independent regulatory agencies. The U.S. Chamber respects the independent status of these agencies, and their role in protecting consumers, consistent with the authorities and responsibilities Congress has delegated to each agency. However, efforts at creating a cohesive and comprehensive cybersecurity framework would fall short should independent agencies not be included in future planning. In consultation with industry and the Administration, the **U.S. Chamber urges Congress to consider legislation to address this challenge** [emphasis added]."

The Administration supports Chairman Peters's legislation – consistent with the views previously provided to the Committee – that would allow ONCD to better carry out our mission by bringing independent regulatory commissions to the table in a policymaking process, which

[5] Initiative 1.1.5 in the National Cybersecurity Strategy Implementation Plan Version Two states: "The Office of the National Cyber Director (ONCD), working with regulatory departments and agencies (including through the Cybersecurity Forum for Independent and Executive Branch Regulators) and building on findings from its regulatory harmonization request for information, will explore one or more regulatory harmonization and reciprocity pilot programs to establish baseline cybersecurity requirements that model approaches to harmonization and reciprocity."

would act as a catalyst to develop a cross-sector framework more quickly for harmonization and reciprocity. While our current work is piloting a reciprocity framework, our authorities to test harmonization and reciprocity more broadly are limited. Chairman Peters's bill also helpfully includes a limited-scope pilot authority which would allow us, with the consent of a regulated entity, to quickly implement proposals and see if they reduce administrative costs while producing the same (or better) cybersecurity outcomes. We look forward to continuing the dialogue with this Committee and your counterparts in the House to advance this important legislation.

We will also continue to work closely with our partners at the Department of Homeland Security and the Cybersecurity and Infrastructure Security Agency (CISA) as they implement the *Cybersecurity Incident Reporting for Critical Infrastructure Act of 2022*. This Committee provided a novel mechanism to achieve reciprocity for incident reporting in the statute and established the Cyber Incident Reporting Council (CIRC) to harmonize incident reporting regulations. We are committed to helping our partners develop these reciprocity agreements over the next year to minimize duplicative reporting once CISA's final rule goes into effect, and to supporting the CIRC's efforts. We will also continue to work with NIST as they further use of the Cybersecurity Framework 2.0 to be used with international standards and to implement regulatory requirements.

Conclusion

Cybersecurity regulatory harmonization is a problem only government can solve. It means changing how we think about and implement regulations and achieving better cybersecurity outcomes with fewer compliance dollars. By applying more effort on the front end to design strategic regulatory regimes, we can address fundamentally cross-sector cybersecurity risk in a cross-sector – and not siloed – manner.

Regulatory harmonization is a hard problem. It involves coordinating dozens of agencies, each implementing its own unique authorities. It is a problem that has existed for decades – and the trend line is generally heading toward more fragmentation, not more harmonization. National Cyber Director Harry Coker, Jr., has remarked that solving hard problems is why ONCD exists. Given our focus on Federal coherence, regulatory harmonization has been and will remain an ONCD priority.

Finally, cybersecurity regulatory harmonization is a joint problem. It affects all levels – and all branches – of government. It affects regulated entities of all sizes across the country. It requires leadership from the Administration and Congress, informed by the private sector, to together improve our national cybersecurity posture while reducing regulatory burdens.

That national leadership is urgently needed. In meetings with our international counterparts, ONCD personnel, including the Director, have heard that the world is waiting to see where the United States goes next in how it manages cybersecurity risk. They will not wait indefinitely. We have the opportunity to set the stage for more harmonized future, and I hope we will do so, together.

United States Government Accountability Office

GAO

Testimony

Before the Committee on Homeland Security and Governmental Affairs, U.S. Senate

For Release on Delivery
Expected at 10:00 a.m. ET
Wednesday, June 5, 2024

CYBERSECURITY

Efforts Initiated to Harmonize Regulations, but Significant Work Remains

Statement of David B. Hinchman,
Director, Information Technology and Cybersecurity

GAO Highlights

Highlights of GAO-24-107602, a testimony before the Committee on Homeland Security and Governmental Affairs, U.S. Senate

Why GAO Did This Study

Cyber-based intrusions and attacks on both federal and nonfederal systems by malicious actors are becoming more common and more disruptive. These attacks threaten the continuity, confidence, integrity, and accountability of essential systems. Moreover, the risks to these systems—including insider threats from witting or unwitting employees, mounting threats from around the globe, and the rise of new and more destructive attacks—collectively threaten to compromise sensitive data and destabilize critical operations.

GAO initially identified cybersecurity as a High-Risk area in 1997 and expanded it in 2003 to include critical infrastructure cybersecurity. Due to the persistent threat and need for urgent action, GAO continues to view the area as high risk.

Because the private sector owns most of the nation's critical infrastructure, it is vital that the public and private sectors work together to protect these assets and systems. However, according to ONCD, when critical infrastructure sectors are subject to multiple cybersecurity regulations, the result can be conflicting guidance, inconsistencies, and redundancies.

GAO was asked to testify on harmonizing cybersecurity regulations. This testimony summarizes the Administration's current efforts to address cybersecurity regulatory harmonization.

This statement is based on prior GAO reports and public information, as of May 2024, regarding the Administration's plans to harmonize regulations.

View GAO-24-107602. For more information, contact David B. Hinchman at (214) 777-5719 or HinchmanD@gao.gov.

June 5, 2024

CYBERSECURITY

Efforts Initiated to Harmonize Regulations, but Significant Work Remains

What GAO Found

Harmonization refers to the development and adoption of more consistent standards and regulations. Such consistency is important when critical infrastructure sectors are subject to multiple cybersecurity regulations. According to the White House, harmonizing regulatory requirements can lead to better security outcomes at lower costs.

Without harmonization, adverse impacts can occur. For example, GAO reported in 2020 that four federal agencies had established cybersecurity requirements for states to follow in securing data. However, these requirements had conflicting parameters such as the number of unsuccessful log-on attempts prior to locking out users. The percentage of total requirements with conflicting parameters ranged from 49 percent to 79 percent. Slightly more than half of state officials surveyed said that such requirements led to a great increase or very great increase in the time and staff hours needed to address the conflicts. GAO made 12 recommendations to agencies; eight of them are implemented and four are not including two priority ones to the Office of Management and Budget to ensure agencies collaborate on requirements and state cybersecurity assessments.

Recognizing the importance of harmonizing cybersecurity regulations for our nation's critical infrastructure sectors, the Administration and Congress have begun relevant initiatives.

- **National cybersecurity strategy and implementation plan.** In March 2023 and July 2023, respectively, the White House released the National Cybersecurity Strategy and an accompanying implementation plan. Among other things, the strategy and implementation plan identified the need to establish an initiative on cyber regulatory harmonization but did not provide a time frame for completing subsequent actions to harmonize regulations.
- **Request for information on cybersecurity regulation harmonization.** In August 2023, the Office of the National Cyber Director (ONCD) issued a request for information seeking input on challenges with cybersecurity regulatory overlap and received over 100 public comments. ONCD has not published a summary of the comments.
- **National security memorandum on critical infrastructure security and resilience.** In April 2024, the Administration released *National Security Memorandum-22 on Critical Infrastructure Security and Resilience*. The memorandum calls for the Department of Homeland Security (DHS) to develop a plan to harmonize cybersecurity regulations as part of a national plan for infrastructure risk management, which is to be issued by April 2025.
- **Cyber incident reporting legislation.** The Cyber Incident Reporting for Critical Infrastructure Act was enacted in 2022 to help prioritize efforts to combat cyber threats by requiring certain entities to submit cyber incident reports to DHS. Pursuant to the act, in September 2023, DHS issued a report with eight recommendations and three proposed legislative changes to streamline and harmonize cyber incident reporting.

These key initial steps can inform the broader effort to harmonize cybersecurity regulations. Following through and executing specific plans and meeting established time frames are essential to achieving harmonization.

Chairman Peters, Ranking Member Paul, and Members of the Committee:

Thank you for the opportunity to discuss our work on the cybersecurity challenges that are impacting our nation's critical infrastructure. Our nation increasingly depends on computer-based information systems and electronic data to execute fundamental operations and to process, maintain, and report crucial information. Further, nearly all federal and nonfederal operations, including the nation's critical infrastructure, are supported by these systems and data.[1] Consequently, the safety of these systems and data is critical to public confidence and the nation's security, success, and welfare.

However, cyber-based intrusions and attacks on both federal and nonfederal systems by malicious actors are becoming more common and more disruptive. These attacks threaten the continuity, confidence, integrity, and accountability of these essential systems. Moreover, the risks to these systems—including insider threats from witting or unwitting employees, mounting threats from around the globe, and the rise of new and more destructive attacks—collectively threaten to compromise sensitive data and destabilize critical operations.

Because the private sector owns the majority of the nation's critical infrastructure, it is vital that the public and private sectors work together to protect these assets and systems. Toward this end, various federal agencies are responsible for assisting the private sector in protecting critical infrastructure, including enhancing cybersecurity. However, according to the Office of the National Cyber Director (ONCD), when critical infrastructure sectors are subject to multiple cybersecurity regulations, this can result in conflicting guidance, inconsistencies, and redundancies.[2] According to the White House, harmonizing regulatory

[1] The term "critical infrastructure" as defined in the Critical Infrastructures Protection Act of 2001 refers to systems and assets, whether physical or virtual, so vital to the United States that their incapacity or destruction would have a debilitating impact on security, national economic security, national public health or safety, or any combination of these. 42 U.S.C. § 5195c(e). Federal policy identifies 16 critical infrastructures: chemical; commercial facilities; communications; critical manufacturing; dams; defense industrial base; emergency services; energy; financial services; food and agriculture; government facilities; health care and public health; information technology; nuclear reactors, materials, and waste; transportation systems; and water and wastewater systems.

[2] Request for Information on Cyber Regulatory Harmonization; Request for Information: Opportunities for and Obstacles To Harmonizing Cybersecurity Regulations, 88 Fed. Reg. 55,694 (Aug. 16, 2023).

requirements can lead to better security outcomes at lower costs. The Administration has recently taken initial steps towards harmonizing and streamlining cybersecurity regulations to help address such concerns.

My statement today will discuss our past reporting and the Administration's recent work to harmonize cybersecurity regulations. To review the status of these efforts, we relied on prior GAO reports and public information, as of May 2024, regarding the Administration's harmonization plans and the impact of those plans on improving the nation's cybersecurity.

We conducted the work on which this statement is based in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

Background

GAO has identified cybersecurity as a government-wide high-risk area for more than 25 years. Recognizing a growing threat, we first designated information security as a government-wide high-risk area in 1997. Subsequently in 2003, we expanded the information security high-risk area to include the cybersecurity of critical infrastructure. We further expanded this high-risk area in 2015 to include protecting the privacy of personally identifiable information.[3]

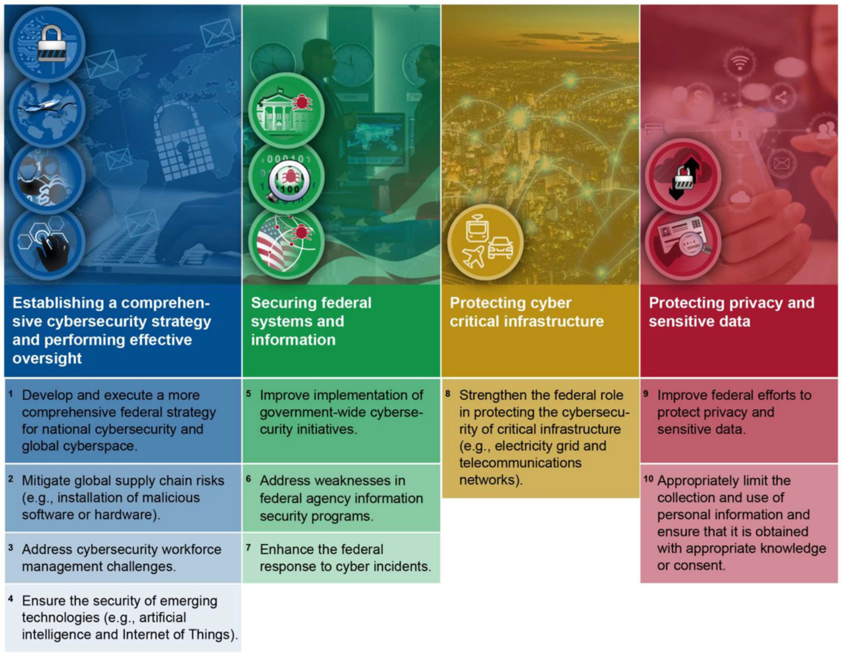
In September 2018, as part of our High-Risk Series, we identified four major cybersecurity challenges and 10 critical actions that the federal government and other entities need to take to address those challenges.[4] The major challenges are: (1) establishing a comprehensive cybersecurity strategy and performing effective oversight, (2) securing federal systems and information, (3) protecting cybersecurity of critical infrastructure, and (4) protecting privacy and sensitive data. Figure 1 provides an overview of

[3] In general, personally identifiable information is any information that can be used to distinguish or trace an individual's identity, such as name, date or place of birth, and Social Security number; or that otherwise can be linked to an individual.

[4] GAO, *High-Risk Series: Urgent Actions Are Needed to Address Cybersecurity Challenges Facing the Nation*, GAO-18-622 (Washington, D.C.: Sept. 6, 2018).

the major challenges and the critical actions needed to address these challenges.

Figure 1: Four Major Cybersecurity Challenges and 10 Associated Critical Actions



Establishing a comprehensive cybersecurity strategy and performing effective oversight

1 Develop and execute a more comprehensive federal strategy for national cybersecurity and global cyberspace.

2 Mitigate global supply chain risks (e.g., installation of malicious software or hardware).

3 Address cybersecurity workforce management challenges.

4 Ensure the security of emerging technologies (e.g., artificial intelligence and Internet of Things).

Securing federal systems and information

5 Improve implementation of government-wide cybersecurity initiatives.

6 Address weaknesses in federal agency information security programs.

7 Enhance the federal response to cyber incidents.

Protecting cyber critical infrastructure

8 Strengthen the federal role in protecting the cybersecurity of critical infrastructure (e.g., electricity grid and telecommunications networks).

Protecting privacy and sensitive data

9 Improve federal efforts to protect privacy and sensitive data.

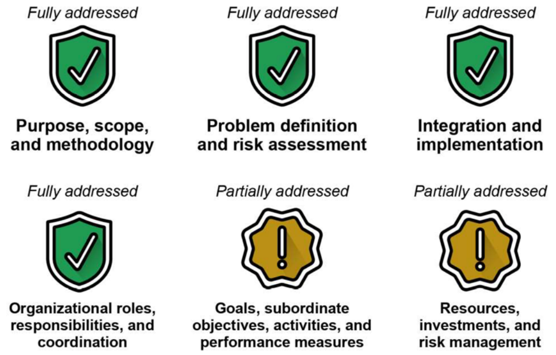
10 Appropriately limit the collection and use of personal information and ensure that it is obtained with appropriate knowledge or consent.

Sources: GAO (analysis and icons), Who is Danny (blue image); Gorodenkoff/stock.adobe.com (green image); metamorworks/stock.adobe.com (yellow image); Monster Ztudio/stock.adobe.com (red image); motorama/stock.adobe.com (icons); https://www.whitehouse.gov (logo). | GAO-24-107602

In our most recent update on this high-risk area in April 2023, we reiterated that fully establishing and implementing a national cybersecurity strategy was needed to protect the nation's information systems and infrastructure.[5] We plan to further update this important area in the summer of 2024.

More recently, we reported on the Administration's efforts to establish and implement the National Cybersecurity Strategy.[6] Specifically, in February 2024 we found that that the strategy and its July 2023 implementation plan fully addressed four of six desirable characteristics of a national strategy, as identified in our prior work, and partially addressed the other two (see fig. 2).

Figure 2: Extent to Which the March 2023 National Cybersecurity Strategy and July 2023 Implementation Plan Addressed GAO's Desirable Characteristics of a National Strategy


Fully addressed
Purpose, scope, and methodology
Fully addressed
Problem definition and risk assessment
Fully addressed
Integration and implementation
Fully addressed
Organizational roles, responsibilities, and coordination
Partially addressed
Goals, subordinate objectives, activities, and performance measures
Partially addressed
Resources, investments, and risk management

Sources: GAO (analysis and yellow icon); YEVHENIIA/stock.adobe.com (green icon). | GAO-24-107602

[5] GAO, *High-Risk Series: Efforts Made to Achieve Progress Need to Be Maintained and Expanded to Fully Address All Areas*, GAO-23-106203 (Washington, D.C.: Apr. 20, 2023).

[6] GAO, *Cybersecurity: National Cyber Director Needs to Take Additional Actions to Implement an Effective Strategy*, GAO-24-106916 (Washington, D.C.: Feb. 1, 2024).

For the partially addressed characteristics, the strategy and its implementation plan did not describe:

- *Outcome-oriented performance measures* that assess the extent to which initiatives are achieving outcome-oriented objectives, such as improving information sharing or modernizing federal agency defenses. ONCD staff said it was not yet realistic to develop outcome-oriented measures, because such measures did not currently exist in the cybersecurity field in general. However, we believe it is feasible to develop such measures where applicable. For example, regarding the key initiative of disrupting ransomware attempts, the Department of the Treasury already collects information on the number and dollar value of ransomware-related incidents—for 2021 the reported total dollar value was about $886 million. This demonstrates that developing such measures is feasible and can be used for measuring effectiveness.
- *Resources and estimated costs* associated with the strategy, such as budgetary, human capital, IT, research/development, and contracts. While the implementation plan outlined initiatives that require executive visibility and interagency coordination, it did not identify how much it will cost to implement the initiatives. ONCD staff said estimating the cost to implement the entire strategy was unrealistic. However, while certain initiatives may not warrant a specific cost estimate, other activities supporting some of the key initiatives with potentially significant costs justify the development of a cost estimate. Such cost estimates are essential to effectively managing programs.

We concluded that without actions to address these shortcomings, ONCD will likely lack information on plan outcomes and encounter uncertainty on funding of activities. Consequently, we made two recommendations to ONCD to (1) assess initiatives that lend themselves to outcome-oriented measures and develop such performance measures for these initiatives and (2) estimate the costs of implementation activities. ONCD partially agreed with our finding on outcome-oriented measures and agreed with the related recommendation to assess the initiatives to identify those that warrant outcome-oriented performance measures. ONCD disagreed with our finding and associated recommendation that the strategy and implementation plan did not include specific details on the estimated cost of the plan's initiatives. Both of these recommendations remain open.

In addition, over the past few years, we have issued numerous reports that identified concerns resulting from varying cybersecurity requirements and the implementation of those requirements. For example:

- In February 2018, we reported on what was known about the extent to which critical infrastructure sectors had adopted the National Institute of Standards and Technology's (NIST) Framework for Improving Critical Infrastructure Cybersecurity.[7] We found that most of the 16 critical infrastructure sectors took action to facilitate adoption of the framework. In addition, 12 of the 16 sectors developed guidance for implementing the framework. Nevertheless, we reported that federal and nonfederal officials identified four challenges to framework adoption.

  Specifically, some entities may face regulatory, industry, and other requirements that could inhibit their adoption of the framework. We made nine priority recommendations that methods be developed for determining framework adoption by sector risk management agencies across their respective sectors, in consultation with their respective partners, as appropriate. Five agencies agreed with the recommendations, while four others neither agreed nor disagreed. Of the nine recommendations, three remain open.

- In August 2019, we identified that the Federal Energy Regulatory Commission's approved standards did not fully address NIST cybersecurity framework guidance for improving critical infrastructure cybersecurity.[8] We recommended that the Federal Energy Regulatory Commission consider our assessment and determine whether to direct the North American Electric Reliability Corporation to adopt any changes to its cybersecurity standards to ensure those standards more fully address the NIST cybersecurity framework and address current and projected risks. The Federal Energy Regulatory Commission agreed with our recommendation and planned to conduct a technical analysis and develop a plan to address it. Our recommendation to the Federal Energy Regulatory Commission remains open.

- In May 2020 we identified adverse impacts that varying cybersecurity requirements issued by four selected federal agencies had on state government agencies.[9] Each of four federal agencies had established cybersecurity requirements for states to follow in securing data.

[7] GAO, *Critical Infrastructure Protection: Additional Actions Are Essential for Assessing Cybersecurity Framework Adoption*, GAO-18-211 (Washington, D.C.: Feb. 15, 2018).

[8] GAO, *Critical Infrastructure Protection: Actions Needed to Address Significant Cybersecurity Risks Facing the Electric Grid*, GAO-19-332 (Washington, D.C.: Aug. 26, 2019).

[9] GAO, *Cybersecurity: Selected Federal Agencies Need to Coordinate on Requirements and Assessments of States*, GAO-20-123 (Washington, D.C.: May 27, 2020).

However, these requirements had conflicting parameters that involved agencies defining specific values. Examples of conflicting parameters included the number of consecutive unsuccessful logon attempts prior to locking out users, the time to retain audit logs related to audited events, the frequency of security controls assessments, and the frequency of scans for system vulnerabilities. The percentage of total requirements with conflicting parameters ranged from 49 percent to 79 percent.

Our review found that state agency officials required to comply with multiple federal agencies' cybersecurity requirements (and related compliance assessments) viewed variances in these requirements as problematic and burdensome. Slightly more than half of state officials surveyed said that such requirements led to a great increase or very great increase in the time and staff hours needed to address the conflicts. We made 12 recommendations to agencies; eight of them are implemented and four are not, including two priority ones to the Office of Management and Budget to ensure agencies collaborate on requirements and state cybersecurity assessments.

- In September 2020 we reported about federal and nonfederal steps to enhance the security and resilience of the U.S. financial services sector.[10] However, we found that Treasury, as the designated lead agency for the financial sector, did not track efforts or prioritize them according to goals established by the sector. We made recommendations to Treasury to track and prioritize the sector's cyber risk mitigation efforts, and to update the sector's plan with metrics for measuring progress and information on how sector efforts will meet sector goals and requirements. While Treasury generally agreed with the recommendations, these recommendations remain open.

  Of note, selected financial firms identified the need for further assistance in improving harmonization among regulatory requirements. For example, four firms mentioned the difficulty of following differing state breach notification requirements, as compared to following one national requirement.

[10] GAO, *Critical Infrastructure Protection: Treasury Needs to Improve Tracking of Financial Sector Cybersecurity Risk Mitigation Efforts*, GAO-20-631 (Washington, D.C.: Sept. 17, 2020).

The Administration Initiated Actions to Harmonize Cybersecurity Regulations, but Significant Work Remains

Harmonization refers to the development and adoption of more consistent standards and regulations. Such consistency is important when critical infrastructure sectors are subject to multiple cybersecurity regulations. According to the White House, harmonizing regulatory requirements can lead to better security outcomes at lower costs.

To address this issue, the Administration and Congress have begun relevant initiatives to address the challenges associated with harmonizing cybersecurity regulations for our nation's critical infrastructure sectors. However, some of these actions are still underway and a planned completion date has not yet been announced.

As previously noted, in March 2023 and July 2023, respectively, the White House released the National Cybersecurity Strategy and the National Cybersecurity Strategy Implementation Plan.[11] Among other things, the strategy and implementation plan identified the need to establish an initiative on cybersecurity regulatory harmonization. As part of this initiative, ONCD was to engage with nongovernmental stakeholders through a request for information to understand existing challenges with regulatory overlap and explore a framework for reciprocity for baseline requirements.

In May 2024, the Administration issued its National Cybersecurity Strategy Implementation Plan (version 2), to update the previous year's version. Ongoing initiatives cited in the plan included setting minimum cybersecurity requirements across critical infrastructure sectors and increasing agency use of frameworks and international standards to inform regulatory alignment. In addition, the Administration added a new initiative to explore cybersecurity regulatory reciprocity pilot programs. The plan specifies that all of these initiatives will be completed by March 2025, or earlier.

In August 2023, in support of a National Cybersecurity Strategy strategic objective, ONCD issued a request for information that invited public comments on opportunities for, and obstacles to, harmonizing cybersecurity regulations.[12] ONCD stated that it was seeking input from

[11] The White House, *National Cybersecurity Strategy*, (Washington, D.C.: March 2023) and *National Cybersecurity Strategy Implementation Plan* (Washington, D.C.: July 2023).

[12] Request for Information on Cyber Regulatory Harmonization; Request for Information: Opportunities for and Obstacles To Harmonizing Cybersecurity Regulations, 88 Fed. Reg. 55,694 (Aug. 16, 2023).

stakeholders to understand existing challenges with regulatory overlap and explore a framework for reciprocity in regulator acceptance of other regulators' recognition of compliance with baseline requirements.[13] According to Regulations.gov, ONCD received over 100 comments on its request for information during the comment period, which closed in early November 2023.[14] ONCD has not published a summary of the comments.

Additionally, in April 2024, the Administration released National Security Memorandum-22, National Security Memorandum on Critical Infrastructure Security and Resilience.[15] Among other things, the memorandum calls for specific actions to be taken in support of the harmonization of cybersecurity regulations.

- Federal departments and agencies with regulatory authorities are to use regulation, drawing on existing consensus standards as appropriate, to establish minimum requirements and effective accountability mechanisms for the security and resilience of critical infrastructure.
- The National Cyber Director, in coordination with the Director of the Office of Management and Budget, is to lead the Administration's efforts for cybersecurity regulatory harmonization with respect to security and resilience requirements.
- The Secretary of Homeland Security is to develop and submit to the President by April 30, 2025, and on a recurring basis every 2 years thereafter by June 30, a National Infrastructure Risk Management Plan. The current National Infrastructure Protection Plan for securing critical infrastructure, which provides the overarching approach for integrating the nation's critical infrastructure protection and resilience activities into a single national effort, has not been updated since

[13] ONCD defined reciprocity in this context as the recognition or acceptance by one regulatory agency of another agency's assessment, determination, finding, or conclusion with respect to the extent of a regulated entity's compliance with certain cybersecurity requirements.

[14] Regulations.gov is a website where the public can comment on proposed federal rules and regulations, See https://www.regulations.gov/document/ONCD-2023-0001-0001.

[15] The White House, *National Security Memorandum on Critical Infrastructure Security and Resilience,* National Security Memorandum-22 (Washington, D.C.: Apr. 30, 2024).

2013.[16] Among other things, the updated National Infrastructure Risk Management Plan is to include:

- the identification, harmonization, and development of recommended national and cross-sector minimum security and resilience requirements to mitigate cross-sector risks not covered under sector-specific requirements; and
- a plan for harmonizing minimum security and resilience requirements across all sectors based on input from sector risk management agencies and other relevant federal departments and agencies.[17]

In addition, Congress and the President enacted the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA). CIRCIA was intended to help prioritize efforts to combat cyber threats by requiring certain entities to submit cyber incident reports to the Department of Homeland Security (DHS).[18] DHS's Cybersecurity and Infrastructure Security Agency (CISA) published a Notice of Proposed Rulemaking on April 4, 2024, seeking public comments on implementing CIRCIA's requirements, including ways to harmonize this regulation with other existing federal reporting requirements.[19] The deadline for comments is July 3, 2024.

CIRCIA also established a Cyber Incident Reporting Council (CIRC) to coordinate, deconflict, and harmonize federal incident reporting requirements, including those issued through regulation.[20] According to DHS, the Secretary of Homeland Security delegated responsibility to

[16] The Homeland Security Act of 2002, as amended, required DHS to develop a national plan for securing critical infrastructure and Presidential Policy Directive-21 required DHS to update that plan. See, 6 U.S.C. § 652(e)(1)(E) and The White House, *Presidential Policy Directive/PPD-21: Critical Infrastructure Security and Resilience* (Washington, D.C.: Feb. 12, 2013). As of April 2024, National Security Memorandum-22 superseded Presidential Policy Directive-21.

[17] Sector risk management agencies serve as day-to-day federal interfaces for their designated critical infrastructure sector and conduct sector-specific risk management and resilience activities.

[18] We have ongoing work related to DHS's efforts to implement the requirements of CIRCIA and plan to issue our report in the summer of 2024.

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

[20] Pub. L. No. 117-103, div. Y, sec. 103(a), 136 Stat. 49, 1054 (Mar. 15, 2022).

chair the CIRC to the DHS Under Secretary for Strategy, Policy, and Plans.

Further, CIRCIA required DHS to issue a report regarding cybersecurity regulatory harmonization. In response, in September 2023, the department issued its Harmonization of Cyber Incident Reporting to the Federal Government.[21] DHS invited the CIRC and 33 agencies to participate in developing the report to Congress. Among other things, the report identified 52 current or proposed federal cybersecurity incident reporting requirements, potentially duplicative federal reporting, and challenges to harmonization of these requirements. Such challenges include differences in the:

- definitions of reportable cyber incidents and thresholds for reporting,
- timelines and triggers for reporting,
- contents of incident reports,
- reporting mechanisms,
- procedural and resource burdens, and
- legal barriers and limited agency authorities.

The report also included eight recommendations that the federal government could adopt to streamline and harmonize cyber incident reporting, and three proposed legislative changes. For example, the report recommended that the federal government adopt model definitions of a reportable cyber incident, reporting timelines, and reporting triggers. The report also proposed that Congress remove any legal or statutory barriers to harmonization identified by the CIRC, including authorizing adoption of the model definitions of a reportable cyber incident, timeline, and trigger provisions.

As noted previously, although both the Administration and Congress have taken important initial steps on the issue of cybersecurity regulatory harmonization, significant work remains to be completed. Specifically, the Administration's efforts to evaluate setting minimum cybersecurity requirements across infrastructure sectors, increase agency use of frameworks and international standards to inform regulatory alignment, and leverage reciprocity pilot programs are still ongoing. In addition, DHS's September 2023 report noted that the CIRC would begin the

[21] DHS, *Harmonization of Cyber Incident Reporting to the Federal Government* (Washington, D.C.: Sept. 19, 2023).

process of implementing the report's recommendations, but did not provide a date for beginning the process or the completion of that work.

These key initial steps and their results can inform the broader effort and longer-term strategy to harmonize cybersecurity regulations, including future plans such as updates to the National Risk Management Plan. This underscores the importance of continuing to make progress on these key initiatives and continuing to address this significant issue.

In summary, as work continues on this important effort, it is vital that the stakeholders involved in this process remain focused on resolving the conflicts, inconsistencies, and redundancies currently found in our nation's cybersecurity regulations. Following through and executing specific plans and meeting established time frames, as supported by key organizations such as ONCD, DHS, and Congress, are essential to achieving harmonization. This, in turn, can better position our country's critical infrastructure sectors to address cybersecurity from a common perspective and help ensure the future safety and security of our nation.

Chairman Peters, Ranking Member Paul, and Members of the Committee, this completes my prepared statement. I would be pleased to respond to any questions that you might have.

GAO Contact and Staff Acknowledgments

If you or your staff have any questions about this testimony, please contact David B. Hinchman, Director of Information Technology and Cybersecurity, at (214) 777-5719, hinchmand@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this statement. GAO staff who made key contributions to this testimony are Michael Gilmore (Assistant Director), Josh Leiling (Assistant Director), Kavita Daitnarayan (Analyst-in-Charge), Amanda Andrade, Tracey Bass, Alexander Engel, Rebecca Eyler, Dwayne Staten, and Scott Pettis.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through our website. Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. You can also subscribe to GAO's email updates to receive notification of newly posted products.

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, https://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or
TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on Facebook, Flickr, Twitter, and YouTube.
Subscribe to our RSS Feeds or Email Updates. Listen to our Podcasts.
Visit GAO on the web at https://www.gao.gov.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact FraudNet:

Website: https://www.gao.gov/about/what-gao-does/fraudnet

Automated answering system: (800) 424-5454 or (202) 512-7700

Congressional Relations

A. Nicole Clowers, Managing Director, ClowersA@gao.gov, (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548

Public Affairs

Sarah Kaczmarek, Acting Managing Director, KaczmarekS@gao.gov, (202) 512-4800, U.S. Government Accountability Office, 441 G Street NW, Room 7149 Washington, DC 20548

Strategic Planning and External Liaison

Stephen J. Sanford, Managing Director, spel@gao.gov, (202) 512-4707
U.S. Government Accountability Office, 441 G Street NW, Room 7814,
Washington, DC 20548

AMERICAN PUBLIC POWER ASSOCIATION
Powering Strong Communities

June 3, 2024

The Honorable Gary Peters
Chairman
Senate Homeland Security &
Government Affairs Committee
340 Dirksen Senate Office Building
Washington, DC 20510

The Honorable Rand Paul
Ranking Member
Senate Homeland Security &
Government Affairs Committee
340 Dirksen Senate Office Building
Washington, DC 20510

Dear Chairman Peters and Ranking Member Paul:

The American Public Power Association (APPA) appreciates the opportunity to submit a statement for the hearing before the Senate Homeland Security & Government Affairs Committee titled, "Streamlining the Federal Cybersecurity Regulatory Process: The Path to Harmonization."

APPA is the voice of not-for-profit, community-owned utilities that power 2,000 towns and cities nationwide. APPA represents public power before the federal government to protect the interests of the more than 54 million people that public power utilities serve in 49 states and five territories, and the 96,000 people they employ. Public power utilities include utilities owned or authorized by a state, utilities owned by a political subdivision of a state (such as a municipality or utility district), and joint action agencies, joint powers agencies, and similar entities formed to collectively serve other public power utilities.

Public power utilities know that a reliable energy grid is the lifeblood of the nation's economic and national security, as well as vital to the health and safety of all Americans. Electric utilities take very seriously their responsibility to maintain a secure and reliable electric grid. The electric sector has mandatory and enforceable federal regulatory standards in place not just for reliability but also for cyber and physical security. These standards include mandatory reporting of specific cyber incidents to the Department of Energy (DOE) via an Electric Emergency Incident and Disturbance Report (OE-417) and the Department of Homeland Security's Cybersecurity & Infrastructure Security Agency (CISA) (via CISA's National Cybersecurity and Communications Integration Center), which are shared with the North American Electric Reliability Corporation and Federal Energy Regulatory Commission (FERC). These requirements are in addition to obligations under individual state laws on data security and data breach reporting that cover many information technology (IT) cyber security incidents.

Outside of these mandatory reporting standards, public power utilities participate in robust voluntary information sharing systems, such as the Electricity Subsector Coordinating Council and the Electricity Information Sharing and Analysis Center, as well as the Multi-State Information and Sharing Analysis Center. Additionally, the electric sector has seen increased adoption of technologies that assist with the visibility and monitoring of its industrial control system and operational technology networks, which also allow some automated sharing of information with government.

CISA's notice of proposed rulemaking (NPRM) is an important step in implementing the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA). CISA has properly proposed to require reporting only of incidents that actually jeopardize an information system. And CISA faithfully implements Congress' directives to report on ransom payments.

CISA's proposal, however, is overbroad with respect to small, distribution-only electric utilities. The NPRM proposes to require *all* electric utilities to report significant cyber incidents to CISA. While such an obligation is appropriate for large utilities that serve millions of customers, it is unnecessary and burdensome to impose the same obligation on the hundreds of community-owned, not-for-profit electric utilities that serve fewer than two thousand customers each. Small utilities that pose a negligible reliability risk to their neighbors or the grid at large should be excluded from CISA's proposed regulations. Or, at minimum, such small utilities should be required to report to CISA only if they experience an actual electrical outage that results from a cyber incident.

CISA has stated its intent to avoid duplicative reporting requirements for all critical infrastructure sectors, including the electric sector. But CISA is going forward with its rule without having finalized plans and agreements to implement that intent. As noted, the electric sector already has several mandatory and voluntary reporting requirements for cybersecurity incidents, and CISA has not offered any explicit confirmation that it will deem those existing reporting requirements to be substantially similar to its proposed requirements. Prior to issuing a final rule, CISA should complete its consultations with DOE and FERC and enter into an information sharing agreement with them. If those information sharing agreements are not executed prior to the CIRCIA rule becoming mandatory on electric utilities, the result will be duplicative reporting requirements contrary to Congress's intent.

APPA appreciates the enormity of the task CISA has been directed to undertake in implementing this law and stands ready to work with the subcommittee and CISA to achieve an outcome that is both workable for public power utilities and provides meaningful information to the government to strengthen our national security.

Sincerely,

Desmarie Waterhouse
Senior Vice President, Advocacy and Communications & General Counsel
The American Public Power Association

bpi | BANK POLICY INSTITUTE

Statement for the Record from the Bank Policy Institute

Before the U.S. Senate Committee on Homeland Security & Governmental Affairs

"Streamlining the Federal Cybersecurity Regulatory Process: The Path to Harmonization"

June 5, 2024

The Bank Policy Institute welcomes the opportunity to provide input on today's Senate Homeland Security and Governmental Affairs Committee hearing on "Streamlining the Federal Cybersecurity Regulatory Process: The Path to Harmonization." Today's hearing examines an important topic many critical infrastructure entities are grappling with given the proliferation of cybersecurity regulatory requirements in recent years. As such, we commend both the Committee and the Office of the National Cyber Director for emphasizing the need for increased harmonization.

Harmonization is particularly relevant for financial institutions that operate in a complex regulatory environment with multiple regulators and overlapping requirements. For example, resident examiners from the prudential financial regulatory agencies—the Office of the Comptroller of the Currency, the Federal Reserve Board and the Federal Deposit Insurance Corporation—regularly evaluate financial institutions to ensure they operate in a safe and sound manner and comply with relevant regulations. These examinations cover topics including information security, cyber risk management and incident reporting, governance, third-party oversight and operational resilience. Other agencies like the Consumer Financial Protection Bureau and the Commodity Futures Trading Commission also conduct similar oversight. Beyond examinations, banks are subject to additional cybersecurity-related regulatory requirements enforced by the Federal Trade Commission, the Securities and Exchange Commission and forthcoming requirements by the Cybersecurity and Infrastructure Security Agency, not to mention various state and international regulatory authorities.

Without appropriate harmonization, the collective effect of supervisory and regulatory obligations causes significant operational strain on financial institution staff and resources, diverting attention from efforts to keep pace with rapidly evolving cyber threats. During an exam, it is not unusual for firms to produce hundreds and sometimes thousands of pages of documents within 24-to-48-hour deadlines. In fact, according to a recent survey of large financial institutions, several firms reported their cyber teams now spend more than 70 percent of their time on regulatory compliance activities. Those same financial institutions also reported their Chief Information Security Officers or comparable senior cyber leaders spend between 30 to 50 percent of their time on the same regulatory compliance matters. Diverting finite cyber resources in this way leaves less time for risk mitigation efforts and more strategic security initiatives to fortify firm defenses over the long term. It leaves firms less well-positioned to confront existing critical threats and emerging risks associated with artificial intelligence and quantum computing, contributes to burnout and attrition among critical cyber personnel and unduly exposes firms to risk.

Based on our experiences within the multifaceted financial regulatory landscape, below are several proposed regulatory principles for the Committee to consider when developing a path to broader harmonization.[1] These principles include better coordination among regulatory agencies, regulatory reciprocity and leveraging common frameworks.

Regulator Coordination

Financial institutions work closely with the prudential financial regulators who coordinate among themselves through the Federal Financial Institutions Examination Council to help promote uniform supervision. There is significant benefit to the collaborative opportunities the FFIEC provides for regulatory agencies to develop joint standards and limit duplication where possible. Even with that coordination, differences in agency mission and exam scope continue to lead to overlap. This is particularly true as technology and cybersecurity play a more pivotal role within financial institutions and regulatory scrutiny of those areas increases.

As a general matter, it is imperative that all regulators consider existing requirements and do not duplicate or create variations of what already exists. Over the last few years, we have seen this does not always occur, especially with independent regulatory agencies. A prime example of this is the SEC's Public Company Disclosure Rule[2] which threatens to directly undermine the central purpose of confidential reporting requirements like the Cyber Incident Reporting for Critical Infrastructure Act.[3]

Relatedly, better coordination is especially necessary for requirements governing cyber incident reporting. Last year, the Cyber Incident Reporting Council identified 45 in-effect reporting requirements across the Federal government, all with varying standards and thresholds.[4] Just a few weeks ago, the Federal Housing Administration issued a new duplicative reporting requirement effective *immediately* requiring incident reporting within 12 hours of detection—all without the opportunity for public notice and comment.[5] The FHA's requirement is not aligned with any existing requirement such as the prudential banking regulators' 36-hour notification rule[6] or CIRCIA. The FHA is not alone in its efforts, as earlier this year we also saw the CFTC propose a separate incident reporting requirement as part of a proposed rule on operational resilience.[7]

As cybersecurity- and resilience-related regulatory requirements continue to expand in number and scope across critical infrastructure sectors, it is imperative that regulatory agencies consider the impact of these requirements on the ability of firms to focus on critical security tasks and preserve the ability to innovate to keep up with the dynamic threat environment. We are encouraged that the Committee is considering legislative approaches to address this need.[8]

Regulatory Reciprocity

[1] *See* Bank Policy Institute & American Bankers Association, Comment Letter on Request for Information on Cybersecurity Regulatory Harmonization (Oct. 31, 2023), https://bpi.com/wp-content/uploads/2023/10/2023.10.31-BPI-ABA-ONCD-RFI-Response-2023.10.31.pdf.

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

[3] *Surveying CIRCIA: Hearing on Sector Perspectives on the Notice of Proposed Rulemaking Before the Subcomm. on Cybersecurity and Infrastructure Protection of the H. Comm. on Homeland Security*, 118th Cong. 3 (2024) (statement of Heather Hogsett, Senior Vice President, BITS/Bank Policy Institute), https://bpi.com/wp-content/uploads/2024/04/Statement-for-the-Record-from-the-Bank-Policy-Institute-H.-Homeland-CIRCIA-Hearing.pdf.

[4] Dep't of Homeland Sec., Harmonization of Cyber Incident Reporting to the Federal Government 4 (2023).

[5] Fed. Housing Admin, Significant Cybersecurity Incident (Cyber Incident) Reporting Requirements (May 23, 2024), https://www.hud.gov/sites/dfiles/OCHCO/documents/2024-10hsgml.pdf.

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

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

[8] Suzanne Smalley, *Senate chairman wants new White House-led panel to streamline federal cyber rules*, THE RECORD (May 30, 2024), https://therecord.media/gary-peters-legislation-new-committee-oncd-harmonize-cyber-regulations.

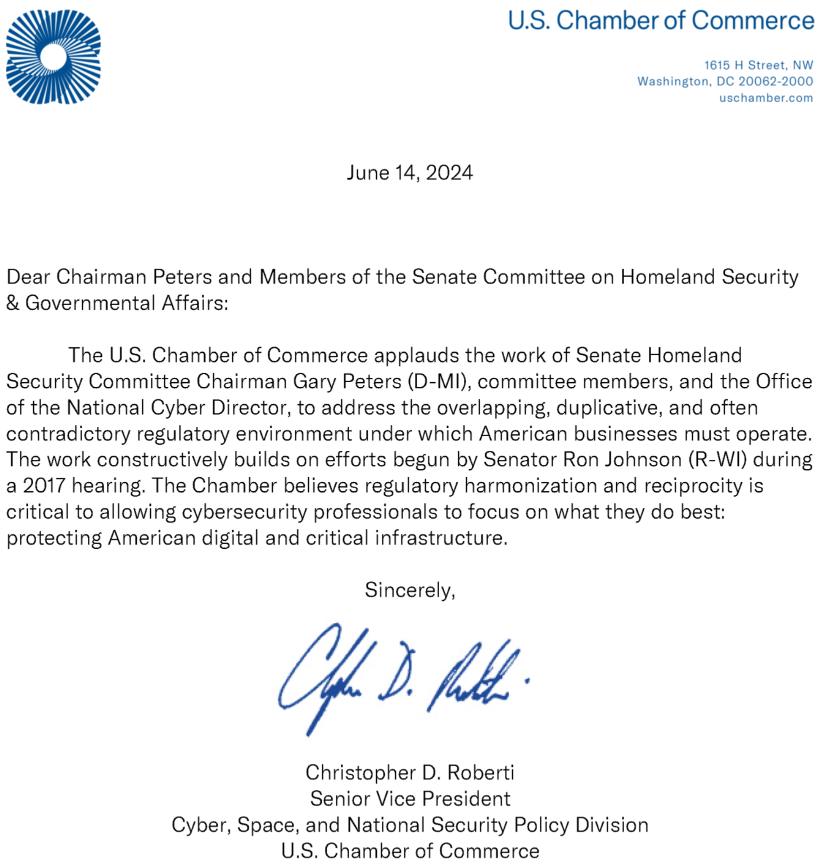
While enhanced harmonization would likely have to occur first, exploring a regulatory reciprocity model is a worthwhile endeavor to promote regulatory coherence. This reciprocity would involve regulators better leveraging each other's documentation, testing, evaluations and findings. Developing such a model would provide regulators with the information they need to fulfill their oversight responsibilities while preventing organizations from having to demonstrate compliance with the same or similar requirements multiple times and to multiple regulators. This would be a much more effective and efficient approach and would reserve more time for core security activities.

Common Frameworks

Last, utilizing existing standards—like the National Institute for Standards and Technology's Cybersecurity Framework—can be valuable for companies as they navigate complex regulatory obligations. Within the financial sector, the Cyber Risk Institute developed the Financial Sector Profile[9]—based on the NIST CSF—which integrates regulatory requirements unique to financial institutions. The Profile provides financial institutions with a single scalable resource for managing cyber risk and compliance requirements. Regulators can similarly use common frameworks to more efficiently tailor oversight activities and determine an organization's baseline security posture.

BPI recognizes the important role regulatory agencies play in promoting sound cybersecurity practices. As noted above, however, it is equally important to strike a balance between regulatory obligations and critical security activities to protect an organization. We look forward to engaging further with the Committee to find that appropriate balance.

[9] *The Profile,* CYBER RISK INSTITUTE, https://cyberriskinstitute.org/the-profile/.



U.S. Chamber of Commerce

1615 H Street, NW
Washington, DC 20062-2000
uschamber.com

June 14, 2024

Dear Chairman Peters and Members of the Senate Committee on Homeland Security & Governmental Affairs:

The U.S. Chamber of Commerce applauds the work of Senate Homeland Security Committee Chairman Gary Peters (D-MI), committee members, and the Office of the National Cyber Director, to address the overlapping, duplicative, and often contradictory regulatory environment under which American businesses must operate. The work constructively builds on efforts begun by Senator Ron Johnson (R-WI) during a 2017 hearing. The Chamber believes regulatory harmonization and reciprocity is critical to allowing cybersecurity professionals to focus on what they do best: protecting American digital and critical infrastructure.

Sincerely,

Christopher D. Roberti
Senior Vice President
Cyber, Space, and National Security Policy Division
U.S. Chamber of Commerce