S. Hrg. 115–310

CYBERSECURITY REGULATION HARMONIZATION

HEARING

BEFORE THE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS UNITED STATES SENATE

ONE HUNDRED FIFTEENTH CONGRESS

FIRST SESSION

JUNE 21, 2017

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

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

U.S. GOVERNMENT PUBLISHING OFFICE
27–395 PDF WASHINGTON : 2018

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

RON JOHNSON, Wisconsin, *Chairman*

JOHN MCCAIN, Arizona	CLAIRE MCCASKILL, Missouri
ROB PORTMAN, Ohio	THOMAS R. CARPER, Delaware
RAND PAUL, Kentucky	JON TESTER, Montana
JAMES LANKFORD, Oklahoma	HEIDI HEITKAMP, North Dakota
MICHAEL B. ENZI, Wyoming	GARY C. PETERS, Michigan
JOHN HOEVEN, North Dakota	MAGGIE HASSAN, New Hampshire
STEVE DAINES, Montana	KAMALA D. HARRIS, California

CHRISTOPHER R. HIXON, *Staff Director*
GABRIELLE D'ADAMO SINGER, *Chief Counsel*
COLLEEN E. BERNY, *Professional Staff Member*
MARGARET E. DAUM, *Minority Staff Director*
JULIE G. KLEIN, *Minority Professional Staff Member*
LAURA W. KILBRIDE, *Chief Clerk*
BONNI E. DINERSTEIN, *Hearing Clerk*

CONTENTS

WITNESSES

WEDNESDAY, JUNE 21, 2017

ALPHABETICAL LIST OF WITNESSES

APPENDIX

CYBERSECURITY REGULATION HARMONIZATION

WEDNESDAY, JUNE 21, 2017

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

The Committee met, pursuant to other business, at 10:29 a.m., in room SD–342, Dirksen Senate Office Building, Hon. Ron Johnson, Chairman of the Committee, presiding.

Present: Senators Johnson, Lankford, Daines, McCaskill, Carper, Tester, Heitkamp, Peters, Hassan, and Harris.

OPENING STATEMENT OF CHAIRMAN JOHNSON

Chairman JOHNSON. Good morning. This hearing will be called to order. I want to welcome our witnesses. Thank you for your testimonies.

I would ask consent that my written statement be entered into the record.[1]

I will just keep my remarks brief.

Cybersecurity is an enormous threat facing this Nation As General Keith Alexander, the former Director of the National Security Agency (NSA), said, the loss of industrial information and intellectual property through cyber espionage constitutes "the greatest transfer of wealth in human history."

I believe this is either our fifth or sixth hearing on different aspects of the problem associated with cybersecurity. We are looking at different parts of this, looking for a proper definition of the problem, certainly laying out the reality of what General Alexander was referring to, but also looking for solutions.

This is an interesting hearing because it combines our concentration on this real threat, cybersecurity, one of the top priorities on the homeland security side of our Committee, with a top priority on the governmental affairs part of this Committee, overregulation—the $2 trillion regulatory burden, about $15,000 per year per household, and how that overregulation is making us less secure in cyberspace.

It is interesting. We had Comptroller General Gene Dodaro here at our annual duplication report hearing, and we had the chancellor of UW-Madison come and testify. The last 2 years she has visited me in my office, she has complained of overregulation. This year she came in armed with a study commissioned by the research

[1] The prepared statement of Senator Johnson appears in the Appendix on page 29.

universities that said that 42 percent of researcher time in these universities on Federal Government grant programs—these are the grants that are supposed to cure diseases and help advance human knowledge and science—42 percent of researcher time is spent filling out and complying with Federal regulations. And, I think what is interesting is that in testimony today from our witnesses, one of the witnesses will testify that about 40 percent of his time or his cybersecurity group's time is spent—guess what?—complying with often contradictory Federal regulations.

So, we obviously have to streamline this. We have to understand the enormous opportunity cost of overregulation, of contradictory regulations. If we want to truly address this very complex problem of the threats we face because of the cyber attacks and our challenges in securing our cyber assets, we have to look to all levels of government, consolidating their regulatory framework, to streamline that regulatory regime as much as possible so professionals within industry and within government, quite honestly, can concentrate on the primary task at hand, which is securing our cyber assets.

With that, I will turn it over to Senator McCaskill.

OPENING STATEMENT OF SENATOR MCCASKILL[1]

Senator MCCASKILL. Thank you, Chairman Johnson. One of my top priorities as a Senator is focusing on how we can make government work better and more efficiently. Eliminating waste, fraud, and abuse in an effort to save taxpayer dollars and improve government services and make government less intrusive into the lives of operating businesses in this country are a priority.

Today's hearing allows for us to hear from representatives from the private sector and the States about how they manage compliance with the variety of regulations they face relating to data and cybersecurity. There is currently no clearinghouse for mitigating conflicts between regulators, and as a result, States and industry bear the burden for ensuring compliance between sometimes redundant and often conflicting regulations.

Regulators play an essential role in mandating security measures like notifications after a data breach and requiring a minimum level of security to protect personally identifiable information (PII). However, as these witnesses will attest, while the goal of the regulation is improved security, due to a lack of harmonization between regulations industry spends too much valuable time sorting through compliance when it could be investing those hours and resources into improving their security systems and services.

We will hear today about how centralized information technology (IT) systems can play a key role in improving efficiency and security. The same can be said about centralizing cyber policy across the Federal Government. We have made significant strides in recent years to authorize and operationalize the Department of Homeland Security's (DHS) National Cybersecurity and Communications Integration Center (NCCIC). President Obama also mandated the creation of National Institute of Science and Technology

[1] The prepared statement of Senator McCaskill appears in the Appendix on page 30.

(NIST) Cybersecurity Framework, which creates a common language for government and industry.

We have spent years working to make DHS the central cybersecurity information sharing entity. We finally passed the Cybersecurity Information Sharing Act (CISA) in 2015, providing liability protection to encourage industry to share threat information with DHS. But, now the Department of Health and Human Services (HHS) has decided that the NCCIC and the existing information sharing structure have limitations. Rather than examining what the private sector was doing to address potential gaps, HHS went ahead and built a health-specific version called the "Health Cybersecurity and Communications Integration Center" (HCCIC). That is the essence of duplicative. It is exactly the problem that we are trying to address in this hearing.

I have questions about the utility of this new entity. It is also not clear that this new cyber center is necessary or that it adds value. We should be looking to enhance information sharing participation and the NCCIC's capabilities, not sprouting a new "kick" for every industry or critical infrastructure sector. This could go on ad nauseam, handcuffing business even more in terms of sharing important threats with people who need to know.

I am glad Chairman Johnson is joining me in sending a letter to HHS asking questions about the genesis of this new HCCIC and how it has been and will coordinate with DHS on the liability protections offered to those that share information with the HCCIC and why this new entity is even necessary. I hope we can stop this before it goes too far.

I look forward to hearing from the witnesses today about other ways we can work to simplify and harmonize their regulatory burden.

Thank you, Mr. Chairman, for holding this hearing.

Chairman JOHNSON. Well, thank you, Senator McCaskill. And, again, I appreciate the leadership you have taken on that. It just kind of proves the point that, bottom line, the government wants to grow, regardless of the Administration. I believe this was started under Obama, and the Trump administration is kind of moving right forward with it. So, hopefully we can prevent that and consolidate this, and that is the purpose of the hearing.

It is the tradition of this Committee to swear in witnesses, so if you will all stand and raise your right hand. Do you swear that the testimony you will give before this Committee will be the truth, the whole truth, and nothing but the truth, so help you, God?

Mr. FEENEY. I do.

Mr. GARFIELD. I do.

Mr. NUTKIS. I do.

Mr. REESE. I do.

Chairman JOHNSON. Please be seated.

Our first witness is Christopher F. Feeney. Mr. Feeney is currently president of BITS.

The technology policy division at the Financial Services Roundtable (FSR). Mr. Feeney has over 30 years of experience in technology, business, sales, executive management, and operating roles at a variety of companies. Before starting at BITS, Mr. Feeney served as Chief Executive Officer (CEO), president, and in execu-

tive roles at Thomson Financial, Bank of America, Telerate, Multex, and Broadridge Financial. He is currently on the Board of Directors at Scottrade, Incorporated, and an executive committee member of the Financial Services Sector Coordinating Council (FSSCC). Mr. Feeney.

TESTIMONY OF CHRISTOPHER F. FEENEY,[1] PRESIDENT, BITS, FINANCIAL SERVICES ROUNDTABLE

Mr. FEENEY. Chairman Johnson, Ranking Member McCaskill, thank you for inviting me to testify on this critically important and timely subject.

The Financial Services Roundtable represents 100 of the leading financial firms in our country, including banks, insurance companies, asset managers, payment firms, and finance companies.

Make no mistake: Cybersecurity is a top-of-mind issue for every one of our CEOs, and the industry is committed to making the investments necessary to protect our critical infrastructure and, ultimately, the information and assets of our customers.

Our industry is one of the most heavily regulated sectors. Nine independent Federal regulators, three self-regulatory organizations, and the State insurance, banking, and securities agencies oversee the industry. With that level of regulatory oversight, it is imperative that financial firms develop strong, collaborative relationships with regulators. In no space is that more relevant than in cybersecurity.

The cybersecurity requirements across the financial industry are, like the sector itself, very diverse in terms of business size, type, and geographic footprint. That said, we have heard from both our members and regulators that 60 to 80 percent of the cyber issuances could be considered common across all regulators. For any regulated entity, words matter. For the financial sector, with our waterfront of State and Federal regulators, it becomes a tangible problem when those tasked with creating cybersecurity rules do not follow a common language and instead approach the shared components of cybersecurity regulations with their own variations addressing the same cyber issues but from different perspectives.

Think about it this way: As you all know, English is the universal language of air traffic controllers, and controllers all over the globe speak to pilots using the same agreed-upon language. Imagine if a pilot flying to Paris, the Middle East, and China had to know every native language as well as the different variations in expectations and protocols for every airspace they pass through.

To put it in the context of this hearing, over the last 2 years State and Federal financial regulators have put forth 46 cybersecurity regulations, updates to guidance, or new tools. Individually, these regulations have merit. However, while we recognize the need to have cyber regulations tailored to the different firms and the markets in which they operate, these regulations do not follow a common language or a common set of exam procedures. This is counterproductive and introduces tremendous inconsistency and duplication of effort for technology operators, governance architects, and executive leadership.

[1] The prepared statement of Mr. Feeney appears in the Appendix on page 33.

More specifically, firms already burdened by a shortage of skilled cyber professionals must take resources away from protecting their platforms to interpret the language of diverse regulations. Ultimately, we hold ourselves accountable, and the financial firms must ensure compliance with the regulatory process.

As for a solution, you might be surprised to hear me say that it is not necessarily fewer regulations but instead rationalized and harmonized regulation around a common approach and a shared language. Our industry is committed to working with regulators to address this issue. In fact, FSR BITS and our industry partners have developed a model cyber framework using consistent language specific to our sector. The foundation of this effort is the NIST Cybersecurity Framework, which has been used in a similar way by other industries.

We were very pleased to see this issue highlighted in the Treasury's report on modernizing financial regulation, which called for better coordination on cybersecurity regulation and examination across State and Federal financial Agencies.

In conclusion, until that goal can be reached, we encourage the regulators to pause any additional cyber regulation which, if issued, will only serve to extend the problems I have described. When a chief information security officer (CISO) at one of our largest member firms estimates that 40 percent of his group's time is spent trying to unravel the web of cybersecurity regulations rather than focusing on protecting systems, that is a serious problem. We must ensure this issue does not fall prey to regulatory one-upmanship or jurisdictional turf battles. We must collaborate to maintain the cyber integrity of the U.S. financial system.

Thank you, Mr. Chairman, and I look forward to your questions.

Chairman JOHNSON. Thank you, Mr. Feeney.

Our next witness is Dean Garfield. Mr. Garfield currently serves as president and CEO of the Information Technology Industry (ITI) Council. Through this role, ITI has helped defined the national and international technology agenda, expanded its membership, and launched a leading innovation foundation. Before joining ITI, Mr. Garfield served as executive vice president and chief strategic officer for the Motion Picture Association of America (MPAA) and vice president of legal affairs at the Recording Industry Association of America (RIAA). Mr. Garfield.

TESTIMONY OF DEAN C. GARFIELD,[1] PRESIDENT AND CHIEF EXECUTIVE OFFICER, INFORMATION TECHNOLOGY INDUSTRY COUNCIL

Mr. GARFIELD. Thank you. Chairman Johnson, Ranking Member McCaskill, and Members of the Committee, on behalf of 60 of the most dynamic and innovative companies in the world, I would like to thank you for engaging us in this conversation. The issues we are talking about today are immensely important, and so I would like to thank you as well for putting the focus on this issue.

We have submitted my testimony for the record, so rather than repeat it, I will presume you have already read it and hone in on three things: one, our definition of the problem; two, what we are

[1] The prepared statement of Mr. Garfield appears in the Appendix on page 58.

doing to help solve for it; and, three, where we see gaps that Congress, and this Committee specifically, can be helpful.

Our definition of the problem is really how do we go about preserving the vibrancy and vitality of the Internet while protecting it against those who seek to do damage to the ecosystem through cyber insecurity. For us, success looks like enhancing the societal and economic benefits of the Internet, its openness, its interoperability, its integrated and international nature, while making sure we are protecting it against cyber insecurity.

Like many shared spaces, whether it is a community play area or the Internet, we know that when there are encroachments, the instinct is to react by adding regulation and adding new rules. In the case of Internet and cyberspace, to do so would be a colossal mistake.

What are we doing to try to help? We are focused on a multifaceted approach, largely targeted in three areas:

One, doing what we do best, which is innovating, making sure that we are thinking about cybersecurity in the first instance as a design feature both at the hardware and software level.

Second is recognizing that because this is a shared space, it is a shared responsibility, and so working in public-private partnerships to make sure that we are advancing cybersecurity. My colleague Mr. Feeney referenced the NIST framework, which we think should be the foundational strategy for how we go about protecting cyberspace.

Third, we are endeavoring to cascade best practices through our supply chains and more broadly. For businesses like the ones I represent, cybersecurity is a CEO issue, and we put the emphasis and the resources that are necessary behind it. For small businesses, they may not have the resources or the know-how to do so, and so we are endeavoring to do what we can to help solve for that.

How can this Committee and Congress help? There are a number of gaps that we have identified, including the ones that are the point of this hearing.

One, there is a lack of coordination. There are three Executive Orders (EO) in the last 5 years focused on cybersecurity and driving greater coordination. That has not occurred.

Second, the point that I made earlier about small businesses and making sure that they are contemplated as part of the solution in this area is another gap that we see.

What we recommend this Committee and Congress do generally is using its oversight powers to ensure that the level of coordination that is called out in those Executive Orders actually happens, built around the strategy that exists in the NIST framework, which is incredibly flexible, adaptable. In the same way that those who are endeavoring to create cyber insecurity are adapting all the time, the NIST framework is really a broader strategy around which we can build.

Second is streamlining. The Department of Homeland Security, which Ranking Member McCaskill noted earlier is working on these issues, last year I spent some time looking at all of the different Federal cybersecurity initiatives around the Internet of Things (IOT), and recognized and identified that there were 30, often competing, different initiatives built solely around IOT. That

is simply emblematic of the broader problem, and I know Mr. Feeney's exhibit over there to our right, in the context of his world, in the financial services sector I think does a good job of capturing the redundancies that occur more broadly.

Third, it is critical, since this is a shared issue, that we take a multifaceted approach. Part of the solution here, including for the private sector but government as well, is our procurement practice. The procurement system actually helps to create these redundancies and complexities, and so streamlining and simplifying our procurement process will help to advance our goals in this area. I know this Committee is contemplating and considering the MGT Act, and from our perspective, moving that in a way that is consistent with your goals is a part of the solution in this area as well.

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

Chairman JOHNSON. Thank you, Mr. Garfield.

Our next witness is Daniel Nutkis. Mr. Nutkis currently serves as founder and chief executive officer at the Health Information Trust Alliance (HITRUST) Alliance. Mr. Nutkis has over 25 years of experience in risk management and health information technology. Before founding HITRUST, he served as executive vice president of strategy and president of care delivery at Zix Corporation, a security technology company. He also served as the national director for Ernst & Young LLP's health care emerging technology practice. Mr. Nutkis.

TESTIMONY OF DANIEL NUTKIS,[1] CHIEF EXECUTIVE OFFICER, HEALTH INFORMATION TRUST (HITRUST) ALLIANCE

Mr. NUTKIS. Chairman Johnson, Ranking Member McCaskill, and Members of the Committee, I am pleased to appear today to discuss the health care industry's experiences in engaging with government Agencies relating to cybersecurity regulatory harmonization and efforts we believe will provide the greatest benefit to industry. I am Dan Nutkis, CEO and founder of the Health Information Trust Alliance. HITRUST was founded in 2007 and endeavored and continues to endeavor to elevate the level of information protection in the health care industry and its collaborators, especially between industry and government. While I prepared my written statement for the record, in my testimony today I will highlight three areas where cybersecurity regulatory harmonization should occur to reduce redundancy, unnecessary expense, and delays to better support the private sector in defending against cyber threats, thereby improving cyber resilience and management of cyber risk.

First is the area of information sharing. In 2010, HITRUST established a mechanism to share Indicators of Compromise (IOCs) and other cyber threat information with organizations of varying cyber maturity. HITRUST has led the industry in the collection and distribution of cyber threat information and continuously evaluates and innovates to support organizations in managing their cyber threats.

[1] The prepared statment of Mr. Nutkis appears in the Appendix on page 74.

From the beginning, HITRUST participated with the DHS Cyber Information Sharing and Collaboration Program (CISCP). We operate the largest and most active Information Sharing and Analysis Organization (ISAO) in health care. We are the first health care organization to begin sharing bidirectionally with the Department of Homeland Security's Automated Indicator Sharing (AIS) program.

It was a surprise to learn that the Department of Health and Human Services recently established its healthcare-specific cybersecurity and communications center to focus its efforts on analyzing and disseminating cyber threats across the health care industry.

There is a significant level of effort required for organizations like HITRUST in coordination with its thousands of constituents to engage in cyber information sharing programs with government. We undertake these efforts because we see the value in the program and participation with government and believe we are all operating toward a common goal. More can and should be done to ensure the role of industry and government are clearly defined when it comes to information sharing.

The second is the area of government as a partner. HITRUST values its partners and recognizes the burden, responsibility, and authority beholden on them to protect the private sector. However, we should expect in areas where the private sector has made a significant investment in establishing an effective program or approach, the government would give it due consideration before seeking a government alternative that replicates or devalues industry efforts.

For instance, last year, the Health and Public Health Sector Coordinating Council (SCC) and Government Coordinating Council (GCC), with input from HITRUST and other sector members including the DHS Critical Infrastructure Cyber Community, developed the Health Sector implementation guide for the NIST Cybersecurity Framework, specifically referred to as the "Healthcare Sector Cybersecurity Framework Implementation Guide." Yet despite the significant public and private effort that went into its publication, HHS is working toward the development of yet another health care-based implementation guide of the NIST Cybersecurity Framework despite the broad adoption of the existing guidance by private sector organizations. We are perplexed as to why HHS would not partner with industry by leveraging programs already in place and offering assistance to improve them instead of replicating and dismissing the hard work of industry. We would ask that Congress require Federal Agencies to give due consideration to existing standards and best practices already in place before developing new ones.

The third is the area of government as a regulator. The Department of Health and Human Services is responsible for overseeing the implementation of the Health Insurance Portability and Accountability Act (HIPAA), and the HHS Office for Civil Rights (OCR) is responsible for assessing compliance with and enforcement of the HIPAA Privacy, Security and Breach Notification Rules, including issuance of civil and criminal penalties.

In support of their role, they conduct annual random audits that are designed to enhance industry awareness of compliance obliga-

tions. We have documented that these random audits are, in fact, causing organizations to divert their attention and resources from enhancing their information protection programs based on the potential for random audits.

We propose that policymakers consider a system whereby organizations that can demonstrate a comprehensive information security program that complies with the privacy and security provisions of HIPAA can receive some form of safe harbor or similar relief, and focus HIPAA audits on those organizations that cannot demonstrate their compliance in meeting the criteria.

I hope my testimony illuminates areas where individual activities may seem innocuous, but in totality begin to create confusion and concern. I have highlighted where additional clarity in regulation and guidance will ensure the private sector understands how to best engage with government and also the complex issues that arise when a regulator is partnering with industry.

Thank you again for the opportunity to join you today and share these insights. I look forward to your questions.

Chairman JOHNSON. Thank you, Mr. Nutkis.

Our final witness is Bo Reese. Mr. Reese currently serves as the chief information officer (CIO) for the State of Oklahoma and vice president of the National Association of State Chief Information Officers (NASCIO). Mr. Reese has been in State government for 25 years and was appointed the Oklahoma State CIO by Governor Mary Fallin in 2014. Prior to this role, he was CIO and deputy administrator and chief operations officer at HealthChoice, the State's self-funded health plan. From 2013 to 2014, Mr. Reese served as the chief operations and accountability officer at the Office of Management and Enterprise Services, Information Services. That is a pretty good mouthful. Mr. Reese.

TESTIMONY OF JAMES "BO" REESE,[1] VICE PRESIDENT, NATIONAL ASSOCIATION OF STATE CHIEF INFORMATION OFFICERS, AND CHIEF INFORMATION OFFICER, INFORMATION SERVICES, OFFICE OF MANAGEMENT AND ENTERPRISE SERVICES, STATE OF OKLAHOMA

Mr. REESE. Chairman Johnson, Ranking Member McCaskill, and Members of the Committee, thank you for inviting me to testify before you today on Federal data security regulations and their impact to State governments.

My name is Bo Reese, and I serve as the chief information officer for the State of Oklahoma. I also serve as the vice president of the National Association of State Chief Information Officers. All 50 States and 2 territories are members of NASCIO, and we represent the interests of Governor-appointed State CIOs who act as the top IT official for State government.

Today, I would like to provide the Committee an overview of how Federal cybersecurity regulations impact our work to introduce efficiencies and generate savings for State taxpayers. I will also touch upon how the complex Federal regulatory environment is duplicative in nature, contributes to inconsistent Federal audits, and

[1] The prepared statement of Mr. Reese appears in the Appendix on page 79.

drives cybersecurity investments based on compliance and not risk, which is the more secure approach.

Based on a 2009 assessment and prior to IT consolidation, the State of Oklahoma was supporting 76 financial systems, 22 unique time and attendance systems, 17 different imaging systems, 48 reporting and analytic applications, and 30 data center locations.

Over the past 5 years, we have reduced these redundancies, made large strides in unifying technology, and completed consolidation of 76 of the 78 mandated State Agencies and more than 30 voluntary agencies. Consolidation has resulted in $283 million of estimated reduced spending and projected savings. One of the biggest hurdles in achieving savings through IT consolidation has been compliance with Federal security regulations.

State CIOs and chief information security officers must comb through thousands of pages of Federal regulations to ensure that States are in compliance with rules from our Federal partners, and even though many Federal regulations are similar in nature in that they aim to protect high-risk information, they are mostly duplicative and have minor differences which can obscure the goal of IT consolidation, the whole point of which is to streamline IT applications and simplify the enterprise IT environment to produce savings for taxpayers.

For example, Internal Revenue Service (IRS) Publication 1075 and the Federal Bureau of Investigation (FBI) both protect very high risk information, but their password policies vary enormously. Also, the IRS requires incident notification within 24 hours, but Center for Medicare and Medicaid Services (CMS) requires notification of a breach without unreasonable delay.

Additionally, the FBI requires us to keep audit logs for one year. The IRS requires us to retain audit records for 7 years.

Further, duplicative regulations also contribute to inconsistent Federal audits. State governments are often audited multiple times by the same Federal agency and have different audit findings, even though they are auditing the exact same IT environment. For example, in Oklahoma, the IRS audited one of the State Agencies twice because it viewed two programmatic elements of the agency as separate entities. My office had to answer questions, attend meetings, and deliver additional explanatory materials twice for one agency because it is seen as two by the IRS auditors. Additionally, one audit team had a finding, and the other did not, despite only one IT environment being the subject of both audits.

In Louisiana, five State Agencies were assessed by five different IRS auditors and ended up with five different outcomes. One agency had 32 findings; another, 27; one had 23; one had 14; and another had only 11. We have several more similar examples in our attachment to the written testimony.

Inconsistent regulations in audits are problematic because it leads CIOs to make cybersecurity investments based on compliance and not risk. When Federal data security audits are conducted and produce findings of a critical nature, State CIOs must direct their attention and resources to remediating and addressing those findings to satisfy Federal auditors and avoid any potential negative impact to citizens. This approach is problematic for State government cybersecurity because it encourages State CIOs to make

check-the-box compliance investments instead of ones based on risk, which is the more secure approach to managing sensitive data.

We appreciate efforts by the Federal Government to secure and protect sensitive citizen information because we also share that responsibility at the State level. But, we must accomplish our shared goal without overly burdening State governments, ensuring that we are delivering government services to citizens in the most efficient and cost-effective manner. In recognition of that shared mission and responsibility, we want to work with our Federal Government partners to harmonize disparate regulatory requirements and normalize the audit process.

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

Chairman JOHNSON. Thank you, Mr. Reese.

If we could put that diagram back up on the board, I would appreciate it.

I think the witnesses have really laid out through anecdotal stories the problem here that I think is pretty obvious and pretty clear. I think the solution is actually pretty clear as well, but, as a diagram, this is pretty good. I do not know how long we actually had printers that could print something this complex. [Laughter.]

But, Mr. Garfield, you mentioned the fact that there have been three Executive Orders basically asking the Federal Government to harmonize the regulation in the space, and you went on to testify that they have not been implemented.

First of all, describe why not. I mean, is there any explanation of why a step that is so obvious, something that is just so imperative that we do, why has it required three Executive Orders and those Executive Orders have gone unimplemented?

Mr. GARFIELD. I think in part it is because of the challenge of putting someone in charge. So, in order to have the level of coordination that is needed to avoid the kind of redundancy that we see reflected in that chart, you need someone who is a center point for coordination. So, we have a strategy, which is the NIST framework, around which we can build, but that strategy has to be driven by a particular entity or person.

For example, in the most recent Executive Order, 13800, from President Trump, he pushes all of the Agencies and actually requires the Agencies to say what they are doing to act consistent with the NIST framework. The second part of it is not asked, and that is, What are the additional regulations that you are advancing related to cybersecurity? It is one thing to say you are implementing the NIST framework. It is another thing to actually do so in a fashion that does not create replication, redundancy, and complete lack of coordination.

So, I think having a center point that is coordinating and advancing this to avoid duplication is central to helping to solve for this.

Chairman JOHNSON. You are not saying there has been some bureaucratic infighting in terms of who wants—so let us—I mean, who should coordinate this? Because in the end, you need some department, some agency, somebody in the Federal Government to take charge of this, to be given the responsibility, to be held ac-

countable to coordinate this action, to make sure that everybody comes into line so that the—again, Mr. Reese, I cannot remember how many you said, the number of different requirements that are required are actually answered in the same way. Who do you think is the best—and I will have all of you answer that question. Which agency, which department of government ought to take control of this? We will start with you.

Mr. FEENEY. I think for us it is important to keep Treasury in the role they are in. They are chartered to be our sector-specific agency through DHS, and that has been very useful. They sit between both the industry and also the regulators. They chair the Federal Banking Infrastructure Council (FBIC), that specifically works with the Federal regulators, plus others like market regulators. So, in our world, that is the logical place. They understand us; they know our business. They understand financial systems and have been a good steward.

Chairman JOHNSON. But, again, the problem with that is you are the financial industry. Then you have the health care industry over there.

Mr. FEENEY. Right.

Chairman JOHNSON. And, now you have different Agencies of government basically trying to ask the same questions, trying to do the same type of regulation to ensure cybersecurity. And, Mr. Nutkis' group's regulators is going to have something completely different. Is that not the problem, Mr. Nutkis?

Mr. NUTKIS. Well, I think for us there are multiple problems. I think some of the guidance that is out there puts DHS squarely in the middle when it comes to cyber information sharing. So, we did not think we had any ambiguity, which I testified in March in a similar hearing, which was we were somewhat confused because we thought the Presidential directive created the ISAOs and then CISA clarified the role of government, which the Presidential directive kind of said you share with government, CISA clarified which part of government you shared with, so industry started moving down a path to do that.

We may see things slightly different. We see HHS as a regulator. They fine, they enforce. So, sometimes when it comes to how openly and willingly you want to share with your regulator makes things a little tough as well. So, I think there is a role for the regulator in the role that they play, but as we look at looking for things like standards and how we apply these, we want them to be applicable across all industries. They can apply to ours as well.

I think also health care is not a box. You have organizations that make fitness equipment. You have organizations that have supplements. You have organizations that deliver care. The lines get fuzzy, so we sometimes find that they do not work in small boxes.

Chairman JOHNSON. So, again, you have the departments, you have the Agencies regulating different industries, and, again, that would be appropriate. What we are talking about here is something over all of those to completely coordinate and harmonize cybersecurity.

Mr. Reese, as a State, you are not dealing with just one Federal agency. You are dealing with a bunch of them. I mean, industries might be dealing with a limited number. You are dealing with all

of them. Is that not what you are asking for, give us basically kind of a one-stop shop to go to, to pretty well dictate—and I hate to say this—within the Federal Government, this is how you are going to develop—this is the framework under which you are going to regulate cybersecurity so we do not have that?

Mr. REESE. Right, so most of the discussions we have had in the past have not been so much about who but how. And, as States, we have an organization like NASCIO where we as States come together and collaborate on a regular basis, and they help facilitate opportunities where we can begin conversations. And, we have begun some conversations with our Federal partners. We have not made a whole lot of headway, and we certainly are looking to this group to help champion some real change, hopefully; but really the how, and I think that is through a collaborative effort. We really want to avoid making those kind of decisions in a vacuum, getting everybody at the table, and making sure that we are in a collaborative environment where we are looking across the board at the different industries and then looking at the impact to States and looking for that true collaboration and shaping and sculpting something maybe from the ground up that is more functional and efficient.

Chairman JOHNSON. Yes, from the ground up, but it has to come eventually to a point, to the top of that pyramid where the decisions are made and things are harmonized. Mr. Garfield, I will let you have the last word on this.

Mr. GARFIELD. Yes, the infrastructure is there, so NIST develops the standards. You do not want a regulatory body developing the standards, as Mr. Nutkis pointed out. And so, the actual strategy, the framework, NIST is there. They are doing it. They are doing it well.

Chairman JOHNSON. But, everybody is going off in different directions on that.

Mr. GARFIELD. Yes.

Chairman JOHNSON. So great, you have NIST. But, you still need somebody to have the power to make sure that everybody is handling it the same way.

Mr. GARFIELD. We also have a cybersecurity coordinator. In the previous Administration, it was Michael Daniel. Now it is Mr. Joyce. I think part of what we are encouraging is that that role or some other role play this part in driving coordination and avoiding redundancy.

That does not mean we are getting rid of the Agencies and their role in cybersecurity. This is multifaceted, and it has to be dealt with in that way. But, it would be helpful to have an entity, a person, a group of people coordinating all of the Agencies, bringing it together, making sure it is working in a holistic risk management approach.

Chairman JOHNSON. The last point I will make is if it is just a person in an Administration, that could change every 4 years, or sooner than that. I think we really need to identify a department—if that is going to be DHS and the NCCIC, we need to identify that. We need to empower that department so that there is consistency long term in this. Senator McCaskill.

Senator MCCASKILL. Thank you, Mr. Chairman.

Yes, in fact, the "I" in CCIC stands for "Integration," and when we passed the bill, I think we envisioned that DHS would be the locus of the integration, while NIST provided the standards. That is why I am so concerned about this effort at Health and Human Services.

Mr. Nutkis, when did you learn about the effort at HHS to essentially duplicate what we were trying to accomplish through the legislation that we signed into law at the Department of Homeland Security?

Mr. NUTKIS. I am not exactly sure when I found out, but I do know I found out through the media. I did not find out through our partnership with HHS, and it was not that long ago.

Senator MCCASKILL. And, are you confident that it is going to duplicate efforts that are already underway? Is there any additional benefit you see coming from HHS trying to create its own entity for integration of cybersecurity policy?

Mr. NUTKIS. I cannot state that there is no value and I am not sure that I am cognizant of all the potential that—and what they want to focus on. I can only talk about what we understood the rules to be and how the role of industry and the role of government were supposed to play and now we have changed the rules.

The rules were there was supposed to be information sharing organizations that we established either at a sector level, a segment level, or a community of interest level to be able to facilitate information sharing and share with government, and that provided the organizations to be able to understand which ones provided the most value. And, we could have sub-information sharing organizations so that they were value-based and there was transparency around—as a matter of fact, DHS was establishing a standard. So, it was not one size fits all, and you could have a best of breed, so if you felt that you were a small organization, there was a community of interest for you. So, those ISAOs were able to innovate.

What we have now done is say we are just going to—the government is going to come in and help us, and we are not sure exactly where the help is needed. There is no question more can be done. The question is: Did we evaluate what was going on and where the help is really needed?

Senator MCCASKILL. I think this is probably another issue around this we have to talk about. One of the reasons the Cybersecurity Act of 2015 is so important is because of the safe harbor it provides. We are trying to incentivize this integration so that we can evaluate real risk and real threats. And, some of the briefings we have had around here in the last few months, classified briefings, have only tightened my grip on the sense of urgency that this is a real danger that our country faces, this threat from cyber warfare.

Do you have confidence that the safe harbor liability protections that we put in that act that apply to DHS even apply to the HHS effort, HCCIC?

Mr. NUTKIS. I only know from reading the CISA Act, like everybody else. It is not a listed agency in CISA.

Senator MCCASKILL. Right. So, are you all currently sharing information with HCCIC?

Mr. NUTKIS. We do not. We share information with the NCCIC.

Senator MCCASKILL. And, I assume that this is a common view of people that are regulated by HHS that it is safer and my understanding is that they want you to share directly without redacting?

Mr. NUTKIS. I am not aware of the expectations of the HCCIC. I do know that the expectations of the thousands of organizations that share with us is we anonymize the information before sending it on to DHS and that we also spent a considerable amount of time having to go back to thousands of organizations to ask them to provide us with the waiver necessary for them to do that.

Senator MCCASKILL. Have you voiced the concern you have about a regulator that has the ability to levy fines also being the point for information sharing? Have you shared that with HHS?

Mr. NUTKIS. I believe we have.

Senator MCCASKILL. And, what was their response?

Mr. NUTKIS. I am not fully sure we ever got an answer.

Senator MCCASKILL. Let me talk to you, Mr. Reese. While I would hope that we would all kind of join hands and try to force as much integration as possible through the NCCIC, through the Department of Homeland Security, because of the efforts we made to codify not only protections for the private sector but also integration in that locus for cybersecurity information sharing with the private sector, but maybe the help that might kind of tell HHS to back off or tell other Agencies we are going to do integration through NCCIC, we are going to do standards through NIST, would maybe be the Federal CIO. Do you believe that the Federal CIO—it would be important for the President to nominate a new Federal Chief Information Officer so that you would have an identified contact that has similar responsibilities at the Federal level that you have in your State?

Mr. REESE. I think that is certainly a very interesting conversation because that is one of the challenges we certainly have, is when we are dealing with so many different Agencies and so many different disparate frameworks and regulations, where do you contact, who do you contact, who do you call for a particular one, and that they all overlap. And, when you are dealing in our environments where we have unified across a State an entire Executive Branch, we are dealing with public safety information, health information, IRS information, all collectively on similar systems. And so, when we have some of these challenges, we are not even sure who we should be seeking out guidance from because there is not a single contact. And, when we often get that guidance, it is usually not something that is very consistent.

Senator MCCASKILL. Well, I certainly would like to join with the Chairman in a bipartisan effort to contact the Administration and let them know that not only are we anxious for them to nominate someone, that we would like to empower them to be somebody who is identifying the conflicts and identifying this issue of NCCIC versus HCCIC, and why is this even happening, because then maybe they would be in a position that they could throughout the government be a point of contact to deconflict and help all of these various private sector entities that are struggling with we want to do the right thing but we just cannot—we cannot do all of the right things because they are not even consistent with one another. Maybe you and I could join——

Chairman JOHNSON. I am happy to work with you. In fact, we have three Executive Orders on this. It is obviously recognized as a problem.

Senator MCCASKILL. Yes, but we do not have the guy in charge.

Chairman JOHNSON. Right. So, we will work with you on that.

Senator MCCASKILL. So, it would be great if we could get that nomination done, and maybe this would be a letter they would look at since maybe you would sign it.

Chairman JOHNSON. They are looking at all your letters. [Laughter.] Senator Daines.

Senator MCCASKILL. I winked when I said that. I was not being confrontational to my friend, the Chairman. [Laughter.]

OPENING STATEMENT OF SENATOR DAINES

Senator DAINES. Thank you, Mr. Chairman, Ranking Member McCaskill, and thank you all for testifying today about this critical area of national security. I was struck by the chart. I thought we were going to be talking about regulations. I did not know it was about spaghetti today. [Laughter.]

That is a sobering-looking flow chart. I am not sure you could use the word "flow" with that chart. Let us just say that redefines complexity.

Policymakers continue to debate the best approach to implement cybersecurity standards. Despite Congress' attempt to get ahead of cyber crimes in 1986—that is going back to President Reagan's second term—with the Computer Fraud and Abuse Act, most legislation and regulation in this area has been in response to a high-profile breach, arguably very reactionary.

Over the years, best practices have emerged. They apply broadly but certainly, as we all know here, it is all about the details, and the devil is in those details. I spent 12 years in the cloud computing industry before I came to the Hill. I understand how important it is for business to guard networks and sensitive data. And, I do not believe we can mitigate this threat by burdening companies with more one-size-fits-all regulations. If there is something that ought to frighten the private sector, it is when Congress, who does not really grasp the details and the challenges, dictating technologies to industry. Some of our best and brightest in the tech sector are, I am always a bit nervous with tech mandates. To quote Senator Mike Mansfield of Montana, he used the words "Tap 'er light." I think that is appropriate advice as we think about this. However, we need to encourage and share best practices and, importantly, punish the criminals and enforce the law.

The debate over cybersecurity standards typically leads policymakers to one of two conclusions: first, the Federal Government should mandate baseline requirements; or voluntary standards, such as the NIST framework should be kept for companies to apply as they see fit. I might argue there is perhaps a third option. There is an old adage in the private sector: "If you aim at nothing, you will hit it." Consider your credit score for a moment, an industry-recognized ranking system based on quantitative data, so taking something that can be somewhat complex and qualitative in nature and quantifying it, your credit score. It enables informed decisions about risk. A score that ranks an organization's cybersecurity prac-

tices based on empirical data would allow consumers to make informed decisions. This approach allows the market to decide and incentivize companies to strive beyond the threshold of regulatory compliance to become industry leaders in cybersecurity.

I know when we were running a cloud computing company, we hosted in our data centers many Fortune 500 companies. We had, as is the best practice in the industry, outside groups that would seek to penetrate our systems here and issue reports to us good guys acting like bad guys and telling us what they found. That is a very helpful way to think about security, and I know it is generally a best practice in the industry.

Mr. Garfield, would you agree that neither purely voluntary frameworks nor overly specific Federal mandates are the best approach?

Mr. GARFIELD. I think the answer to that is yes. As it turns out, NIST is engaged in an exercise in updating the cybersecurity framework where it is looking at metrics and measurements. To the point you made earlier about "tap 'er light," I think we have to be thoughtful in the approach that we take.

For example, the Fair Isaac Corporation (FICO) score that you mentioned is fairly straightforwardly quantitative. How we do that and turn something that is complex, sometimes spaghetti, into something that is fairly straightforward and makes sense will require the kind of multi-stakeholder engagement that you are talking about.

Senator DAINES. The only thing worse than doing nothing is doing something that drives the wrong behaviors, the wrong outcomes, certainly, and it will take thoughtful dialogue. And, I am pretty confident—spending some time with our best and brightest in the private sector, and as well engaging those in the Federal Government and State governments—we could come up with something here that would be a quantitative indicator. But, it is just an idea to throw out there, something that would be actionable going forward.

I want to talk about the support for Rapid Innovation Act. This concept for an empirically driven cybersecurity score was the product of research funded by DHS's Science and Technology Directorate. Through technology transfer, this investment is becoming a viable market-based solution that can adapt to trends in cybersecurity as they emerge. I believe as a government we should be investing in forward-looking solutions like these as precisely the objective of my Support for Rapid Innovation Act, which would allow DHS to foster and enable progress rather than impeding it by setting these static requirements that oftentimes would be obsolete by the time Congress got around to acting.

To the panel, the question is: Where is the Federal Government currently expanding resources for negligible benefit? And, where should it focus its resources as it relates to cybersecurity? I am throwing that question out to see who would like to take it first.

Do not jump all at once.

Mr. GARFIELD. Well, I think we have given some examples. For example, the—and by saying "negligible," I do not mean to suggest that it is not important. So, whenever there is a new area of innovation, there is a rush to jump in and regulate. So, the Internet

of Things is one area. As I pointed out earlier, there are 30 different initiatives aimed at regulating that. I think there is negligible benefit to approaching IOT and IOT security in that fashion. And so, I would say that is one area where resources are being misdirected. The National Highway Traffic Safety Administration (NHTSA) is undertaking an effort looking at cybersecurity solely in the automobile instead of engaging and coordinating its efforts through NIST, which is advancing an initiative based on cyber physical systems, and so the very thing that they are also advancing. And so, I think that effort is also going to be negligible because the experts are elsewhere and the likelihood that you are going to be as forthcoming with a regulator as you would with a scientist I think is misguided, as some of the other witnesses have pointed out. So, those are two examples where I think we can streamline and reduce redundancy.

Senator DAINES. That is very kindly put. Thank you.

Mr. FEENEY. I think it is good money spent when you fund NIST, especially relative to some of their innovation work. So, they are doing considerable work in quantum. For instance, they are looking at IOT. Both of those are relevant and important. They will be upon soon, if not already. So, when you can focus on programs like that, they make real sense for the fuller marketplace. So, that is where I would spend time and effort.

We are a little bit unique in that we are working with independent regulators. They are not subject to the Federal mandates, if you will. So, our view of it is really concentrated within the industry. But, innovation is important. A number of our regulators are working on innovation as well.

Senator DAINES. Thank you. I am out of time. The thoughtful conversation, I appreciate it. This is a town that has a culture of rewarding activity and not results, and we have to get focused back on outcomes here versus checking a box, well, we did all these things here and think that Members of Congress are going to nod their head and think they are bluffed. But, I think we need to focus on the result.

Thank you, Mr. Chairman.

Chairman JOHNSON. Senator Heitkamp, and I do want to thank you for switching the order here to accommodate Senator Daines.

OPENING STATEMENT OF SENATOR HEITKAMP

Senator HEITKAMP. You bet. Not a problem.

I am going to give you another analogy, and one is a bike lock. When I was in college, you had a chain. It had a little padlock, right? And, that was enough of a deterrent. And then, pretty soon people came with wire cutters, and, now we have titanium locks, and people are taking their bike seat off, and the bottom line is it is always going to change. And, if we do not have a system that is adaptable, if we do not have communication and adaptability, then all of this means nothing, I mean, because there is a back door somewhere.

And so, the innovation that Steve talked so eloquently about is absolutely critical, staying ahead of where the threat is and being nimble and being diverse. And, that is the challenge that I see, which is one size fits all may be the most dangerous thing we can

do, is applying, one system to all of this because, number one, it will tap down innovation, but it also will create greater vulnerabilities if we are only doing the same thing over and over again.

And so, this is an area that I think there is incredible bipartisan concern, but also a willingness to look at that, and we can all say that is not where we want to be. And, as a former State official, I can only say I feel your pain. Back in the day before we had all of this technology, I was the tax commissioner—and he nods, and he knows what those IRS audits are, and rightfully so. They want to protect their information. There is a lot of great information sharing. We could not do what we do in terms of enforcement without a relationship with the IRS. But, a lot of that is box checking. It is not real security. It is you have the checklist, you go out there, you ding someone because there is the wrong kind of door as opposed to what is the actual breach.

And so, I want to go to what you are seeing in State government because State government is not as complicated as this, but it definitely is a laboratory for innovation and a laboratory for coordination. And, I want to give you a chance, Mr. Reese, to tell us what you have learned in your role not just in Oklahoma but your role as heading up the Chief Information Officers organization and give us the five things you want us to do.

Mr. REESE. Fantastic. So, what a great opportunity, right? Because being a part of NASCIO, we work with all 50 States and 2 territories, and I assure you what we hear across every State is the same story over and over again. There is overregulation, there is duplicity, there is inefficiency. We can give multiple examples where we are making check-the-box decisions instead of being allowed to work with our Federal partners and make good business decisions.

Things like cybersecurity and dealing with these odds is not just a simple check-the-box type of technology. You have to look at the opportunities. I have had scenarios where, in Oklahoma, because for the last 5 years we have been in a State of flux—we have been going through this consolidation of all of our IT within the Executive Branch and have made tremendous strides and have found tremendous savings and efficiencies. However, we still run up against a lot of hurdles because it becomes very troublesome trying to align with our Federal partners who still treat us as if we are siloed. Here I am working and am incentivized by our Federal partners to consolidate, but when I go engage with my Federal partners, they are not consolidated, and they still treat me as if I am siloed, and, therefore, I end up losing all of my efficiencies because I have to do these repetitive processes.

Senator HEITKAMP. Right.

Mr. REESE. I also make these decisions where, if I know I am working with an agency, and I have great examples of some aging hardware at an agency that was reaching end of life, and I knew I had a plan during the consolidation that I was going to be moving all of that network infrastructure over onto our on-prem shared solution, and, therefore, would be on a newer solution. But, when the auditors came in and identified that hardware was not on their list of approved versions of hardware, they said no, we have to replace

that. We said, wait a minute. We are going to replace it. We have purchased extended maintenance on it so we have mitigated the risk, and we would like to take those dollars and go apply them somewhere else, say on an application layer security, because we know that we are also going to be absorbing it later. Did not matter. We had to check the box. We were forced with making a decision of spending the money to go ahead and replace a piece of hardware before we were prepared, before it was even an appropriate return on investment, and we ended up making that check-the-box decision instead of getting to make a good business decision, which is what I was charged to do in this role, was to go make good business decisions with our Agencies. Those type of scenarios come up over and over and over.

Senator HEITKAMP. So, if we gave you a place that was responsive to this, that was an override that was looking at a broader kind of spectrum of concerns—so let us say in that case they say go buy this equipment, you go, I am going to take this to the Council of, You Are Crazy, and I am going to plead my case that that is not reasonable. I think one of these things that you get is that when things are siloed here, the right hand does not know what the left hand is doing. They are not familiar. They are just like do not confuse me with the facts and your problems. This is my problem, and I have to make sure that you have this.

So, if there were a place, and maybe thinking about this, if there were a place where you could go or industry could go to say, no, I am not going to do that, and I do not want to be dinged for it; I have a logical reason; I am going to appeal your decision someplace so that you have to be accountable for the disruption that you are creating that does not make a lot of sense, because States are very similar in this role to industry. They are the users. They are the regulated in this case.

And so, it seems to me that if we had some place where you could go to say this is not smart in terms of overall security, and you did not get forced into this by the time crunch of an audit or dinged on an audit, that might be helpful.

Mr. REESE. Absolutely. Timing is such a challenge. The Oklahoma Tax Commission is a fantastic partner to me and my organization. They have been great at working with us to find efficiencies in what we can do together, and we have been able to achieve some really good things with those folks. But, yet it comes down to some things that you think would be simple, but because the technology is ahead of the regulations, we find ourselves struggling for guidance.

The Oklahoma Tax Commission recently worked with us on moving to a hosted voice solution, and in trying to determine how we deploy and meet all the Federal requirements for the IRS and others for this solution, we found ourselves struggling with trying to determine what set of standards do we use. Is it the voice regulations or is it cloud-based or hosted solution-type regulations? They do not match. And so, we end up seeking guidance, and it takes months.

Senator HEITKAMP. I think Mr. Garfield wants to add to this.

Mr. GARFIELD. If I could just add that what Mr. Reese is saying is so real, and we hear it so often at the State level, but we also

experience and see it at the Federal level as well. And so, this is a broad-based problem that requires a solution.

Senator HEITKAMP. I just want to make one final point, and that is about risk taking. Everybody has a checklist, and they want to meet that checklist because if something happens, they want to say, "I did my job"; as opposed to "I am part of an evolving, necessary, very dynamic industry that needs to be mobile and agile," and we need to tolerate to some degree—and I am not saying that this—but we need to tolerate that this will not be perfect, and we are going to learn as time goes on. And so, we need to tell people, "Do not do things that do not make sense, and if it did not make sense, we are not going to ding you if something happens."

So, that is part of the problem here, that when you have enforcement actions, the dinging or the risk taking does not happen because people are so afraid that they will be held accountable.

Mr. NUTKIS. Can I add one more thing? Because I think in industry we have tried to innovate, and I think this has been the concern that we have had is we have looked at things for years from risk. We transitioned from compliance-based to risk-based. We have worked with cyber insurance actually to be able to understand how risk scores actually work and how we can develop better frameworks to do this. But, we are driven by a compliance and a regulatory environment that says, just as you said, here is the box. But, I would not—I would certainly look at what industries are doing because there is a lot of work already in place. In industries, we have been doing it for 10 years. We have thousands upon thousands of organizations, tens of thousands, that get assessed against this every year, and it does meet the requirement of HIPAA, but, again, the requirement here is to manage risk, not to check the box.

Senator HEITKAMP. And, we need to be sending the message to the people who are reviewing it, because they are box checkers and they need to be in the risk assessment business. I totally agree.

Chairman JOHNSON. At an earlier hearing on a separate subject, at the end of Senator Heitkamp's questioning—and I am paraphrasing. Maybe this is not an exact quote. "This is crazy. This is insane." I was kind of actually waiting for that. I think what you are seeing here is we are kind of working toward what hopefully will be a bipartisan solution and working together on this. So, thank you, Senator Heitkamp. Senator Lankford.

OPENING STATEMENT OF SENATOR LANKFORD

Senator LANKFORD. Thank you, Mr. Chairman. And, I thank all of you for being here. Mr. Reese, good to see you again. Glad you are here. Thank you for the work that you do in Oklahoma all the time.

I want to be able to highlight several things with you today. One is a point of reference on different Agencies and entities that you interact with. DHS and the FBI, just to be able to give you a point of reference for all of the four of you as well, I just walked out of an Intel hearing that is an open hearing today dealing with cyber attacks from Russia and how they are influencing that, and specifically going after State election systems.

There is this myth that all of you know well is just a myth that foreign actors, whether they be North Korea, Iran, Russia, or China, are interested in hacking into the Pentagon, but they are really not interested in anyone else. That is completely false. We have 21 States during the last election time period that Russians were trying to hack into specific State election systems. They were not able to get to any of the vote tally areas or controlling voting machines, but they were able to get to things like voter registration rolls. And, it raises the question: If they can get into a voter registration roll, could they add people? Could they delete people? Could they change data? Could they complicate the process on election day? If they can get to that data, what else could they get to?

So, you have in front of you the now famous—I should say "infamous"—email that was sent to a DNC employee named Billy Rinehart.[1] Billy never intended to be a national example, but he suddenly became a national example as an employee of the DNC. He was on vacation, was in Hawaii, actually, and he opened up his email and saw this email from Google. And, the email simply reads, "Someone just used your password to try to log into your Google account," had his email address there, and said the location was from the Ukraine. So, it encouraged him to change his password, which he promptly clicked on that, changed his password, and went back to bed. What he actually did was just opened up a portal from Russia into the DNC, and they began exfiltrating data of large quantities based on that. Billy was not the only one that clicked on that. There were others that did from that same email.

So, the question is for the Federal Government and for State governments, it is always the conversation about the weakest link. And, you have regulators hanging over you asking you how many connection points, how many possibilities of logging in. Where is your latest hardware? Have you updated this router in this place? There is a vulnerability. Do you use certain software for virus protection? Where does that information get routed? Has it stayed in the United States? Is it routed through Russia? All of those basic questions that are coming at you all the time.

The issue that we are trying to figure out is how to be able to give you a consistent voice and where does that even go.

Mr. Reese, your statement before that in the consolidation that we did in Oklahoma, which was a very real consolidation where we saved a quarter billion dollars through the work that you did and the others that are around you did through the work that happened there, your testimony that the biggest hurdle that you had was not the consolidation; it was the Federal Government and the regulations and the multiple answers that you were trying to get in the multiple audits that are now coming at you. How do we manage this? This is a real threat. Ninety-one percent of the hacks that come into our Agencies come in through a phishing attack just like that. Some employee clicked it; they now have access. If they now have access to health care data, to tax data, it is connected by forms to other places. How do we manage this best? And, do we need a single point of contact to be able to manage this from a Federal side, as all of you are doing on the State sides? Or what is the

[1] The email submitted by Senator Lankford appears in the Appenidx on page 92.

best way to be able to continue to manage how that data flows rather than having multiple entities?

That is a long, rambling question, but somewhat I want to be able to expose this issue, because I think a lot of Americans think somehow it is some hack that got into a system. Most often it looks just like that. That is just how they got into the system.

Mr. Reese, do you want to try to attack my rambling question?

Mr. REESE. Absolutely. So, to be able to manage these types of scenarios, which we see every day, when we tackle this one, there will be another one tomorrow, right? That takes a tremendous amount of resources. Today we find ourselves—training and awareness is in the forefront of how we protect a State. We have 33,000-plus employees statewide that have access to some degree or level to secure State information. And so, obviously things like this are very difficult because it is about end-user awareness and training, and all the systems we have put in place may not be able to protect us from this.

However, being able to commit those resources and the team that we have and being able to manage the staffing, that is a huge challenge to manage, to actually retain staff, the talent we need in Oklahoma to do this.

Now, NASCIO, polling all 50 States, finds on average the State CIO's office for each State has anywhere from 5 to 15 cybersecurity analysts full-time. That is not a very deep bench. And, where we are constantly struggling to be able to train and retain these folks and trying not to lose them to private industry for sometimes better, higher-paying jobs, we also find that they get very frustrated because when they are working within the State government, they are working with all the different Federal Agencies that we touch. We find this scenario kind of like a well-trained physician who has gone to school for many years and practiced and wants to go heal people, and he finds himself in a practice where he is being told, "Just put a Band-aid on it and move on. You do not have time to treat the illness. You have to just put a Band-aid on it."

Our cybersecurity folks feel like that is what they are being told, "Put a Band-aid on it. Check the box. Move on." There are too many things behind this to worry about, so they cannot go focus on the true issues. They cannot go out and find the next innovative solutions, look at the tools that are available to them, or develop the tools that are necessary in many cases to protect the way we know we could. And, that is kind of the struggle we have, which is——

Senator LANKFORD. So, how do we fix that?

Mr. REESE. So, I think we have to simplify the communication, first off, like you said. I can just only imagine the man-hours that could be saved within a State if we were to simplify these regulatory challenges we have. I could focus these folks more on these type of issues and less on just doing audits alone.

Some great examples we have, like the State of Maine documented last year they spent over 11,000 hours in audits. These are the same folks that are trying to address these problems. Eleven thousand hours were spent on audits, working with six Federal Agencies and trying to review over 1,000 pages of regulatory compliance. They could do some pretty amazing things if those man-

hours could have been truly focused on forward-thinking solutions rather than just trying to check the box and appease——

Senator LANKFORD. Filling out paperwork, trying to track down answers to someone's questions, yet another audit from yet another agency, multiply the audit that just came 6 months ago from somebody else, and on and on.

Mr. REESE. Exactly.

Senator LANKFORD. Let me make just a quick comment, and then let me get this back to the Chair. I can assure you the Russians were probing our systems in 2016. They are actively pursuing what they are going to do for 2018 elections. Each State manages their State's integrity of their voting systems and what happens there. I know you are all actively involved in that. But, if they are able to engage in any State election system, alter any data or exfiltrate any data in 2018, I cannot imagine the pressure both on that State and on the Federal Government to be able to explain when we had 2 years of warning.

So, that is all something you are all aware of. That is nothing new to any of you. You deal with those issues all the time. But, it is something that we have to pay attention to here, and I know you are paying attention to, and I appreciate what you are doing to be able to protect the integrity of the systems and a lot of very personal data that our systems have.

Chairman JOHNSON. Thank you, Senator Lankford.

I will also point out, just pay attention to the trial in Montenegro about what Russia did, basically a coup attempt prior to their election. So, this is not something unusual or they just do in America. They are attacking countries across the world. Senator Peters.

OPENING STATEMENT OF SENATOR PETERS

Senator PETERS. Well, thank you, Mr. Chairman, and I will concur with that last comment. I just came back from Lithuania and Latvia, which are also subjected to constant attacks from the Russians as well, and very concerned about their security, and being right on the border with Russia puts them at significant risk. This is something we have to grapple with in a broad-based way, and I appreciate this hearing. And, I certainly appreciate each of the folks who have testified today. I think without question cyber is the most significant national security risk that we face, and the fact that we are coming together to figure out how to do this in a more effective way is incredibly important.

But, I want to focus on one particular industry that I have been actively engaged with, will continue to be actively engaged with as a Senator from Michigan, and it is the auto industry. Perhaps the most transformative new technology that is coming down the pike that will be every bit as big if not bigger as when the first car came off of the assembly line, and that is autonomous vehicles, which will be changing how we think about mobility. It is going to offer some incredible promises in terms of safety. We can eliminate most auto accidents, and at a time when 40,000 people die on our highways every year, that is a big deal, in addition to all of the other injuries that occur. You will be able to change the way vehicles are out on the road as far as spacing, as well as how we organize our communities, all of those wonderful things. But, by the same token,

all these vehicles are going to be connected to each other, and it only works with vehicle-to-vehicle technologies, where a Ford is speaking to a Toyota and a Toyota is speaking to a Nissan and then a GM, and the infrastructure will be talking to these vehicles as well. We will have bridges that will tell our cars that they are icing over, and the cars will automatically respond to that incredibly important and exciting technology.

But, with a shift in technology, we also have to make sure our policies are keeping up with that and, in particular, when it comes to cyber. As I have often said, it is one thing for someone to break into your bank account and steal your money. You are pretty angry about that. If someone breaks into your car and drives you into a wall, that is existential. That is considerably worse. So, we have to make sure we are hardening these systems.

SAE International, a standards development organization for engineering professionals, has begun to promulgate some basic standards for the automobile industry, such as taxonomy and definitions that currently have been serving as a basis for Federal AV guidance. In fact, I am working on legislation now with Senator Thune to deal with some AV guidance issues as well.

But, Mr. Feeney, I am going to start with you. For the auto industry, even a small number of conflicting or duplicative regulations would obviously significantly impact AV technology development. To maintain the current pace of innovation, what are your thoughts on the role of voluntary risk-based guidelines as a technical basis for future AV cybersecurity standards?

Mr. FEENEY. Right. Thank you for that question. I think it is critical. I have been a control owner, if you will, in cloud operations. I have been a CIO, and now I am doing more work on the policy and governance side. And, what I find is that the closer you get to a framework—we happen to like NIST, and we actually think about it in a customized way. It incorporates risk, it incorporates judgment, it incorporates flexibility to adapt, which is something that is critical in the space you just described, and it will adapt fast. It allows you to be nimble.

So, I think if you set standards, you adopt them ahead of time, you build in by design the approach you want to take versus bolting it on later, that is a critical aspect of getting it right. It will never be 100 percent right. We mentioned some of the things that go on in this space. It is a dynamic threat environment from the external side. But, you have to have those bases in place in order to accomplish what you are looking to do, and I think that is an appropriate and probably best practices way to go about it.

Senator PETERS. Any thoughts?

Mr. NUTKIS. Yes, I would agree with that. So, from our perspective, we certainly develop and are based on risk-based. Because we saw the whole threat landscaping and our previous iterations were based on our breach data and how we looked at the threat based on a retrospective, we actually went prospective now to say that we are going to look at the emerging threats and actually build those into our framework so the framework becomes more threat-based, even risk-based. So, based on the threats that we see emerging, the framework actually evolves.

The one caution I would make is understanding how you measure the effectiveness of the framework and then also transparency. Just because you have a framework, how do you ensure that they are actually complying with it effectively? And then, when one person looks at it, just as we heard from Mr. Reese, you could have 14 audits using the exact same set of guidance and get 14 different results. So, ensuring that everybody knows how to do that.

Senator PETERS. Mr. Garfield.

Mr. GARFIELD. Yes, I think the example that you just gave speaks to the convergence that is taking place in our world, but also the lack of convergence that is taking place on the policy side. And so, that is why standards are so important, because they speak to and accomplish all of the things that the other witnesses have pointed to. But, as well, the oversight both from the Congressional level but a central point in the Executive Branch where we can avoid these redundancies on top of that broader strategy and that flexible framework is absolutely essential and important as well.

Senator PETERS. Mr. Reese.

Mr. REESE. So, in Oklahoma, from a State perspective, when we look at things such as autonomous vehicles, you start looking at from a State perspective the intelligent transportation systems, we work very closely with our Oklahoma Department of Transportation, and we have done a great job focusing on where we can help them with financial systems and administrative systems alike. And, when we get into things that are really specific niche areas, such as intelligent transportation systems and how they manage and share those, the challenges we get into when we sit down at the table and we start talking about how we are going to leverage the State's infrastructure or how we are going to leverage the State's cybersecurity efforts and the things that our security information officer has put in place to protect all of these systems, they start feeling challenges and pushback from their Federal partners who tell them, "No, no, no, no, no. When it comes to intelligent transportation systems, you are basing a lot of that infrastructure and building it out on Federal dollars." And, their Federal partners are telling them if that control in any way shifts to a centralized IT office, such as the CIO's office, they are going to lose funding. And, that is truly the mind-set that a lot of Agencies have because they are basing that on past audit experiences they have had, from third-party auditors that came in, and they are making the determinations and setting that example of how those Agencies now interpret what they should be doing and how they should be engaging with my office and moving forward, and often, without proper guidance and being able to get questions answered timely, we end up using the most restrictive interpretation of the Federal guidelines and it costs us more money, and it slows us down.

Senator PETERS. All right. Well, thank you for your thoughtful responses from all of you. I appreciate it.

Chairman JOHNSON. Thank you, Senator Peters.

I want to thank all of our witnesses. Normally, I say this before the hearing, but we had the business meeting. But, I talk to the witnesses, and I say the purpose of this hearing, of every hearing, literally is to lay out a reality, to define the problem so that you

can find areas of agreement, to work toward a bipartisan solution. I think you saw that is exactly what happened here today. I want to thank all the Committee Members, Senator Peters, my Ranking Member—who is at a Finance Committee hearing. We are juggling a lot of balls here. But, I think what you have witnessed here is by laying out a reality, by defining the problem, by looking for areas of agreement, I think this is an important hearing. I will encourage everybody to take a look at your thoughtful testimony, which is in far greater detail than what you were able to provide just in terms of your verbal testimony. We have really described the problem in a way that we can all take a look at what the solution needs to be. And, it is about harmonizing. It is about integrating.

And so, I am looking forward to working with my colleagues that were here and asked great questions, and let us write a piece of legislation. Working with the witnesses, working with your groups, let us get that central point within government so we can streamline this, so that we can certainly take the burden off of States, the health care industry, the financial industry, every industry, so that we can secure our cyber assets. This is an enormous threat. We have to recognize that. But, again, that is what this hearing really pointed out. So, again, I just want to thank all of our witnesses for your written testimony, your thoughtful answers to our questions, and your verbal testimony.

With that, the hearing record will remain open for 15 days until July 6th at 5 p.m. for the submission of statements and questions for the record. This hearing is adjourned.

[Whereupon, at 11:51 a.m., the Committee was adjourned.]

APPENDIX

Chairman Johnson's Opening Statement
"Cybersecurity Regulation Harmonization"
Wednesday, June 21, 2017

As submitted for the record:

Cybersecurity is one of this Committee's top priorities. Today's hearing is our fifth hearing examining this threat. In other hearings on this topic we explored the importance of information sharing and the need for liability protections; the OPM and IRS data breaches; and the broad cybersecurity threat landscape—criminal attacks, malicious attacks, industrial espionage, and cyber warfare.

The Committee has also highlighted one of the greatest impediments to the U.S. economy realizing its full potential: our regulatory burden. According to the Competitive Enterprise Institute, the total annual federal regulatory cost amounts to $2 trillion. To put this in perspective, this burden amounts to approximately $15,000, per year, per household. There are only seven economies in the world that are larger than the regulatory burden we impose on our economy and American families.

Today's hearing considers both of these problems. Cyber threats are real and growing. As they have evolved, so has the response from government regulatory bodies. Though these efforts are well intended, the result has been a myriad of duplicative, sometimes conflicting, rules imposed on industries throughout the economy. Not only do these rules impose regulatory costs, but they can also lessen security, as companies spend limited time and resources concentrating on regulatory compliance at the expense of security. As an example, one financial services firm reports that 40 percent of its time is spent on regulations and reporting requirements, time better spent enhancing the security of its networks.

In December, I had the opportunity to meet with Dr. Eviatar Matania, the Director General of Israel's National Cyber Directorate. Dr. Matania established a comprehensive cyber strategy for Israel with a direct reporting line to the Prime Minister. The United States would be well served by evaluating Israel's approach and look for opportunities to harmonize the federal government's approach to cybersecurity to ensure consistent, effective, and non-duplicative rules of the road.

We also should re-prioritize our efforts. At our last cybersecurity hearing, former Assistant Director of the FBI Cyber Division Steven Chabinsky testified that:

> We should spend less in anticipation of cybercrime (on antivirus, firewalls, etc.) and more in response—that is, on the prosaic business of hunting down cyber-criminals and throwing them in jail. For this to occur, we will need to reconsider how we fund cybersecurity efforts. . . . Our underfunding threat deterrence also hurts the private sector, which largely has been left to fend for itself. One financial institution disclosed that it planned to spend $600 million and dedicate 2,000 employees to cybersecurity last year.

Today, witnesses from financial services, the tech sector, healthcare, and state government will explain exactly how they are fending for themselves—both in securing their networks and in responding to the current diffuse regulatory landscape. I want to thank all of these witnesses for being here today, and I look forward to your testimony.

U.S. Senate Homeland Security and Governmental Affairs Committee

"Cybersecurity Regulation Harmonization"

June 21, 2017

Ranking Member Claire McCaskill

Opening Statement

Thank you, Chairman Johnson. One of my top priorities as a senator is focusing on how we can make government work better and more efficiently. I have spent my career concentrating on eliminating waste, fraud and abuse in an effort to save taxpayer dollars and improve government services.

Today's hearing allows us to hear from representatives from the private sector and the states about how they manage compliance with the variety of regulations they face related to data and cybersecurity. There is currently no clearinghouse for mitigating conflicts between regulators, and as a result, states and industry bear the burden for ensuring compliance between sometimes redundant and conflicting regulations.

Regulators play an essential role in mandating security measures, like notifications after a data breach and requiring a minimum level of security to protect personally identifiable information. However, as these witnesses

will attest, while the goal of the regulations is improved security, due to a lack of harmonization between regulations, industry spends valuable time sorting through compliance when it could be investing those hours and resources into improving their systems and services.

We'll hear today how centralization of IT systems can play a key role in improving efficiency and security. The same can be said about centralizing cyber policy across the federal government. We have made significant strides in recent years to authorize and operationalize the Department of Homeland Security's (DHS) National Cybersecurity and Communications Integration Center (NCCIC). President Obama also mandated the creation of the NIST Cybersecurity Framework, which creates a common language for government and industry.

We have spent years working to make DHS the central cybersecurity information sharing entity in the federal government. We finally passed the Cybersecurity Information Sharing Act (CISA) in 2015, providing liability protection to encourage industry to share threat information with DHS. But now, the Department of Health and Human Services (HHS) has decided that the NCCIC and the existing information sharing structure have limitations. Rather than examining what the private sector was doing to address potential

gaps, HHS went ahead and built a health-specific version called the Health Cybersecurity and Communications Integration Center, referred to as the HCCIC. Talk about duplicative.

I have questions about the utility of this new entity. It also is not clear to me that this new HHS cyber center is necessary or that it adds value. We should be looking to enhance information sharing participation and the NCCIC's capabilities, not sprouting a "kick" for each industry or critical infrastructure sector.

I'm glad Chairman Johnson is joining me in sending a letter to HHS asking questions about the genesis of the HCCIC, how it has been and will coordinate with DHS, information on the liability protections offered to those that share information with the HCCIC, and why this new entity is necessary.

I look forward to hearing from the witnesses today about other ways we can work to simplify and harmonize their regulatory burden. Thank you.

Testimony of

Christopher F. Feeney

On behalf of

The Financial Services Roundtable – BITS

Before the

United States Senate Committee on Homeland Security & Governmental Affairs

Hearing entitled:

"Cybersecurity Regulation Harmonization"

June 21, 2017

Chairman Johnson, Ranking Member McCaskill, and members of the Committee, thank you for the opportunity to testify before you today.

My name is Christopher F. Feeney, and I am the President of BITS, the technology policy division of the Financial Services Roundtable (FSR). BITS addresses emerging threats and opportunities facing some of the largest financial services firms, particularly those related to cybersecurity, fraud reduction, critical infrastructure protection and innovation. Working with CEOs and their C-suite executives, BITS identifies key issues at the intersection of financial services, technology and commerce, and facilitates collaboration, developing policies and practices to improve the technology environment for member companies and their customers.[1]

In addition to my role as BITS President, I am also a member of the Financial Services Sector Coordinating Council's (FSSCC) Executive Committee and Co-chair of the Policy Committee. The mission of the FSSCC is to strengthen the resiliency of the financial services sector against attacks and other threats to the nation's critical infrastructure by proactively identifying threats and promoting protection, driving preparedness, collaborating with the U. S. Federal government, and coordinating crisis response for the benefit of the Financial Services sector, consumers and the nation.[2] I also hold leadership positions in several other industry organizations focused on addressing the security and resiliency of financial institutions.

In these roles, my charge is to advance policies to protect the nation's financial infrastructure, firms' infrastructure and, most importantly, the consumers that use and depend on these financial systems every day. On behalf of our member firms, I offer the following testimony regarding the challenging cybersecurity regulatory environment, its potential impact on the security of our nation's critical infrastructure, and the financial sector's efforts to work collaboratively with regulators and across our government.

A. Overview of the Financial Services Sector

The financial services sector consists of more than 13,000 banks and credit unions, payment companies, insurance companies, wealth and asset managers and financial market utilities that process transactions, payments and move money across domestic and international markets.

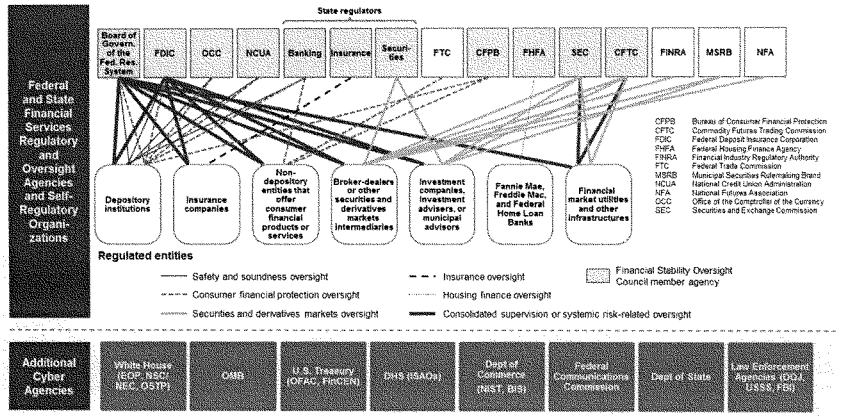
The sector is overseen by nine federal regulators (all of which are independent from the executive branch), three self-regulatory organizations, The U.S. Department of the Treasury (Treasury) as its sector-specific agency,[3] and every state banking, insurance, and securities agency. When agencies tasked with cybersecurity-related authorities are added, the list expands even further (see Figure 1).

---

[1] For more information, please visit: http://www.fsroundtable.org/

[2] For more information, please visit: https://www.fsscc.org/

[3] For more information, please visit: https://www.dhs.gov/financial-services-sector



Note: The figure depicts the primary regulators in the US financial regulatory structure, as well as their primary oversight responsibilities. "Regulators" generally refers to entities that have rulemaking, supervisory, and enforcement authorities over financial institutions or entities. There are additional agencies involved in regulating the financial markets and there may be other possible regulatory connections than those depicted in this figure
Source: GAO; GAO-18-175

(Figure 1. The United States Financial Services Regulatory Structure in 2017 as It Relates to Cybersecurity)[4]

Cybersecurity is a top priority for our member firms. It is a key concern and focus area for CEOs and Boards of Directors, all the way to the frontline defenders sitting at keyboards monitoring network activity. Firms' senior management have made clear that cybersecurity risk is not solely a technology issue, but an enterprise-wide risk that should be considered across all levels of the organization. As such, cybersecurity is a regular agenda item at Board of Directors meetings, often with the Chief Information Security Officer or equivalent providing updates on threats, risks, and strategies for mitigation. With this senior-level support, firms have sharpened priorities and their commitment to cybersecurity.

According to a report published by Homeland Security Research Corp., the financial services cybersecurity market in the United States reached an estimated $9.5 billion in 2016, making it the largest non-government cybersecurity market.[5] Of that number, the top four U.S. banks spent nearly $1.5 billion.[6] In addition, other reports

[4] Figure reproduced from the FSSCC and BCG Platinion May 17, 2017 presentation at the NIST Cybersecurity Workshop event: https://www.nist.gov/sites/default/files/documents/2017/05/18/financial_services_csf.pdf

[5] See: http://homelandsecurityresearch.com/2014/10/u-s-banking-financial-services-retail-payment-cybersecurity-market-2015-2020/

[6] See: https://www.forbes.com/sites/stevemorgan/2015/12/13/j-p-morgan-boa-citi-and-wells-spending-1-5-billion-to-battle-cyber-crime/#7204cf13116d

indicate that firms within the financial sector "...spend more on IT security than any other sector, spending three times as much as comparably sized non-financial institutions."[7]

Recognizing that cybersecurity affects the entire industry, financial firms also have a long history of significant investment and collaboration to improve cybersecurity preparedness, response and resiliency across the sector. For example, prior to the passage of the Homeland Security Act of 2002 and the Cybersecurity Act of 2015, the financial services sector established the cyber threat information sharing and analysis center known as the FS-ISAC – a gold standard for critical infrastructure cyber threat information sharing organizations.

In addition, as a CEO-level organization, the Financial Services Roundtable-BITS has facilitated nine semi-annual CEO-led "Joint Financial Associations Cybersecurity Summits." These summits bring together financial institution CEOs, trade association CEOs, and key Congressional and government agency leaders to actively address sector resiliency, respond to capability gaps, and encourage coordination and investment. Other sector-wide activities include the "Hamilton Series" of cybersecurity response exercises; the establishment of a not-for-profit organization – Sheltered Harbor – that has developed standards for the safe storage and restoration of financial account data in the event of a catastrophic cyber incident; fTLD Registry Services, a secure website domain for banking and insurance companies; and updates and testing of the sector's cyber response plans, including the "All-Hazards Crisis Response Playbook," which provide guidance on intra-sector and government coordination in the event of a cyber incident.

Much of this collaborative work includes regulators, and our government partners at the Treasury and Department of Homeland Security (DHS). Under the DHS National Infrastructure Protection Plan, Treasury is our sector-specific agency and helps organize regular meetings of the FSSCC along with our government counterparts, referred to as the Financial and Banking Information Infrastructure Committee (FBIIC). These meetings help our industry, our regulators and our government partners work collaboratively to improve resiliency and the policies that enable it.

B. Cybersecurity Regulatory Overlap

Industry and regulators share the same goal: To ensure the financial services sector is strong, safe and secure. We support regulators' attention to the critical issue of cybersecurity; however, as recently noted by the Treasury, there is growing duplication and overlap in financial cybersecurity regulations and a need to better harmonize efforts among regulators.[8] We have requested regulators' collaborate more closely among themselves and with industry to ensure that the multitude of layered requirements does not detract from firms' ability to perform critical security work.

---

[7] See: https://go.kaspersky.com/rs/802-IJN-240/images/Financial_Survey_Report_eng_final.pdf.

[8] See: https://www.treasury.gov/press-center/press-releases/Documents/A%20Financial%20System.pdf

Since the publication of the National Institute of Science and Technology's (NIST) Cybersecurity Framework in 2014 – which was intended to provide a common way of identifying and addressing cyber risks – we have tracked the issuance of nearly 30 new or proposed cybersecurity rules, guidelines, tools or frameworks that directly affect firms.[9] While regulators may have different statutory authorities and areas of specific focus, much of the information they seek from firms is common.

Some of these new cybersecurity proposals incorporate the NIST Cybersecurity Framework's organizational structure and terminology, but many do not, instead opting for novel approaches and different language. The lack of harmonization and alignment causes firms to expend substantial personnel and resources reconciling notionally similar, but semantically different cybersecurity proposals and agency expectations.

This unnecessary duplication has been a growing concern of our member firms because it diverts the attention of cybersecurity professionals away from keeping up with dynamic cyber threats and implementing new protective measures, to instead focus on comparing and answering compliance questionnaires.

For example, one firm's Chief Information Security Officer estimated that 40% of his time and that of his team was devoted to reconciling various requirements of regulatory agencies. Due to one framework issuance in particular, the reconciliation process delayed the implementation of a security event monitoring tool intended to better detect and respond to cyber-attacks by 3-6 months. Choices like these are made by firms every day as they work to respond to changes in cyber issuances. Each new issuance requires them to develop or modify operating procedures and reporting to properly respond to examination requests, while also keeping their customers and our financial systems secure.

This challenge is compounded by the shortage of cybersecurity professionals. According to the 2015 (ISC)[2] "Global Information Security Workforce Study," the estimated 2017 shortfall of cybersecurity professionals in the Americas will be 389,000; for 2018, it increases to 516,000.[10] Our member institutions report similarly: One FSR member firm stated that as of last month, it had over 40 open positions related to cybersecurity that it was struggling to fill. This trend is expected to continue, with the global shortfall reaching 1.8 million positions by 2022.[11]

C. Enhancing Alignment to the NIST Cybersecurity Framework

Over the last two years, we have had numerous discussions within our industry and with regulators about a possible solution to the growing overlap and complexity of

---

[9] See Appendix A table 1, plus tables 2 and 3 for additional cybersecurity-related issuances.

[10] See: https://www.isc2cares.org/uploadedFiles/wwwisc2caresorg/Content/GISWS/FrostSullivan-(ISC)%C2%B2-GlobalInformation-Security-Workforce-Study-2015.pdf.

[11] See: http://blog.isc2.org/isc2_blog/2017/02/cybersecurity-workforce-gap.html

cybersecurity requirements. We believe harmonization can be achieved based on the NIST Cybersecurity Framework. Doing so would provide a number of benefits to industry and regulators, and help foster collaboration with other critical infrastructure sectors, such as energy and telecommunications.

The NIST Cybersecurity Framework was developed through a transparent multi-stakeholder process and produced a cybersecurity risk management framework for critical infrastructure based on international standards and best practices. Federal and state agencies, sector-representative organizations and individual private sector entities from across the country participated. The financial services sector was a key contributor throughout the process.

From that collaborative endeavor, NIST issued the "Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0"[12] (NIST Cybersecurity Framework) in February 2014. In passing the Cybersecurity Enhancement Act that same year, Congress codified its approval of the Framework, the process used to develop it, and NIST's role in its evolution. Perhaps because of NIST's multi-stakeholder development process and the Framework's accessibility from the control room to the boardroom, firms began to quickly integrate the NIST Cybersecurity Framework into their information security programs. By late 2015, PwC reported that approximately 91% of companies it surveyed were using either the NIST Cybersecurity Framework or ISO standard.[13] Certain sectors and subsectors, such as telecommunications,[14] electricity,[15] manufacturing,[16] and the maritime bulk liquids transfer subsector[17] worked with either NIST, their sector-specific agencies, regulatory agencies, or some combination thereof to harmonize existing and proposed assessment or regulatory regimes around the NIST Cybersecurity Framework.

As financial sector agencies have issued cybersecurity proposals that use new terminology and methodologies, many firms spend countless hours trying to align their internal processes to the new requirements. To assist financial institutions in the reconciliation process, the FSSCC began mapping a select set of cyber regulations and regulatory proposals against the NIST Cybersecurity Framework. This effort took several months, and once completed, the mapping document was uploaded to a data visualization and analysis tool. The resulting graphic illustrates the complexity in

---

[12] See: https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf.

[13] PwC. "Global State of Information Security Survey 2016." 9 October 2015: http://www.pwc.com/gx/en/issues/cyber-security /information-security-survey.html.

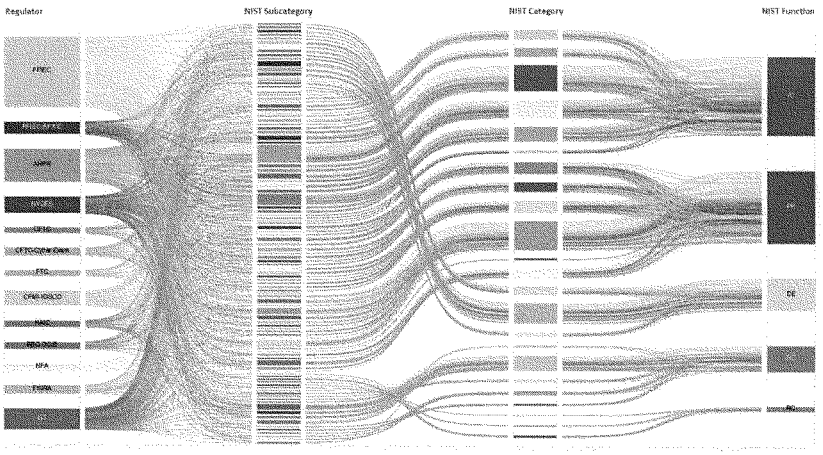
[14] See: https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG4_Final_Report_031815.pdf.

[15] See: https://energy.gov/sites/prod/files/2015/01/f19/Energy%20Sector%20Cybersecurity%20Framework%20Implementation%20Guidance_FINAL_01-05-15.pdf.

[16] See: http://csrc.nist.gov/cyberframework/documents/Manufacturing-Profile-DRAFT.pdf.

[17] See: http://mariners.coastguard.dodlive.mil/2016/11/10/release-maritime-bulk-liquids-transfer-cybersecurityframework-profile/.

reconciling a subset of select proposals against the NIST Cybersecurity Framework (see Figure 3).



(Figure 3. Complexity in Reconciling Select Proposals to the NIST CSF)

The current fragmented approach introduces inefficiencies by requiring institutions to identify, draft, and compile functionally equivalent sets of data from the same systems to satisfy each different regulator and each different regulatory standard. As a result, institutions are forced to create single-use compliance data, rather than focusing their time on developing security and mitigation techniques that improve a firm's cybersecurity program. While each agency proposal or set of requirements may have its own merit, when continuously layered, the added complexity is unsustainable as there are simply not enough cybersecurity professionals available to perform the necessary work. One example of the complexity of cyber regulations is captured in Appendix B, which summarizes the differing expectations adopted by multiple regulators to address the common practice of penetration testing.

The lack of harmonization also complicates efforts to coordinate across critical infrastructure sectors and with the federal government for cyber incident response. A key focus for the federal government and DHS, in particular, has been to foster a "whole of nation" approach to cybersecurity. This effort to foster greater public-private partnership is critical if we are to effectively protect our economy, our customers, and our citizens from cyber threats. As regulations pull financial institutions away from using NIST, this could endanger not only our sector, but other critical infrastructure sectors if a coordinated response is needed.

D. Interactions with the Regulatory Community

The industry first suggested regulators align their efforts more closely to the NIST Cybersecurity Framework in a September 21, 2015 submission[18] to the Federal Financial Institutions Examination Council, a coordinative body for the banking-specific agencies and organizations.[19] This suggestion included a request that regulators work collaboratively with industry to find a solution that would allow regulators to fulfill their responsibilities while better allowing firms to focus on critical cybersecurity activities.

In October 2016, industry (through the FSSCC) and our government coordinating council, the FBIIC, agreed to a joint working group to discuss opportunities to better harmonize cybersecurity related requirements and expectations. The FSSCC had hoped to begin an ongoing and constructive dialogue immediately but the regulatory community requested additional time to organize and prepare for these discussions.

In the interim, industry undertook the mapping project discussed above. In late February of this year, the FSSCC began customizing the NIST Cybersecurity Framework for the financial sector by incorporating key focus areas and priorities of our regulators. This effort is referred to as the "Financial Services Sector Specific Cybersecurity Profile" and is designed to help demonstrate how alignment to the NIST Framework could be used to meet the needs of regulators, assist firms in reducing the compliance burden and satisfy market-specific requirements. This customized profile, along with a proposed set of common examination questions, is intended to help generate discussion with the regulatory community.

In May of this year, the FSSCC previewed draft portions of this NIST customization with a number of financial services regulatory agencies and with the larger cybersecurity community at the NIST Cybersecurity Framework workshop on May 16-17. The draft was well-received by NIST, the private sector, and financial services agency representatives in attendance. Coming out of the meeting, interest in collaboration around this working draft and the proposed common set of examination questions was renewed.

---

[18] See: https://www.fsscc.org/files/galleries/FSSCC_FFIEC_Cybersecurity_Assessment_Comment_Letter_(FR_2015-17907).pdf.

[19] For more information on the FFIEC, including its membership and statutory authorities, please see: https://www.ffiec.gov/. Chaired by the U.S. Department of Treasury's Assistant Secretary for Financial Institutions, members include representatives from the 2) American Council of State Savings Supervisors, 3) Commodity Futures Trading Commission, 4) Conference of State Bank Supervisors, 5) Consumer Financial Protection Bureau, 6) Farm Credit Administration, 7) Federal Deposit Insurance Corporation, 8) Federal Housing Finance Agency, 9) Federal Reserve Bank of Chicago, 10) Federal Reserve Bank of New York, 11) Federal Reserve Board, 12) National Association of Insurance Commissioners, 13) National Association of State Credit Union Supervisors, 14) National Credit Union Administration, 15) North American Securities Administrators Association, 16) Office of the Comptroller of the Currency, 17) Securities and Exchange Commission, and 18) Securities Investor Protection Corporation.

From those interactions, FSSCC learned that under Treasury's leadership, the FBIIC established a cybersecurity harmonization working group. Additionally, Treasury signaled its support and approval of this approach in its recently released report to the President of the United States – "Core Principles for Regulating the United States Financial System."[20] In the report, they recommended greater coordination in two respects: "First, financial regulatory agencies should work to harmonize regulations, including using a common lexicon. Second, financial regulators should work to harmonize interpretations and implementation of specific rules and guidance around cybersecurity."[21] To achieve this, Treasury recommended FBIIC as the coordinative body. The FSSCC supports these recommendations.

E. The Sector's Congressional Requests

Congress has an important role to play in encouraging the agencies to meet with the private sector and coordinate amongst themselves to achieve regulatory harmonization. A multi-stakeholder process of agencies and private sector representatives, similar to the one employed by NIST, is necessary for success.

To foster this collaboration, we encourage this Committee to recommend that agencies pause any in-process cybersecurity related proposals, rulemakings, or other formal activities to allow time for effective collaboration. There are several agency cybersecurity initiatives that if completed and issued[22] would further complicate an already complex regulatory environment.

F. Conclusion

The financial services sector shares the same cybersecurity-related goals as our regulatory community: Advancing the safety, soundness, and resilience of the financial system by protecting financial institutions and the financial sector from increasing cybersecurity risks. Given the complexity of our regulatory environment, a lack of harmonization negatively impacts the ability of financial institutions to devote resources to security activities.

This is only exacerbated by the shortage of cybersecurity professionals, and we hope that all would agree the experts that are available should be able to devote more time to security rather than interpreting notionally similar, but semantically different regulatory expectations.

---

[20] See, p.31: https://www.treasury.gov/press-center/press-releases/Documents/A%20Financial%20System.pdf

[21] See, p.31 and Appendix B, p.123: https://www.treasury.gov/press-center/press-releases/Documents/A%20Financial%20System.pdf

[22] E.g. the advancement of the jointly issued Federal Reserve System-Office of the Comptroller of the Currency-Federal Deposit Insurance Corporation advanced notice of proposed rulemaking on proposed "Enhanced Cyber Risk Management Standards" to the notice of proposed rulemaking stage, a substantial revision of the FFIEC issued Cybersecurity Assessment Tool, and the completion of a National Association of Insurance Commissioners authored "Cybersecurity Model Law"

As discussed, there is a solution: The sector-specific "Profile," if adopted, would provide the harmonized and rationalized approach to cybersecurity regulation our sector needs. We request that you recommend to agencies to pause further cyber-related issuances while the "Profile" is being considered.

We stand ready to work with our regulatory community on this more rationalized approach, and we ask for your public encouragement. It is needed.

Thank you.

Appendix A

Cybersecurity-related Regulations, Requirements, Examination Expectations, and Other Initiatives Affecting Financial Institutions since the release of the NIST Cybersecurity Framework, Version 1.0 in February 2014.

The following tables illustrate the complexity of the cyber regulatory landscape for financial services firms and include rules, guidance, tools and recommendations since the release of the NIST Cybersecurity Framework, version 1.0 in February 2014. These lists are not exhaustive, and inclusion does not represent a judgment of the relative benefits or burdens of each singular issuance.

For a list of statutory and regulatory requirements that predate the NIST Cybersecurity Framework and which apply solely to banking firms, please refer to the FSSCC's September 21, 2015, submission on the "FFIEC Cybersecurity Assessment Tool,"[23] as well as the Center for Strategic and International Studies' (CSIS) July 2015 report, entitled, "The Evolution of Cybersecurity Requirements for the U.S. Financial Industry"[24].

Table A. Regulatory Requirements, Issuances, and Proposals affecting financial institutions' cybersecurity programs directly.

	Issuing Org	Date	Description
1	DE	5/16/2017	House Bill 180 would expand data breach notification law to include requirement that those "conducting business" in Delaware must "implement and maintain reasonable procedures and practices to prevent the unauthorized access to or acquisition, use, modification, disclosure, or destruction of personal information collected or maintained in the regular course of business." http://legis.delaware.gov/BillDetail?legislationId=25794
2	NV	3/20/2017	Senate Bill 395 would require cybersecurity plans for all critical infrastructure in the state. https://legiscan.com/NV/text/SB395/2017

[23] See FSSCC's September 21, 2015, submission on the "FFIEC Cybersecurity Assessment Tool," p.4, found here: https://www.fsscc.org/files/galleries/FSSCC_FFIEC_Cybersecurity_Assessment_Comment_Letter_(FR_2015-17907).pdf

[24] See: https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/150717_Carter_CybersecurityRequirements_Web.pdf

	Issuing Org	Date	Description
3	CO	3/6/ 2017	Notice of Proposed Rulemaking of the Colorado Division of Securities; proposed rules include "guidance to broker-dealers and investment advisers on what factors the Division will consider when determining if the procedures by the firm are reasonably designed to ensure cybersecurity." https://drive.google.com/file/d/0BymCt_FLs-RGUWI5c3lDUVlzeDg/view
4	NAIC	2/27/ 2017	Issuance of proposed "Insurance Data Security Model Law," Version 3. Once finalized, NAIC will move for the model law to be passed by its state constituents via the accreditation process. http://www.naic.org/documents/cmte_ex_cybersecurity_tf_170307_data_security_model_law_clean.pdf
5	NYDFS	2/16/ 2017	NYDFS issues financial services specific cybersecurity regulations, entitled, "Cybersecurity Requirements for Financial Services Companies," 23 NYCRR 500 http://www.dfs.ny.gov/legal/regulations/adoptions/rf23-nycrr-500_cybersecurity.pdf, which takes effect on 3/1/2017.
6	OCC	1/24/ 2017	OCC Bulletin 2017-7 "Supplemental Examination Procedures for Risk Management of Third-Party Relationships," which "expand on the cores assessment contained in the 'Community Bank Supervision,' 'Large Bank Supervision,' and 'Federal Branches and Agencies Supervision' booklets of the *Comptroller's Handbook*," by providing "additional guidance" on, among other things, examination of third party selection and due diligence vis a vis cyber resiliency and contractual clause adequacy in addressing cyber incident notification. https://www.occ.gov/publications/publications-by-type/comptrollers-handbook/pub-third-party-exam-supplemental-procedures.pdf
7	SEC	11/15/ 2016	Order approving the "National Market System Plan Governing the Consolidated Audit Trail," which codifies certain cybersecurity requirements for "Plan Processors." https://www.sec.gov/rules/sro/nms/2016/34-79318.pdf
8	FRB, OCC, FDIC	10/26 /2016	*Federal Register* notice of advanced notice of proposed rulemaking (ANPRM), entitled, "Enhanced Cyber Risk Management Standards," which imposes new cybersecurity regulatory requirements on financial institutions with asset sizes of $50B+ and which is not directly aligned with past regulatory regimes.

	Issuing Org	Date	Description
			https://www.federalregister.gov/documents/2016/10/26/2016-25871/enhanced-cyber-risk-management-standards
9	OCC	9/29/2016	*Federal Register* notice of finalized enforceable guidelines, "Guidelines Establishing Standards for Recovery Planning by Certain Large Insured National Banks, Insured Federal Savings Associations, and Insured Federal Branches," with reference to cyber stress testing. https://www.gpo.gov/fdsys/pkg/FR-2016-09-29/pdf/2016-23366.pdf
10	SEC	9/28/2016	*Federal Register* notice of adoption of a final rule of the "Enhanced Regulatory Framework for Covered Clearing Agencies"; the rule includes cybersecurity related requirements. https://www.federalregister.gov/documents/2016/10/13/2016-23891/standards-for-covered-clearing-agencies
11	CFTC	9/19/2016	Federal Register notice of final rule for "System Safeguards Testing Requirements," which promulgates new cybersecurity testing requirements. http://www.cftc.gov/idc/groups/public/@lrfederalregister/documents/file/2016-22174a.pdf
12	FTC	9/12/2016	*Federal Register* solicitation concerning update to the "Disposal of Consumer Information and Records Rule," which requires properly dispose of consumer report information and reasonable measures to protect it from unauthorized access; solicitation poses question whether disposal requirements should be more prescriptive and/or reference other information destruction frameworks. https://www.ftc.gov/system/files/documents/federal_register_notices/2016/09/160915frn.pdf
13	FFIEC	9/9/2016	Revised "Information Security Booklet" issued for the "FFIEC IT Examination Handbook." https://www.ffiec.gov/press/PDF/FFIEC_IT_Handbook_Information_Security_Booklet.pdf
14	FTC	8/29/2016	*Federal Register* solicitation concerning update to the "Standards for Safeguarding Customer Information" (the Safeguards Rule), which requires financial institutions to develop, implement and maintain a comprehensive information security program for handling customer information; solicitation

	Issuing Org	Date	Description
			proposes incorporation of the NIST Cybersecurity Framework and expansion of certain key definitions. https://www.ftc.gov/system/files/documents/federal_register_notices/2016/09/frn_standards_for_safeguarding_customer_informtion.pdf
15	FFIEC	4/29/2016	"Appendix E: Mobile Financial Services" issued as an appendix to the "Retail Payments Booklet" of the "FFIEC IT Examination Handbook." https://www.ffiec.gov/press/PDF/FFIEC_CCR_System_Federal_Register_Notice.pdf
16	NCUA	1/11/2016	Letter No.: 16-CU-01, "Supervisory Priorities for 2016", which states "NCUA encourages all credit unions to use the FFIEC tool to manage cybersecurity risks. NCUA also plans to begin incorporating the Cybersecurity Assessment Tool into our examination process in the second half of 2016." https://www.ncua.gov/regulation-supervision/pages/policy-compliance/communications/letters-to-credit-unions/2016/01.aspx
17	CFTC	12/23/2015	*Federal Register* notice of proposed rulemaking, "System Safeguards Testing Requirements for Derivatives Clearing Organizations." http://www.cftc.gov/idc/groups/public/@newsroom/documents/file/federalregister121615b.pdf
18	CFTC	12/23/2015	*Federal Register* notice of proposed rulemaking, "System Safeguards Testing Requirements." http://www.cftc.gov/LawRegulation/FederalRegister/ProposedRules/2015-32143
19	FFIEC	11/10/2015	Revised "IT Examination Handbook: Management Booklet" issued. http://ithandbook.ffiec.gov/it-booklets/management.aspx
20	NFA	10/23/2015	Adoption of interpretive notice, "9070 - NFA COMPLIANCE RULES 2-9, 2-36 AND 2-49: INFORMATION SYSTEMS SECURITY PROGRAMS," effective March 1, 2016 and requiring adoption and enforcement of a written information systems security program. https://www.nfa.futures.org/nfamanual/NFAManual.aspx?RuleID=9070&Section=9

	Issuing Org	Date	Description
21	Maine	10/16 /2015	Bureau of Financial Institutions' Bulletin #80 regarding "Cybersecurity Assessments & the FFIEC Cybersecurity Assessment Tool," requesting completed FFIEC CAT Assessments starting 11/1/2015 http://www.maine.gov/pfr/financialinstitutions/bulletins/bull80.htm
22	Mass.	9/30 /2015	Division of Banking's Bulletin regarding "Cybersecurity Assessments & the FFIEC Cybersecurity Assessment Tool," requiring measurement of "inherent cyber risks" and "cybersecurity maturity" using the FFIEC CAT by 3/31/2016 or to call Division staff to discuss whether use of an alternative framework would be acceptable http://www.mass.gov/ocabr/docs/dob/industry-letter-cyber-09302015.pdf
23	Texas	9/15/ 2015	Department of Banking's "Industry Notice 2015-8" requiring banks to measure "inherent cyber risks" and "cybersecurity maturity" using the FFIEC CAT by 12/31/2015 or to call Department of Banking staff to discuss whether use of an alternative framework would be acceptable http://www.dob.texas.gov/public/uploads/files/news/Industrynotices/in2015-08.pdf
24	SEC	9/15/ 2015	Office of Compliance Inspections and Examinations' "Risk Alert" announcing further cyber exams of broker/dealers and investment advisors with new focus areas https://www.sec.gov/ocie/announcement/ocie-2015-cybersecurity-examination-initiative.pdf
25	FFIEC	6/30 /2015	FFIEC Cybersecurity Assessment Tool https://www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT_June_2015_PDF2.pdf
26	FTC	6/30 /2015	FTC Issues "Start with Security, A Guide for Business: Lessons Learned from FTC Cases," which details cybersecurity expectations to avoid UDAP enforcement action. The FTC regulates through rulemaking as well as through enforcement actions. https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf
27	SEC	4/28 /2015	Division of Investment Mgmt.'s "Guidance Update: Cybersecurity Guidance" for investment advisors https://www.sec.gov/investment/im-guidance-2015-02.pdf

	Issuing Org	Date	Description
28	FFIEC	2/6/2015	Revised "Information Technology Examination Handbook: Business Continuity Planning Booklet" issued, which included the addition of a new appendix, "Appendix J: Strengthening the Resilience of Outsourced Technology Services." http://ithandbook.ffiec.gov/it-booklets/business-continuity-planning/appendix-j-strengthening-the-resilience-of-outsourced-technology-services.aspx

Table B. Regulatory Requirements and Proposals affecting financial institutions' cybersecurity programs generally.

	Issuing Org	Date	Description
29	CFPB	11/22/2016	*Federal Register* notice and "Request for Information Regarding Consumer Access to Financial Records," seeking comment on whether to undertake a rulemaking subject to Dodd-Frank Section 1033 and with what requirements; as described in comments by Director Cordray and in the RFI, a subsequent rule could conflict with "safety and soundness" information security requirements https://www.federalregister.gov/documents/2016/11/22/2016-28086/request-for-information-regarding-consumer-access-to-financial-records
30	FinCEN	10/25/2016	Advisory FIN-2016-A005 issued, entitled "Advisory to Financial Institutions on Cyber-Events and Cyber-Enabled Crime," which directs financial institutions to file Suspicious Activity Reports (SARs) for certain enumerated "cyber-events" https://www.fincen.gov/sites/default/files/advisory/2016-10-25/Cyber%20Threats%20Advisory%20-%20FINAL%20508_2.pdf
31	SWIFT	9/27/2016	Launched "Customer Security Programme" (CSP), which consists of five strategic initiatives: (1) Improve information sharing; (2) Enhance SWIFT-related tools for customers; (3) Enhance guidelines and provide audit frameworks; (4) Support increased transaction pattern detection; and (5) Enhance support by third party providers. SWIFT members will have to comply with the SWIFT compliance framework by January 2018. Non-compliant members will be reported to their

	Issuing Org	Date	Description
			regulators. https://www.swift.com/myswift/customer-security-programme-csp_#topic-tabs-menu
32	CPMI-IOSCO	6/29/2016	Publication of "Guidance on cyber resilience for financial market infrastructures," which provides guidance for financial market infrastructures to enhance cyber resilience. IOSCO member agencies regulate "more than 95% of the world's securities markets in more than 115 jurisdictions." https://www.iosco.org/library/pubdocs/pdf/IOSCOPD535.pdf
33	PCI	4/28/2016	Issuance of the "Payment Card Industry Data Security Standard" (PCI-DSS), version 3.2, which is required for those that accept or process payment cards. https://www.pcisecuritystandards.org/document_library
34	SEC	12/31/2015	*Federal Register* notice of advance notice of proposed rulemaking, concept release, and request for comment on "Transfer Agent Regulations," which poses 21 questions related to potential cybersecurity regulation of transfer agents. https://www.gpo.gov/fdsys/pkg/FR-2015-12-31/pdf/2015-32755.pdf
35	NAIC	12/17/2015	NAIC adoption of "Roadmap for Cybersecurity Consumer Protections," which include requirement that privacy policies include a statement on how consumer data is stored and protected and that insurance companies "take reasonable steps to keep unauthorized persons from seeing, stealing or using your personal information" http://www.naic.org/documents/committees_ex_cybersecurity_tf_related_roadmap_cybersecurity_consumer_protections.pdf
36	SEC	7/8/2015	Request for comment on "Possible Revisions To Audit Committee Disclosures," including whether a publicly traded company's Audit Committee should oversee "treatment" of "cyber risks." https://www.sec.gov/rules/concept/2015/33-9862.pdf
37	FINRA	2/3/2015	Summary of cybersecurity principles and effective practices as reported in its February 3, 2015 Report on Cybersecurity Practice https://www.finra.org/sites/default/files/p602363%20Report%20on%20Cybersecurity%20Practices_0.pdf

Table C. Government-led Cybersecurity Initiatives affecting financial institution cybersecurity programs.

	Issuing Org	Date	Description
38	DHS	1/18/2017	Issuance of an updated "National Cyber Incident Response Plan." NCIRP builds upon PPD-41 and outlines the roles and responsibilities of federal, state, local, tribal, territorial, private sector, and international stakeholders during a cyber incident; identifies the core capabilities required in the event of a cyber incident; and describes the coordination structure the Federal Government will use to coordinate its activities with affected stakeholders. https://www.us-cert.gov/sites/default/files/ncirp/National_Cyber_Incident_Response_Plan.pdf
39	NIST	1/10/2017	Issuance of an updated NIST Cybersecurity Framework – a version 1.1 – that expands the original Framework to include "supply chain risk management," with a solicitation for comment. https://www.nist.gov/sites/default/files/documents/2017/01/30/draft-cybersecurity-framework-v1.1-with-markup.pdf
40	Treasury as part of G-7	10/11/2016	Publication of the Group of 7 (G-7) "Fundamental Elements of Cybersecurity for the Financial Sector," which are described as a concise set of principles on best practices in cybersecurity for public and private entities in the financial sector. While these fundamental elements are described as principles, outside the United States (Treasury is not a regulatory agency), these principles as described and arranged could form the basis for downstream regulations in the other G-7 countries where regulatory oversight and jurisdiction is less complex than in the United States. https://www.treasury.gov/resource-center/international/g7-g20/Documents/G7%20Fundamental%20Elements%20Oct%202016.pdf
41	White House	7/26/2016	Presidential Policy Directive/PPD-41, entitled "United States Cyber Incident Coordination," which sets forth principles governing the Federal Government's response to any cyber incident, whether involving government or private sector entities. https://www.whitehouse.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident

	Issuing Org	Date	Description
42	CPMI-IOSCO	6/29/2016	Publication of "Guidance on cyber resilience for financial market infrastructures," which provides guidance for financial market infrastructures to enhance cyber resilience. IOSCO member agencies regulate "more than 95% of the world's securities markets in more than 115 jurisdictions." https://www.iosco.org/library/pubdocs/pdf/IOSCOPD535.pdf
43	NAIC	12/17/2015	NAIC adoption of "Roadmap for Cybersecurity Consumer Protections," which include requirement that privacy policies include a statement on how consumer data is stored and protected and that insurance companies "take reasonable steps to keep unauthorized persons from seeing, stealing or using your personal information" http://www.naic.org/documents/committees_ex_cybersecurity_tf_related_road map_cybersecurity_consumer_protections.pdf
44	NIST	12/1/2015	The NIST-led initiative to "pursue the development and use of international standards for cybersecurity," as detailed in the "Interagency Report on Strategic U.S. Government Engagement in International Standardization to Achieve U.S. Objectives for Cybersecurity" and required by Cybersecurity Enhancement Act of 2014, Section 502 http://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8074v1.pdf
45	FCC	7/10/2015	Issuance of "TCPA Omnibus Declaratory Ruling and Order," which placed impediments on financial institutions and businesses generally in notifying customer of potential security breaches via mobile/cellular channels. https://apps.fcc.gov/edocs_public/attachmatch/FCC-15-72A1_Rcd.pdf
46	BIS	5/20/2015	Department of Commerce, Bureau of Industry and Security proposed rulemaking to implement Wassenaar Arrangement agreement to limit the import/export (or deemed "export") of intrusion software (e.g., penetration testing software). While the United States is unlikely to implement the rule, those other 40 countries that are part of the Wassenaar arrangement may well do so, as limited revisions were accepted at the December 2016 plenary. https://www.bis.doc.gov/index.php/forms-documents/doc_download/1236-80-fr-28853

Appendix B

Penetration Testing – Non-Exhaustive

As an example of the overlap among financial services cybersecurity related requirements, below is a sample of existing guidelines and expectations regarding a component of vulnerability management: penetration testing. Penetration testing is used to determine how an adversary may infiltrate a firm's information systems. Once known, firms work to close the system gaps exposed by the testing.

I. Voluntary Guidance

1. National Institute of Standards and Technology
   NIST Cybersecurity Framework
   https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf

   NIST Protect Function, Information Protection Processes and Procedures Category, Subcategory: A vulnerability management plan is developed and implemented

2. *Federal Financial Institutions Examination Council (FFIEC)*
   Cybersecurity Assessment Tool
   https://www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT_May_2017.pdf

Cybersecurity Maturity Domain	Assessment Factor	Component	Maturity Level	Mapping Number	Declarative Statement
3: Cybersecurity Controls	3: Corrective Controls	2: Remediation	Evolving	D3.CC.Re.E.2	Formal processes are in place to resolve weaknesses identified during penetration testing.
3: Cybersecurity Controls	3: Corrective Controls	2: Remediation	Advanced	D3.CC.Re.A.1	All medium and high risk issues identified in penetration testing, vulnerability scanning, and other independent testing are escalated to the board or an appropriate board committee for risk acceptance if not resolved in a timely manner.

3: Cybersecurity Controls	2: Detective Controls	1: Threat and Vulnerability Detection	Baseline	D3.DC.Th.B.1	Independent testing (including penetration testing and vulnerability scanning) is conducted according to the risk assessment for external-facing systems and the internal network. (FFIEC Information Security Booklet, page 61)
3: Cybersecurity Controls	2: Detective Controls	1: Threat and Vulnerability Detection	Evolving	D3.DC.Th.E.1	Independent penetration testing of network boundary and critical Web-facing applications is performed routinely to identify security control gaps.
3: Cybersecurity Controls	2: Detective Controls	1: Threat and Vulnerability Detection	Intermediate	D3.DC.Th.Int.1	Audit or risk management resources review the penetration testing scope and results to help determine the need for rotating companies based on the quality of the work.

II. Agency Expressed Requirements and Expectations

1. ***New York Department of Financial Services (NYDFS) (a State-based regulator)***
   23 NYCRR 500 - Cybersecurity Requirements for Financial Services Companies
   http://www.dfs.ny.gov/legal/regulations/adoptions/dfsrf500txt.pdf

   Section 500.05 Penetration Testing and Vulnerability Assessments.
   The cybersecurity program for each Covered Entity shall include monitoring and testing, developed in accordance with the Covered Entity's Risk Assessment, designed to assess the effectiveness of the Covered Entity's cybersecurity program. The monitoring and testing shall include continuous monitoring or periodic Penetration Testing and vulnerability assessments. Absent effective continuous monitoring, or other systems to detect, on an ongoing basis, changes in Information Systems that may create or indicate vulnerabilities, Covered Entities shall conduct:

(a) annual Penetration Testing of the Covered Entity's Information Systems determined each given year based on relevant identified risks in accordance with the Risk Assessment; and

(b) bi-annual vulnerability assessments, including any systematic scans or reviews of Information Systems reasonably designed to identify publicly known cybersecurity vulnerabilities in the Covered Entity's Information Systems based on the Risk Assessment.

2. *National Futures Association (NFA)*
9070 - NFA COMPLIANCE RULES 2-9, 2-36 AND 2-49: INFORMATION SYSTEMS SECURITY PROGRAMS
http://www.nfa.futures.org/nfamanual/NFAManual.aspx?RuleID=9070&Section=9

Review of Information Security Programs.
Members should monitor and regularly review the effectiveness of their ISSPs, including the efficacy of the safeguards deployed, and make adjustments as appropriate. A Member should perform a regular review of its ISSP at least once every twelve months using either in-house staff with appropriate knowledge or by engaging an independent third-party information security specialist. Under appropriate circumstances, a Member's review may include penetration testing of the firm's systems, the scope and timing of which is highly dependent upon the Member's size, business, technology, its electronic interconnectivity with other entities and the potential threats identified in its risk assessment.

3. *Commodity Futures Trading Commission (CFTC)*
System Safeguards Rule - 17 CFR 37.1401
https://www.law.cornell.edu/cfr/text/17/37.1401

(h) A swap execution facility shall conduct regular, periodic, objective testing and review of its automated systems to ensure that they are reliable, secure, and have adequate scalable capacity. It shall also conduct regular, periodic testing and review of its business continuity-disaster recovery capabilities. Such testing and review shall include, without limitation, all of the types of testing set forth in paragraph (h) of this section.

(3)*External penetration testing.* A swap execution facility shall conduct external penetration testing of a scope sufficient to satisfy the requirements set forth in paragraph (k) of this section.
(i) A swap execution facility shall conduct such external penetration testing at a frequency determined by an appropriate risk analysis.

(ii) A swap execution facility shall conduct external penetration testing by engaging independent contractors or by using employees of the swap execution facility who are not responsible for development or operation of the systems or capabilities being tested.

(4) *Internal penetration testing.* A swap execution facility shall conduct internal penetration testing of a scope sufficient to satisfy the requirements set forth in paragraph (k) of this section.

(i) A swap execution facility shall conduct such internal penetration testing at a frequency determined by an appropriate risk analysis.

(ii) A swap execution facility shall conduct internal penetration testing by engaging independent contractors, or by using employees of the swap execution facility who are not responsible for development or operation of the systems or capabilities being tested.

(k) *Scope of testing and assessment.* The scope for all system safeguards testing and assessment required by this part shall be broad enough to include the testing of automated systems and controls that the swap execution facility's required program of risk analysis and oversight and its current cybersecurity threat analysis indicate is necessary to identify risks and vulnerabilities that could enable an intruder or unauthorized user or insider to:

(1) Interfere with the swap execution facility's operations or with fulfillment of its statutory and regulatory responsibilities;

(2) Impair or degrade the reliability, security, or adequate scalable capacity of the swap execution facility's automated systems;

(3) Add to, delete, modify, exfiltrate, or compromise the integrity of any data related to the swap execution facility's regulated activities; or

(4) Undertake any other unauthorized action affecting the swap execution facility's regulated activities or the hardware or software used in connection with those activities.

4. *Securities and Exchange Commission Office of Compliance Inspection and Examination*

OCIE's 2015 Cybersecurity Examination Initiative
https://www.sec.gov/ocie/announcement/ocie-2015-cybersecurity-examination-initiative.pdf

APPENDIX

This document provides a sample list of information that the U.S. Securities and Exchange Commission's Office of Compliance Inspections and Examinations ("OCIE") may review in conducting examinations of registered entities regarding cybersecurity matters. Some of the questions track information outlined in the "Framework for Improving Critical Infrastructure

Cybersecurity," 2 released on February 12, 2014 by the National Institute of Standards and Technology. OCIE has published this document as a resource for registered entities. This document should not be considered all-inclusive of the information that OCIE may review or the validation and testing we may perform of firm policies and procedures. Accordingly, OCIE will alter its requests for information it reviews, as well as whether it asks for production of information in advance of an examination or reviews certain information on site, as it considers the specific circumstances presented by each firm's business model, systems, and information technology environment.

Governance and Risk Assessment

• Information regarding the firm's policies related to penetration testing, whether conducted by or on behalf of the firm, and any related findings and responsive remediation efforts taken.

5. *Federal Financial Institutions Examination Council (FFIEC)*
FFIEC IT Examination Handbook, Information Security Booklet
https://ithandbook.ffiec.gov/it-booklets/information-security/iv-information-security-program-effectiveness/iva-assurance-and-testing/iva2-types-of-tests-and-evaluations/iva2(b)-penetration-tests.aspx

IV.A.2(b) Penetration Tests
A penetration test subjects a system to real-world attacks selected and conducted by the testers. A penetration test targets systems and users to identify weaknesses in business processes and technical controls. The test mimics a threat source's search for and exploitation of vulnerabilities to demonstrate a potential for loss. Some tests focus on only a subset of the institution's systems and may not accurately simulate a determined threat actor. There are many types of penetration tests (e.g., network, client-side, web application, and social engineering), and management should determine the level and types of tests employed to ensure effective and comprehensive coverage.

The frequency and scope of a penetration test should be a function of the level of assurance needed by the institution and determined by the risk assessment process. The test can be performed internally by independent groups, internally by the organizational unit, or by an independent third party. Management should determine the level of independence required of the test.

6. *Federal Financial Institutions Examination Council (FFIEC)*
FFIEC IT Examination Handbook, E-Banking Booklet

http://ithandbook.ffiec.gov/it-booklets/e-banking/risk-management-of-e-banking-activities/information-security-program/information-security-controls.aspx

Information Security Controls
Security threats can affect a financial institution through numerous vulnerabilities. No single control or security device can adequately protect a system connected to a public network. Effective information security comes only from establishing layers of various control, monitoring, and testing methods. While the details of any control and the effectiveness of risk mitigation depend on many factors, in general, each financial institution with external connectivity should ensure the following controls exist internally or at their TSP [Third Party Service Provider].

- *Independent testing.* Financial institutions should have a testing plan that identifies control objectives; schedules tests of the controls used to meet those objectives; ensures prompt corrective action where deficiencies are identified; and provides independent assurance for compliance with security policies. Security tests are necessary to identify control deficiencies. An effective testing plan identifies the key controls, then tests those controls at a frequency based on the risk that the control is not functioning. Security testing should include independent tests conducted by personnel without direct responsibility for security administration. Adverse test results indicate a control is not functioning and cannot be relied upon. Follow-up can include correction of the specific control, as well as a search for, and correction of, a root cause. Types of tests include audits, security assessments, vulnerability scans, and penetration tests.

Written Testimony of

Dean C. Garfield
President & CEO
Information Technology Industry Council (ITI)

Before the

Committee on Homeland Security and Governmental Affairs
U.S. Senate

Cybersecurity Regulation Harmonization

June 21, 2017

Written Testimony of:
Dean Garfield
President & CEO, Information Technology Industry Council (ITI)

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

Cybersecurity Regulation Harmonization

June 21, 2017

Chairman Johnson, Ranking Member McCaskill, and members of the committee, thank you for the opportunity to testify today. I am Dean Garfield, President and CEO of the Information Technology Industry Council (ITI), and I am pleased to testify before the Homeland Security and Governmental Affairs Committee on the important topic of cybersecurity regulation harmonization. We welcome your interest and engagement on this subject.

ITI[1] represents 60[2] of the world's leading information and communications technology (ICT) companies. We are the global voice of the tech sector and the premier advocate and thought leader in the United States and around the world for the ICT industry. ITI's member companies are comprised of leading technology and innovation companies from all corners of the ICT sector, including hardware, software, digital services, semiconductor, network equipment, internet companies, and companies using technology to fundamentally evolve their businesses. Cybersecurity and cybersecurity technology are critical to ITI members. Facilitating the protection of our customers (including governments, businesses, and consumers), securing and protecting the privacy of our customers' and individuals' data, and making our intellectual property, technology, and innovation available to our customers to enable them to improve their businesses are core drivers for our companies. Consequently, ITI has been a leading voice in advocating for effective approaches to cybersecurity, both domestically and globally.

Cybersecurity is rightly a priority for governments and our industry, and we share a common goal of improving cybersecurity. Further, our members are global companies, doing business around the world. As both producers and users of cybersecurity products and services, our members have extensive experience working with governments across the globe on cybersecurity policy. This is important for the committee to keep in mind because when it comes to cybersecurity, our connectedness is through an internet that is truly open, global and borderless. We acutely

[1] **About ITI.** ITI is the global voice of the tech sector. We advocate for public policies that advance innovation, open markets, and enable the transformational economic, societal, and commercial opportunities that our companies are creating. Our members represent the entire spectrum of technology: from internet companies, to hardware and networking equipment manufacturers, to software developers. ITI's diverse membership and expert staff provide a broad perspective and intelligent insight in confronting the implications and opportunities of policy activities around the world. Visit http://www.itic.org/ to learn more. Follow us on Twitter for the latest ITI news @ITI_TechTweets.
[2] See membership list at http://www.itic.org/about/member-companies.

understand the impact of governments' policies on security innovation and on our customers, and thus the need for U.S. policies to be compatible with – and lead – global norms.

I will focus my testimony on four areas: (1) using public-private partnerships and leveraging existing cybersecurity policies to achieve greater regulatory streamlining; (2) harmonizing federal cybersecurity policies around risk management and international standards, including for the Internet of Things (IoT); (3) prioritizing implementation of existing federal policies on regulatory streamlining through federal agency coordination; and (4) reforming government acquisition procedures to allow the use of agile federal procurement processes to acquire cybersecurity products and services.

Assess & leverage existing cybersecurity policies and build upon public-private partnerships to achieve greater regulatory streamlining at the international, federal, and state levels.

There has been a flurry of cybersecurity policymaking activity in the U.S. over the past few years. The Obama Administration issued several executive actions dealing with cybersecurity, including Executive Order (EO) 13718 that launched the Commission on Enhancing National Cybersecurity[3] and EO 13636[4] that called for the National Institute of Standards and Technology (NIST) to develop the *Framework for Improving Critical Infrastructure Cybersecurity* (the *Framework*). NIST is now leading an effort to update the *Framework*, soliciting comments from the private sector earlier this year. Last month, the Trump Administration issued EO 13800 on *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*,[5] and Congress has passed prominent cybersecurity laws, particularly cybersecurity threat information sharing legislation.[6]

These new initiatives complement well-established public-private partnership activities, and together, the public and private sectors have begun implementing many of these policy instruments. Congress should consider the public and private sectors' ongoing collaboration and efforts to implement pre-existing regulations before further legislating on cybersecurity so that Members may arrive at a holistic, federal cybersecurity strategy approach.

It is well-known that the private sector owns/operates approximately 85 percent of critical infrastructure in the United States and elsewhere, and that the ICT industry creates nearly the entire cyberspace infrastructure. What is not known are the many ways the ICT industry works cooperatively with federal, state, and local governments to improve cybersecurity and ensure that approaches to cybersecurity are adaptive, flexible, and effective. For well over a decade, ICT companies have provided leadership, subject-matter experts, technical and monetary resources, innovation, and stewardship to help enable all stakeholders to better manage and mitigate

[3] Executive Order 13718, *Commission on Enhancing National Cybersecurity,* February 9, 2016, *available at* https://obamawhitehouse.archives.gov/the-press-office/2016/02/09/executive-order-commission-enhancing-national-cybersecurity.
[4] Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*, February 12, 2013, *available at* https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.
[5] Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure,* May 11, 2017, *available at* https://www.whitehouse.gov/the-press-office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal.
[6] *Cybersecurity Act of 2015*, passed as Division N of the FY 2016 Omnibus Appropriations Act, P.L. 114-113, December 18, 2015.

cybersecurity risk. Cyberspace would be much less secure in the absence of these partnerships and initiatives. For example, the Information Technology Information Sharing and Analysis Center (IT-ISAC) has been invaluable to help address sector specific and cross-sectoral threats and vulnerabilities. It helped monitor and collaborate with its members on large-scale threats such as Conficker and the DNS Cache Poisoning Vulnerability. The IT-ISAC provided a forum for members to engage in collaborative analysis on those significant issues and share alerts and potential solutions with members, other ISACs, and the public.

Policymakers, as they seek to advance critical infrastructure (CI) protection, stand to gain by leveraging existing work, as appropriate, prior to establishing new policies- particularly by continuing to harness the public-private partnerships that have been in existence for decades. For example, many companies previously shared limited cyber threat information through ISACs and Sector Coordinating Councils (SCCs), but Congress improved upon and bolstered those partnerships through the 2015 cybersecurity threat information sharing legislation by eliminating barriers that precluded the sharing of specific, actionable threat information between public and private sectors.

In addition, Congress should ensure NIST continues to serve as the federal coordinator for cybersecurity best practices and guidelines. One of the best examples of effective public-private collaboration on cybersecurity is NIST's continuing work on the *Framework*, as well as its other efforts such as the *IoT-Enabled Smart City Framework*.[7]

To streamline federal, state, local, as well as international, cybersecurity regulatory efforts, we need a common language or cybersecurity risk management taxonomy that can be effectively used by policymakers globally and at all levels of U.S. government. It is counterproductive to create siloed, agency-specific or country-specific approaches to cybersecurity, and the federal government should promote polices that help break down the artificial barriers that hinder cybersecurity efforts. Unfortunately, without a common lexicon for cybersecurity and risk management efforts, federal, state, local, and international governments tend to create separate approaches to cybersecurity that ultimately lead to greater insecurity for governments, consumers, and private industry.

ITI strongly recommends the *Framework* as a policymaking tool. Promoting the *Framework* as a common language for policymakers can help align U.S. federal agency cybersecurity and risk management efforts. The *Framework* leverages public-private partnerships, is grounded in sound risk management principles, and helps foster innovation due to its flexibility and basis in global standards. The *Framework* has consistently been lauded for providing a common language to better help organizations comprehend, communicate, and manage cybersecurity risks. While it is important to stress that we are still in the early phase of a multi-year effort and we do not see this as a silver bullet solution, we believe the *Framework* has already helped and will continue to help improve cybersecurity, and its approach is worth prioritizing and replicating domestically and globally for both organizations and governments.

[7] National Institute of Standards & Technology, IoT-Enabled Smart City Framework, *available at* https://pages.nist.gov/smartcitiesarchitecture/.

The potential of the *Framework* to provide a common taxonomy for policymakers domestically and globally has yet to be fully realized. We urge Congress to support and oversee the implementation of the Trump Administration's cybersecurity EO that requires federal agencies to use the *Framework* to manage each agency's cybersecurity risk.

Without a guideline like the *Framework* around which to orient their efforts individual federal agencies, state governments, and other countries may fill the void with disparate and conflicting guidelines and regulations. For example, in April 2016, the National Highway Traffic Safety Administration (NHTSA) at the Department of Transportation released a request for public comment on an Enforcement Guidance Bulletin on Safety-Related Defects and Emerging Automotive Technologies.[8] The NHTSA Bulletin endeavored to create a separate cybersecurity scheme for automobiles, but failed to create a prioritization of cybersecurity risks in a way that aligns with cybersecurity risk management best practices. The ongoing convergence of the automotive and technology sectors alone does not call for a separate regulatory structure to address automotive cybersecurity. NHTSA should, instead, leverage existing work like that being done by NIST, under the *Framework* and *Cyber Physical Systems Working Group*, or by the Department of Homeland Security (DHS) and international standards bodies.

States are beginning to legislate solutions and issue regulations as well, which is adding more complexity. Nevada Senate Bill 395 was recently introduced and opposed by ITI because of its intent to define CI in the state and develop a subsequent state plan with requirements that are not consistent with sound cybersecurity policy, or existing federal policy. This legislation would create a conflicting and competing definition of CI with those at the federal level designated by DHS. DHS is already in charge of designating CI and working with the private sector owners and operators to mitigate CI risk through federal law and policy. Additionally, the need to preserve and promote innovation and innovative technologies would be hindered by over-designating CI, which would thinly stretch already limited resources. Lastly, the bill would effectively provide public disclosure of vulnerabilities within CI systems, which is contrary to commonly recognized cybersecurity best practices. States should not be in the business of designating CI outside of the federal government's definition. It is incumbent upon industry and the federal government to educate states on the work currently being done at the federal level to mitigate security vulnerabilities at all levels of government.

Congress should look for ideal *outcomes*, not ideal *regulations*, which may not always be the same. This way of thinking opens the door to creative approaches that seek to harmonize cybersecurity regulations around a common set of principles that are flexible and adaptable to changing technologies and constant innovation.

[8] Department of Transportation, National Highway Traffic Safety Administration, Request for Public Comments, Docket No. NHTSA-2016-0040, April 1, 2016.

The federal government should harmonize cybersecurity policies around risk management and international standards based in the *Framework for Improving Critical Infrastructure Cybersecurity* to avoid duplicative resources and requirements on federal agencies, state governments, and the private sector.

The technology sector partnered with NIST for nearly three years to develop the *Framework* pursuant to EO 13636, which called for the government to partner with owners and operators of CI to improve cybersecurity through the development and implementation of a framework of voluntary, consensus, risk-based standards. The *Framework* provides an overarching structure, grounded in proven international standards and consensus best practices, to address organizational security across all CI sectors, while providing adaptability and flexibility to meet unique sector needs and address new threats.

As noted earlier, the *Framework* includes a common language for organizations to manage cybersecurity risks, and that language can be the basis for action by policymakers globally and domestically. Among other benefits, this approach can help prevent duplicative regulatory efforts.

One area where the *Framework* can be used in such a fashion is to drive cybersecurity alignment across federal agencies. As discussed further below, it is extremely important to push for alignment of federal agency cybersecurity practices, including orientation of federal agency efforts to the *Framework*, which will in turn facilitate mapping of agencies' cybersecurity risks to their missions' government-wide. In fact, the recent cybersecurity EO clearly called for this risk management tactic.[9] The order requires each agency head to use the *Framework*, or any successor document, to manage the agency's cybersecurity risk and submit a risk management report to DHS and the Office of Management and Budget (OMB).

ITI previously recommended the executive branch develop guidance for federal agencies to apply the *Framework* to help them use business drivers to guide cybersecurity activities and consider cybersecurity risk as part of their risk management processes. To support agency heads in responding to the Trump cybersecurity EO, NIST released a request for comment on its proposed *Framework* implementation guidance.[10] NIST is effectively developing government-wide guidance in the same manner that many sectors currently do for their own use, and such a streamlined effort will reduce regulatory redundancy.

Beyond using the *Framework* in its exact form, private industry also adapts the principles expressed in the *Framework* to develop their own guidance, precluding the need for the federal government to create more granular cybersecurity regulations. For example, the financial sector compiled the Federal Financial Institutions Examination Council's Information Security Booklet, which was updated in September 2016 to provide a tool for financial institutions to implement a cybersecurity

[9] Executive Order 13800, *supra* note 5.
[10] National Institute of Standards & Technology, *The Cybersecurity Framework: Implementation Guidance for Federal Agencies*, Interagency Report 8170, *available at* http://csrc.nist.gov/publications/drafts/nistir-8170/nistir8170-draft.pdf.

program consistent with the *Framework*.[11] In the communications sector, the Communications Security, Reliability and Interoperability Council (CSRIC) provides recommendations to the Federal Communications Commission on optimal security and reliability of communications systems.[12] The CSRIC working group IV recently developed detailed voluntary risk management guidance mapped to the *Framework* for the communications sector.[13] NIST further developed a version of the *Framework* for small businesses to use to assist in protecting their data and intellectual property.[14]

International Standards. The global ICT industry is heavily invested in developing standards for security management, and the United States should continue to lead the way in promoting adoption of industry-led, voluntary, globally recognized cybersecurity standards and best practices that avoid country-specific requirements. Many international governments have already been inspired by efforts like the *Framework* to develop their cybersecurity guidelines. Furthermore, the technology sector has supported organizations across the globe who use the *Framework*, and it is gaining traction internationally (e.g., Italy developed its own version of the *Framework* using a similar public-private partnership process; Israel has incorporated the Framework into its own cybersecurity guidance; and the British Standards Institute is developing a standard that assesses organizations' application of the *Framework).*

A central element of ITI's global advocacy efforts involve helping governments understand the critical importance of cross-border data flows, not only to the ICT sector, but also to the global economy. Global cybersecurity relies on the ability for data to flow across borders. Threat indicators, research and development, product design, and other information, when shared globally, aids in the development of robust mechanisms to protect against threats. It also ensures companies can perform operations, manage production schedules and communicate with subsidiaries and employees across the globe in a secure manner, enabling them to invest in and create technologies which are secure and, in turn, help protect the entire ecosystem upon which all stakeholders rely. The free flow of data across borders is necessary to enable a seamless and secure Internet experience for hundreds of millions of citizens around the globe.

Some international developments threaten the ability for these essential data flows to continue. The proposed Wassenaar Rule imposing restrictions on the sale of cybersecurity technology such as intrusion detection software is an extension of a troubling global trend of erecting barriers to the free movement of global data. Another example of this trend is the 2015 invalidation of the U.S.-EU Safe Harbor Framework by the Court of Justice of the European Union.[15] While preventing misuse of certain types of technology and protecting the privacy of individuals are both legitimate goals, if

[11] FFIEC Information Technology Examination Handbook, *Information Security,* September 2016, *available at* http://ithandbook.ffiec.gov/media/216407/informationsecurity2016booklet.pdf.
[12] Communications Security, Reliability and Interoperability Council IV, FCC, *available at* https://www.fcc.gov/about-fcc/advisory-committees/communications-security-reliability-and-interoperability-0.
[13] Communications Security, Reliability and Interoperability Council IV, *Cybersecurity Risk Management and Best Practices, Working Group 4: Final Report,* March 2015, *available at* https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG4_Final_Report_031815.pdf.
[14] National Institute of Standards & Technology, *Small Business Information Security: The Fundamentals,* November 2016, NISTIR 7621, *available at* http://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf.
[15] *Maximillian Schrems v Data Protection Commissioner,* https://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf.

not handled in a targeted manner, broad restrictions can undermine the security of global cybersecurity infrastructure.

Global Standards and the Internet of Things (IoT). Many of the existing foundational elements that drove the development, evolution, and investment in the modern internet ecosystem are necessary to realize the potential of the IoT. Adoption of global, consensus-based standards, as discussed above, is critical for providing the interoperability necessary for the IoT to thrive. As the IoT technology landscape comes into greater focus, various global, industry-led standards-setting organizations (SSOs) have formed technical and study groups to ascertain to what extent additional standards development is necessary, including for cybersecurity. These bodies are typically international in scope, drawing experts and participation from across the globe and various industry sectors that will be impacted by and benefit from the IoT. It is important for the Department of Commerce and, more generally, all governments to share their needs and requests with these SSOs and, when appropriate, actively participate in these processes.

Federal agencies should similarly support IoT standardization and encourage other governments to follow a similar approach which opts for global standards and approaches rather than undertaking standardization activities that may be duplicative of, or even conflict with, global, industry-led IoT standards. In fact, government, industry, and other stakeholders, through collaborative efforts, have stepped up to address the issue of cybersecurity pertaining to connected devices.

Disparate cybersecurity regulations can cause confusion among federal, state, local, and international governments as well as private industry, and multiple legislative efforts to tackle cybersecurity in a disconnected fashion on a sector-by-sector basis can not only cause confusion, but also create a false sense of security for both companies and consumers. Thus, harmonizing cybersecurity policies around a risk management approach informed by international standards can help to optimally allocate resources without imposing duplicative compliance burdens on federal agencies, state governments, and the private sector, while providing better security.

The fast pace of technological innovation, such as the Internet of Things, accelerates the need for harmonization and adaptability of cybersecurity regulations.

The IoT is a collection of external devices and sensors that generate data, which, through an internet connection, can be analyzed to provide actionable information. The range and application of these devices is virtually limitless, but we generally view them in three distinct categories: 1) commercial or industrial; 2) personal or mobile; and 3) household.

Commercial and industrial IoT devices are by far the largest category, and where many of our companies see the biggest opportunity to enhance productivity and efficiencies, improve real-time decision making, and solve critical societal problems. Estimates predict the value of this category will eclipse $7 trillion by 2030.[16] Examples of commercial and industrial IoT include predictive

[16] Accenture, *Winning with the Industrial Internet of Things*, released 2015.

equipment maintenance, facility heating, cooling and lighting management, transportation fleet management and improvement, as well as other large scale uses.

Personal or mobile IoT technologies are likely familiar to most, given the ubiquity of wearable watches, health monitors, and similar devices connecting to the Internet via wireless broadband connections or mobile phones. But the more significant gross domestic product impact will be derived from autonomous vehicles and cars connected to the Internet via cellular or other wireless technologies.

Finally, household IoT applications range from smart appliances to smart thermostats, and intelligent home monitoring and security systems. These products connect through residential broadband or home Wi-Fi networks to provide energy savings and home automation and security benefits.

While IoT is not new – since the internet was invented, various devices have been connected and networked in attempts to improve convenience, functionality, and other purposes – these now hallmarks of IoT are increasingly achieving much greater success and occurring on a more pervasive scale. Indeed, the rapid growth of networked devices and internet applications due to the availability of components, internet service, and the technology that make internet connection possible – such as Smart Grid, Smart Cities, and Connected Autos – have us rapidly evolving toward an internet of everything. Given this, the U.S. government and other government bodies must look at the underlying technologies and assess where current authority, oversight, and regulation already exist. They should also seek to identify areas where government has taken successful approaches, and replicate that activity in other areas. There are a number of relevant policy areas where authorities already exist, where government is facilitating IoT development, and where industry is working with government to address new or evolving issues stemming from the IoT, including cybersecurity.

Where such regulations, guidance, and oversight do not exist or are ineffective in covering emerging technologies, this should reinforce the importance of creating adaptable, technology-neutral approaches that can outlast new developments in technology.

Cybersecurity and IoT. Significant activity continues to take place across both government agencies and the private sector to strengthen our cybersecurity, including for IoT. The interests of government and industry are aligned as both aim to minimize vulnerabilities and create networks, products, and devices that are as secure as possible. Consequently, much of the activity designed to enhance cybersecurity takes place in consultation and close collaboration with the private sector, and we strongly encourage that public-private partnership approach to continue.

ITI's member companies are at the forefront of providing security solutions from devices at the expanding network edge to the cloud, and across the network and IoT. With billions of additional devices coming online, ITI's companies ensure that security is embedded in IoT platforms at the outset of the manufacturing and design process for each new device. Security by design must be

built into both hardware and software at the outset to ensure there are redundancies, to prevent intrusions, and to create secure and trusted IoT systems. Advances in hardware technology allow for security to be physically built into a system. For example, semiconductor manufacturers can design chips with built-in safeguards. Encryption, for instance, can be baked in at the chip level. Manufacturers can also prevent chips from being rewritten by designing fuses into chips. If a hacker attempts to access or rewrite data, the fuse pops and prevents the data from being rewritten. Similarly, on the network side, devices communicating with the network will require a reliable level of service and connectivity, as well as high security, to prevent unwanted intervention. New internet protocol architectures are more adaptable and use advanced technologies to pervasively distribute security, treat individual users and devices with an appropriate level of performance and privacy based on their needs, and automate manual processes to improve scale and availability. Application programming interfaces (APIs) facilitate data interactions between edge devices, code modules, applications, and backend IT systems. Organizations can leverage API management software to address security as an architectural challenge in the development of IoT applications.

Federal government stakeholders have a critical role to play in fostering security across the IoT; excellent groundwork has already been laid in this area and should be leveraged going forward. The result of industry partnership with the NIST on the *Framework* is a set of voluntary guidelines, best practices, and standards to help critical infrastructure, businesses, and other private and public actors to better manage cybersecurity risks, including for the IoT.

Taking a similar public-private partnership approach, NIST recently released a *Framework for Cyber-Physical Systems* (the *CPS Framework*),[17] also developed in partnership with industry, academic, and government experts. One of the key working groups in the cyber-physical systems project is focused on cybersecurity and privacy.[18] The *CPS Framework* provides guidance to manufacturers, including detailed technical guidance for building secure products for IoT, Smart Cities, Industrial Internet and other applications. On the flip side, viewing cybersecurity uniquely for each application, whether it be a home computer or an automobile, and mandating prescriptive security checklists is inflexible and will leave industry less able to quickly and efficiently respond to new threats, potentially stifling innovation.

Perhaps of greater concern is the potentially counterproductive precedent of creating siloed approaches to cybersecurity across different ICT applications, as part of the IoT and beyond. As more "things" are connected to the internet to make our lives richer and more efficient, we do not need to reinvent the wheel when it comes to security, as each of these applications or use cases gains prominence. At different stages of the recent past, policymakers have considered whether new regulatory regimes were needed to better secure CI, the electric grid, cloud computing, or health IT, and in each instance, after close examination, the benefits of approaches grounded in voluntary, consensus-based international standards that both promote innovation and preserve the

[17] National Institute of Standards & Technology, *Cyber-Physical Systems Framework*, May 2016, *available at* https://s3.amazonaws.com/nist-sgcps/cpspwg/files/pwgglobal/CPS_PWG_Framework_for_Cyber_Physical_Systems_Release_1_0Final.pdf.
[18] https://www.nist.gov/el/cyber-physical-systems/cps-pwg-security

promise of interoperability have carried the day. The alternative – a world in which we endeavor to separately regulate each new ICT application or IoT vertical – is not realistically scalable, and simply unsustainable in an IoT world.

Thus, the technology industry constantly works to stay ahead of threats to the IoT, not only through its own solutions, but also in partnership with the federal government. The ICT industry leads and contributes to a range of significant public-private partnerships, including information sharing, analysis, and emergency response with governments and industry peers. In addition to the NIST CPS Working Group and NIST *Framework*, some examples include: 1) NIST Cybersecurity for IoT program; 2) National Telecommunications & Information Administration Multi-stakeholder process on IoT patching; 3) DHS IoT security principles; and 4) Federal Trade Commission (FTC) 2015 Internet of Things Staff Report, among others.

Policymakers and regulators should reinforce this collaborative environment to encourage innovative, public-private cooperation on these issues, rather than top-down regulations that may duplicate ongoing work. Through oversight, policymakers should also better coordinate the many IoT security-related policy efforts currently in progress across the administration.

For example, we were encouraged to see DHS take the lead on IoT security through its publication of non-binding principles in its IoT security guidelines[19] released in November 2016. Industry was given the opportunity to provide input prior to its publication; however, at the time of publication, DHS may not have been fully aware of other federal government efforts around IoT security. For example, following a request from the Information Technology Sector Coordinating Council (IT-SCC) during the DHS IT Sector Leadership Meeting in April 2017, after reviewing the public websites of over 70 Federal Departments and Agencies, the DHS Office of Cybersecurity and Communications (CS&C) staff compiled a list of existing federal IoT projects and highlighted overlap between those projects and CS&C's proposed initiatives in federal IoT procurement guidance, end-user critical infrastructure sector guidance, and smart city guidance. They discovered 30 IoT-related security initiatives across the federal government—from one-time white papers and policy proposals to working groups and fully developed programs and guidance.

Multiple agencies already have workstreams on IoT issues surrounding smart cities, smart grid security, home device security, medical devices, and automobiles, among others. While all may have value in specific industries, and perhaps more broadly to the general IoT security discussion, lack of coordination can minimize the effectiveness of both the implementation of the initiatives and any public-private collaboration that may have contributed to them.

Following its publication of current federal IoT efforts the IT-SCC and DHS are working collaboratively on a specific workstream—providing actionable IoT buying and deployment guidance for public and private stakeholder use. As Congress considers what action, if any, it

[19] Department of Homeland Security, *Strategic Principles for Securing the Internet of Things (IoT)*, November 15, 2016, *available at* https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL....pdf.

should take regarding IoT security, before moving forward, we recommend members first use these results and conduct a similar evaluation of current laws and existing proposed legislation on IoT security that may overlap or create duplicative requirements on governments, companies, and consumers. Further, if Congress decides to act, it should seek flexible, risk management solutions that are adaptable in multiple industries rather than mandating prescriptive checklists that slow, or even halt, security innovation.

In lieu of IoT security legislation, we recommend Congress act to fill gaps that have already been identified:

- First, Congress should pass the Developing Innovation and Growing the Internet of Things Act (DIGIT Act),[20] which brings together federal departments with a role in IoT to coordinate activity, including on cybersecurity, and would be a significant down payment on the problem of lack of coordination in development of IoT security best practices.

- Second, the Small Business Administration (SBA) has programs to educate small and medium-sized business owners (SMBs) about cybersecurity, provide resources to assess information security resilience, and create customized cybersecurity plans. Congress can reinforce these and other programs by providing more resources to these programs and for agencies to educate SMBs on risk management.

- Third, Congress could direct the SBA to work with NIST and Small Business Development Centers to address IoT security by creating, maintaining, updating, and disseminating cybersecurity resources specific to SMBs development, adoption, and use of IoT products.

- Finally, Congress could also direct the FTC to work with NIST to create, maintain, and update cybersecurity resources for consumer development, adoption, and use of IoT products so that consumers can look critically at IoT devices.

The IoT is in its very nascent stages and presents us with limitless possibilities if we have the vision and environment to achieve them. We look forward to working with Congress to advance IoT security, and we ask that you evaluate existing policy tools and use caution before taking actions that may inadvertently or unnecessarily impede IoT innovation and disadvantage U.S. competitiveness.

The federal government should prioritize implementing Section 10 of Executive Order 13636, which clearly contemplated regulatory streamlining, by designating one agency or combination of agencies to assess and coordinate federal agency cybersecurity practices.

[20] S. 88/H.R. 686, *Developing Innovation and Growing the Internet of Things Act*, 115th Cong. (2017).

Executive Order 13636, *Improving Critical Infrastructure Cybersecurity,*[21] called for a voluntary, risk-based cybersecurity framework, and that is exactly what NIST produced, with significant input from industry. While we support and value the inherent "voluntariness" of the *Framework* and do not suggest NIST and Congress lose sight of that, it is clear -- given the recent Trump Administration cybersecurity executive order and increasing use of the *Framework* approach internationally and at the state and local level -- that policymakers and regulators are increasingly looking to the *Framework* for inspiration. Indeed, this was anticipated in Section 10 of EO 13636, which contemplated opportunities the *Framework* created for regulatory streamlining. Indeed, then White House cyber coordinator, Michael Daniel, indicated the Obama Administration was "beginning a process to identify federal regulations that are excessively burdensome, conflicting, or ineffective."[22]

We believe more can and should be done to reinforce the *Framework* as voluntary while also embracing its use by regulators to streamline and eliminate superfluous cybersecurity regulations. Reconciling the multiple and often divergent cybersecurity policy efforts across the federal government is becoming an increasingly urgent need. Having achieved widespread cybersecurity awareness, seemingly every federal agency is examining a separate piece of the cybersecurity puzzle through its own lens, often developing their own guidance and/or prescriptive requirements, and leading to an overall cybersecurity approach more reminiscent of a patchwork than a coordinated strategy. Instead, to fully realize the benefits offered by the IoT and innovations such as Big Data Analytics, the federal government should promote policies that help break down barriers to connecting devices and correlating data.

How can we accomplish this? The key is that the *Framework* should not serve as the impetus or rationale for extra layers of regulation—that's not regulatory streamlining, it is regulatory redundancy, and multiple layers of redundant regulations will not create better cybersecurity for anyone. Rather, it can be held up as a voluntary risk-management based tool around which policymakers and regulators should orient their efforts to improve cybersecurity. While not the perfect or only solution, doing so will help reduce regulatory redundancy.

EO 13636 required agencies to "1) assess the sufficiency of existing regulatory authority to establish requirements based on the *Cybersecurity Framework* to address current and projected cyber risks; and 2) identify proposed changes in order to address insufficiencies identified."[23] Several agencies released reports,[24] and concluded "existing regulatory requirements, when

---

[21] Executive Order 13636, *supra* note 4.

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

[23] Michael Daniel, *Assessing Cybersecurity Regulations,* May 22, 2014, *available at* https://obamawhitehouse.archives.gov/blog/2014/05/22/assessing-cybersecurity-regulations.

[24] Department of Homeland Security, *Executive Order 13636—Improving Critical Infrastructure Cybersecurity*, Reports, 2014 *available at* https://www.dhs.gov/publication/eo-13636-improving-ci-cybersecurity; Department of Health & Human Services, *Executive Order 13636, Section 10(b)—HHS Assessment,* May 12, 2014, *available at* https://www.phe.gov/Preparedness/planning/cip/Pages/eo13636.aspx; Environmental Protection Agency, *Drinking Water and Wastewater Resilience*, 2014, *available at* https://www.epa.gov/waterresilience.

complemented with strong voluntary partnerships, are capable of mitigating cyber risks to our critical systems and information."[25]

Thus, we recommend this administration and Congress complete what the prior administration did not—consult CI partners within and outside the federal government to identify those ineffective, duplicative, or burdensome regulations and take action to eliminate them. President Trump has taken initial steps to examine and streamline regulations through two executive orders that would 1) require elimination of two regulations for every new regulation and prudent cost management of planned regulations;[26] and 2) create regulatory reform officers within each agency to implement regulatory reform initiatives and policies, including reducing the number of regulations and controlling regulatory costs.[27]

Efforts to improve IoT cybersecurity, and overall federal cybersecurity, should leverage public-private partnerships and build upon existing initiatives and resource commitments. Working together, federal government partners, including DHS, NIST, and the White House, can work with industry to help spearhead a regulatory streamlining effort to rationalize not only IoT security initiatives, but also overall federal government cybersecurity regulatory efforts.

Reform government acquisition procedures to allow for deployment of agile federal procurement processes to acquire cybersecurity products and services, and align corresponding guidance among agencies for consistent application across the government.

Improving and strengthening our nation's cybersecurity posture is rightly a top priority for our government and changing how the federal government integrates cybersecurity into its own acquisition process for procuring of goods and services will help improve federal government cybersecurity resiliency. Over the last few years, the federal government issued several cybersecurity orders[28] and regulatory measures to enhance cybersecurity resiliency within the federal government and CI controlled by the private sector. Federal agencies recognize the need for greater control over federal network security, and have thus created their own unique cybersecurity acquisition systems and regulations.

With a lack of coordination by OMB, agencies will continue to perpetuate a patchwork of requirements for contractors, and each agency will develop their own cybersecurity requirements for acquisition purposes. Federal requirements on contractors to sell cyber products and services and to protect federal data and information are growing, and industry is concerned over the increasingly complicated regulatory landscape they face to ensure information assurance while

---

[25] *Id.* at Department of Homeland Security, *Executive Order 13636—Improving Critical Infrastructure Cybersecurity,* Reports, 2014.

[26] Executive Order 13771, *Reducing Regulation and Controlling Regulatory Costs,* January 30, 2017, *available at* https://www.whitehouse.gov/the-press-office/2017/01/30/presidential-executive-order-reducing-regulation-and-controlling.

[27] Executive Order 13777, *Enforcing the Regulatory Reform Agenda,* February 24, 2017, *available at* https://www.whitehouse.gov/the-press-office/2017/02/24/presidential-executive-order-enforcing-regulatory-reform-agenda.

[28] EO 13636, *supra* note 4; and Executive Order 13691, *Promoting Private Sector Cybersecurity Information Sharing,* February 13, 2015, *available at* https://obamawhitehouse.archives.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-shari.

providing services to federal agencies.

Illustrative of the number of overlapping and potentially conflicting requirements contractors currently face is the following inventory of ongoing regulatory actions:

- Department of Defense (DOD) Final Rule on Network Penetration and Contracting for Cloud Computing;
- DHS Safeguarding of Controlled Unclassified Information Proposed Rule;
- OMB's proposed guidance on cybersecurity protections;
- DHS Class Deviation 15-01 Safeguarding of Sensitive Information;
- NARA Safeguarding of Controlled Unclassified Information Final Rule;
- DOD, GSA and NASA Basic Safeguarding of Contracting Information Systems; and
- Anticipated Federal Acquisition Regulations (FAR) clauses on these topics (along with the fact that the FAR does not currently address the existing regime).

This complexity of cybersecurity regulations is burdensome not only to current contractors, but also to new entrants and small businesses.[29] In some cases, existing contractors are exiting the federal marketplace because of the regulatory compliance cost. For instance, small businesses' implementation of the DOD network penetration rule is burdensome and not affordable. Recently, DOD and DHS initiated efforts to reach out to Silicon Valley to explore ways for more non-traditional ICT companies to sell their products and services to the federal government.[30] Setting many complex and confusing rules can create an impediment for agencies to accomplish what DoD and DHS seek—small business and non-traditional players as federal government suppliers. In 2016 alone, approximately 7 rules were issued impacting contractors.[31]

We recommend that Congress direct OMB to develop guidance to create an efficient and effective cybersecurity acquisition infrastructure. OMB should harmonize cybersecurity regulations for federal agencies to ensure that they are applied consistently across the entire federal enterprise. Without such management, this array of new requirements, regulation, and guidance will add further confusion for the acquisition community, increase the compliance burden for both the government customer and the vendor community, and significantly increase costs to the taxpayer for the technology goods and services the government mission requires.

Finally, Congress should reform government acquisition procedures to allow for deployment of agile federal procurement processes to acquire cybersecurity products and services, and align corresponding guidance among agencies for consistent application across the government. The federal government procurement system cannot keep up or stay ahead of ever-growing cybersecurity threats. According to the *State of Federal IT Report,* "Agency CIOs sometimes

[29] https://www.crowell.com/files/Contractors-Caught%20in-the-Cyber-Minefields-More-Rules-and-Greater-Confusion-for-Public-Sector-Cybersecurity.pdf.
[30] DHS Silicon Valley Program, *available at* https://www.dhs.gov/science-and-technology/hsip; DoD Diux Program, *available at* https://www.diux.mil/.
[31] http://www.natlawreview.com/article/more-cybersecurity-changes-expected-contractors-2017.

anticipate that potential acquisitions will take up to two years to ultimately select a vendor. A result of this delay is that technologies that are considered state-of-the-art when a new procurement is envisioned are often outdated by the time a contract is awarded. The lengthy procurement process can also create significant barriers to improving the cybersecurity posture of an agency because of difficulties in rapidly procuring and deploying innovative, cutting-edge cybersecurity technologies."[32] We recommend Congress incentivize agencies to use more agile processes, such as those used in the private sector, to procure cybersecurity goods and services and harmonize all regulations with which contractors must comply.

Conclusion

The ICT industry is constantly innovating and is committed to facilitating the protection of our customers, including governments, businesses, and consumers. Security is essential to the federal government mission and should no longer be treated and addressed in a patchwork, uncoordinated fashion. Allowing the furtherance of uncoordinated security approaches will simply perpetuate a security regime that is only as strong as the weakest link. This committee's oversight of cybersecurity regulation harmonization will be critical to developing effective and efficient cybersecurity policies for the federal government, particularly our critical infrastructure, which, in turn, will impact the private sector.

We stand ready to provide you any additional input and assistance in our collaborative efforts to develop balanced policy approaches that help all of us to collectively improve cybersecurity risk management and resilience while avoiding duplicative and costly regulations.

I thank the chairman, ranking member, and members of the committee for inviting me to testify today and for their interest in and examination of this important issue. I look forward to your questions.

Thank you.

[32] State of Federal IT Report, pg. 120, January 2017.

Testimony of Daniel Nutkis
CEO of HITRUST Alliance
Before the U.S. Senate Committee on
Homeland Security & Governmental Affairs
Hearing entitled: "Cybersecurity Regulation Harmonization"
June 21, 2017

Prepared for Submission

Chairman Johnson, Ranking Member McCaskill, and Members of the Committee, I am pleased to appear today to discuss the health industry's experiences in engaging with government agencies relating to cybersecurity regulatory harmonization and efforts we believe will provide the greatest benefit to industry. I am Daniel Nutkis, CEO and Founder of the Health Information Trust Alliance, or HITRUST. HITRUST was founded in 2007, after industry recognized the need to formally and collaboratively address information privacy and security for healthcare stakeholders representing all segments of the industry and organizational sizes. HITRUST endeavored—and continues to endeavor—to elevate the level of information protection in the healthcare industry and its collaborators, especially between industry and government. Our goal is to raise the competency level of information security professionals while maintaining trust with consumers and patients regarding their health information, and to promote cyber resilience for industry organizations.

In my testimony today, I will highlight three areas where cybersecurity regulatory harmonization should occur to reduce redundancy, unnecessary expense and delays to better support the private sector in defending against cyber threats, thereby improving cyber resilience and the management of cyber risk. First is the area of information sharing. Second is the role of government as a partner. And third is the role of government as a regulator.

1. Information Sharing

In 2010, HITRUST established a mechanism to share Indicators of Compromise (or IOCs) and other cyber threat information with organizations of varying cyber maturity. HITRUST has led the industry in the collection and distribution of cyber threat information through the development of enhanced standards and collection practices, it has published numerous reports on its progress, it continues to evaluate its effectiveness, and it continually innovates to support organizations in managing their cyber threats.

From the beginning, HITRUST participated with the Department of Homeland Security's Cyber Information Sharing and Collaboration Program (CISCP). Prior to 2015, when Executive Order 13691 was issued, HITRUST engaged with DHS to become an Information Sharing and Analysis Organization (ISAO) per the guidance provided in the Executive Order. The Order outlines the role of ISAOs in supporting information sharing to a sector or segment and how to engage with DHS to support the goals of the Order. Additionally, when DHS established a

mechanism to improve information sharing with an automated system, we were the first healthcare organization to begin sharing bi-directionally with the DHS' Automated Indicator Sharing (AIS) program.

As an ISAO, we have worked with the DHS's National Cybersecurity and Communications Integrations Center (NCCIC) as a conduit for coordination and additional information on cyber threats. HITRUST was an early supporter of the Cybersecurity Act of 2015 (CISA), allowing additional liability protections to be granted when sharing with the Departments of Homeland Security, Commerce, Defense, Energy, Justice, Treasury, and the Office of the Director of National Intelligence. We have always approached the role of an ISAO as a partner of both industry and government and believed that we were operating in a partnership towards a common goal as we understood our roles and expectations based on the Executive Order and other guidance.

We were then surprised to learn that the Department of Health and Human Services (HHS) recently established its healthcare-specific cybersecurity communication center to focus its efforts on analyzing and disseminating cyberthreats across the healthcare industry.

HHS states that the Healthcare Cybersecurity and Communications Integrations Center (HCCIC) intends to: (1) strengthen engagement across HHS Operating Divisions; (2) strengthen reporting and increase awareness of the healthcare cyber threats across the HHS enterprise; and (3) enhance public-private partnerships through regular engagement and outreach. The HCCIC intends to help organizations by sharing information and best practices around cyber threats and mitigation techniques.

While we agree these are important objectives, we believe it raises some important issues, as it appears the role of the HCCIC parallels the intended role and capabilities of ISAOs. Clear guidance and communication should be established to ensure private sector activities are supported and not duplicated by government programs.

We recognize that there is a large role for government to play in supporting information sharing and ensuring liability protection. We continue to support the role of government in fostering transparency by establishing guidance that clarifies roles and responsibilities and encourages industries and communities of interest to determine how to engage with information sharing organizations based on their applicability, level of performance and overall value.

There is a significant level of effort required for organizations like HITRUST to engage in cyber information sharing programs with the government. Though we anonymize the information shared to protect the contributing organization, the process requires soliciting buy-in, gaining approvals and amending agreements from its thousands of constituents questioning the value, liability and effort to participate in these programs. We undertake these efforts because we see the value in the program and partnership with government and believe we are all operating towards a common goal. More can and should be done to ensure the roles of industry and government are clearly defined when it comes to information sharing.

2. Government as a Partner

HITRUST values its government partners and recognizes the burden, responsibility and authority beholden on them to protect the private sector. However, we would expect in areas where the private sector has made a significant investment in establishing an effective program or approach, the government would give it due consideration before seeking a government alternative that replicates or devalues industry efforts.

Last year, the Health and Public Health (HPH) Sector Coordinating Council (SCC) and Government Coordinating Council (GCC), with input from HITRUST and other sector members including the DHS Critical Infrastructure Cyber Community (C3), developed the Health Sector implementation guide for the NIST Cybersecurity Framework, specifically referred to as the "*Healthcare Sector Cybersecurity Framework Implementation Guide*".[1] This *Implementation Guide* is listed on the US-CERT website identifying multiple sector-specific guidance for NIST CSF implementation.

The Health Sector Guide supports implementation of a sound cybersecurity program that addresses the five core functions of the NIST Cybersecurity Framework to ensure alignment with national standards, help organizations assess and improve their level of cyber resiliency, and provide suggestions on how to link cybersecurity with other information security and privacy risk management activities in the Healthcare Sector. The Healthcare Sector leverages the HITRUST risk management framework, including the HITRUST CSF and CSF Assurance Program, to effectively provide the Sector's implementation of the NIST Cybersecurity Framework.

This guidance continues to be updated and enhanced to ensure greater applicability and ease of adoption through the efforts of the Joint (SCC/GCC) HPH Cybersecurity Working Group. Yet despite the significant public and private effort that went into its publication, HHS is working towards the development of yet another healthcare-based implementation guide of the NIST Cybersecurity Framework despite the broad adoption of the existing guidance by private sector organizations that have already made the effort to leverage existing marketplace resources.

As recent as last year, after careful deliberation, the Department of Labor's ERISA Advisory Council published "*Cybersecurity Considerations for Benefit Plans*" recommending that Retirement Plans consider following existing privacy and security frameworks available through organizations such as HITRUST.

We state these points in an effort to highlight that not only is the HITRUST CSF already the most widely accepted cyber resilience framework in healthcare with tens of thousands of organizations having adopted it, it also has support in other areas of government as well as other industries. Additionally, we have developed a CSF BASICs program, which is a streamlined version of the HITRUST CSF, designed to help small and lower-risk organizations meet otherwise difficult regulatory and risk management requirements.

---

[1] See https://www.us-cert.gov/ccubedvp/cybersecurity-framework, and https://www.us-cert.gov/sites/default/files/c3vp/framework_guidance/HPH_Framework_Implementation_Guidance.pdf.

HITRUST has been collaborating with industry for over 10 years and has an advisory council to ensure we are meeting the needs of the entire industry. This council has representatives from many of the leading healthcare membership organizations representing hospitals, health plans, medical practices and physician groups.

We are perplexed as to why HHS would not partner with industry by leveraging programs already in place and offering assistance to improve them instead of replicating and dismissing the hard work of industry. We would ask that Congress require federal agencies to give due consideration to existing standards and best practices already in place before developing new ones.

3. Government as a Regulator

The Department of Health and Human Services is responsible for overseeing the implementation of the Health Insurance Portability and Accountability Act or HIPAA, and the HHS Office for Civil Rights (OCR) is responsible for assessing compliance with and enforcement of the HIPAA Privacy, Security and Breach Notification Rules, including issuance of civil and criminal penalties.

In support of their role, they conduct annual random audits that are designed to "enhance industry awareness of compliance obligations and enable OCR to better target technical assistance regarding problems identified through the audits. Through the information gleaned from the audits, OCR will develop tools and guidance to assist the industry in compliance self-evaluation and in preventing breaches."[2]

There is no question that organizations, both large and small, that create, store or transmit protected health information need to comply with the HIPAA regulations, and that the HIPAA Security Rule outlines a number of actions organizations must take including implementing appropriate security controls based on their risk assessments. Further, it is clear that HHS is responsible for enforcement of the HIPAA Security Rule.

While the mission of OCR is noble, and one that we recognize as required, we have documented that these random audits are in fact causing organizations to divert their attention and resources from enhancing their information protection programs based on the potential for random audits. Said differently, organizations that have, in fact, implemented appropriate and effective information security programs are diverting resources to focus on preparing for a random OCR audit rather than investing those resources on additional cyber defense or resilience programs.

We also recognize that this is not the case across the healthcare industry. Take the recent WannaCry incident, where vulnerabilities were exploited by cyber threat actors using ransomware impacting organizations that did not appropriately implement security controls such

[2] See https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/phase2announcement/index.html?language=es

as patching, end point protection and the necessary network segmentation of devices and systems.

At the same time, there are many organizations that have implemented a comprehensive security framework, such as the HITRUST CSF, performed a risk assessment, engaged in cyber information sharing and are complying with the HIPAA regulations that were not impacted by WannaCry.

Yet, under the current audit model, OCR is using its limited resources to audit organizations that have already implemented appropriate privacy and security controls and conducted required risk assessments, for which OCR has no visibility. OCR resources could be better served in focusing on organizations not adequately addressing the HIPAA privacy and security requirements.

We propose that policy makers consider a system whereby organizations that can demonstrate a comprehensive information security program that complies with the privacy and security provisions of HIPAA can receive some form of safe harbor or similar relief, and focus HIPAA audits on those organizations that cannot demonstrate their compliance in meeting the criteria. As noted above, the Sector has done a tremendous amount of work, and there are a number additional industry-led initiatives that should be leveraged to incentivize industry to do the right thing, make the necessary investments and protect their environments.

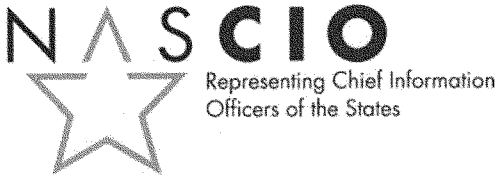
We are advocating that guidelines be established to enable organizations to communicate that they have obtained a comprehensive assessment covering the HIPAA Privacy and Security Rules, such as a HITRUST CSF Assessment, and that they be excluded from random OCR HIPAA privacy and security audits.

This approach would create cost savings to industry by not having to prepare for unnecessary government audits, and save government resources by not using tax payer dollars to assess organizations that can already demonstrate compliance. The approach would likely increase compliance by providing greater incentives for organizations to comply with the privacy and security provisions of HIPAA and allowing OCR to target resources towards organizations not complying with the privacy and security provisions of HIPAA.

HITRUST is currently conducting a study that will substantiate and communicate the approach and benefits outlined above, which we hope to complete in the next 90 days. I look forward to updating the Committee on the results.

I hope my testimony illuminated a number of areas where individual activities may seem innocuous, but in totality begin to create confusion and concern. I have highlighted where additional clarity in regulation and guidance will ensure the private sector understands how to best engage with government and also the complex issues that arise when a regulator is partnering with industry.

Thank you again for the opportunity to join you today and share these insights. I look forward to your questions.



Statement before the Senate Homeland Security and Governmental Affairs Committee

"Cybersecurity Regulation Harmonization"

Testimony of James "Bo" Reese

Vice President, National Association of State Chief Information Officers (NASCIO) & Chief Information Officer, Office of Management and Enterprise Services Information Services, State of Oklahoma

June 21, 2017

Chairman Johnson, Ranking Member McCaskill, and members of the committee, thank you for inviting me to testify before you today on federal data security regulations and their impact to state governments.

My name is James "Bo" Reese, and I serve as the chief information officer (CIO) for the State of Oklahoma. In Oklahoma, I lead Information Services, a division of the Office of Management and Enterprise Services (OMES), with the mission of partnering "with State of Oklahoma agencies and affiliates to deliver quality, cost effective and secure IT services." I also serve as the vice president of the National Association of State Chief Information Officers (NASCIO).

NASCIO is a nonprofit, 501(c)(3) association representing state chief information officers and information technology (IT) executives and managers from the states, territories, and the District of Columbia. State chief information officers (CIOs) are governor-appointed, executive branch officials who serve as business leaders and advisors of information technology policy and implementation at the state level. All states have a CIO and all CIOs serve the executive branch of state government. The state CIO role takes many forms, some are cabinet officials and others are executive directors; regardless of the title, state CIOs share the common function of setting and implementing a state's IT policy.

Today, I would like to provide the committee an overview of how federal data security regulations impact our work to introduce efficiencies and generate savings for state taxpayers. I will also touch upon how the complex federal regulatory environment is duplicative in nature, contributes to inconsistent federal audits, and drives cybersecurity investments based on compliance and not risk, which is the more secure approach.

IT Consolidation/Optimization Produces Efficiencies and Savings for Taxpayers

As the technology solutions provider for state executive branch agencies, state CIOs aim to operate IT infrastructure as if state government were one, unified enterprise. In doing so, state CIOs seek to maximize efficiency and leverage economies of scale where possible; this results in savings for state government and ultimately the taxpayer. Because of these known benefits, IT consolidation/optimization remains a top priority for state CIOs across the country. Indeed, every year for the past ten years, IT consolidation/optimization has appeared in the top three on the annual NASCIO Top Ten Priority list.

Regarding the IT consolidation effort in my state, the Oklahoma Legislature passed the Oklahoma Information Services Act[1] in 2009, which created the position of chief information officer. It also mandated an assessment of technology and telecommunications assets and services. The 2009 study found:

- An inability to leverage buying power across state government.
- The over-provisioning of IT infrastructure and human capital resources as each agency incorporated its surge capacity into its design and procurement.
- Expensive integration requirements to share data across agencies.

[1] https://legiscan.com/OK/text/HB1170/2010

- Significant risks due to a lack of maturity in basic processes including, backup, fault tolerance and disaster recovery.

The assessment's findings accurately reflected the pre-consolidated IT environment during which the state was supporting 76 financial systems, 22 unique time and attendance systems, 17 different imaging systems, 48 reporting and analytics applications, and 30 data center locations. To address these inefficiencies, the Oklahoma Legislature passed and the governor signed the Information Technology Consolidation and Coordination Act of 2011, which charged the Oklahoma Office of Management and Enterprise Services (OMES) with increasing the effectiveness and efficiency of the state's technology services. The law's legislative intent was to:

- Reform and consolidate the IT structure, operations and purchasing procedures of the state to ensure that state government promotes and encourages private sector growth in a competitive global economy;
- Move state government forward with respect to electronic purchasing, billing and payment services, and other transactions, to ensure that the state delivers essential public services to its citizens in the most efficient manner at the lowest possible cost to taxpayers;
- Streamline and consolidate systems for financial and administrative services, with particular emphasis on combining the 76 financial systems, 22 unique employee time and record-keeping systems, 17 types of document imaging systems, 30 data center locations and 129 electronic mail and smart phone services used by the state; and
- Coordinate and require central approval of state agency IT purchases and projects to enable the chief information officer to assess the needs and capabilities of state agencies.

Over the past five years, OMES has reduced redundancies, made large strides to unifying technology, and completed consolidation of the 72 of the 78 mandated[2] state agencies and more than 30 voluntary agencies. Consolidation has resulted in $283 million of estimated reduced spending and projected savings. To complete the legislative mandate, OMES Information Services will consolidate the remaining mandated agencies by the end of FY 2017. While we are well on our way to achieving the goals set by our legislature, one of the biggest hurdles in achieving this vision has been compliance with federal data security regulations.

STATE CIOS MUST COMPLY WITH VOLUMINOUS FEDERAL DATA SECURITY REGULATIONS

I have described how we have approached consolidation/optimization in Oklahoma and would also like to give you the national perspective. As previously mentioned, state CIOs aim to operate the state government IT environment as a unified, single entity or "enterprise." The efficiencies and financial savings achieved by streamlining or consolidating the state's IT

[2] A "mandated" agency can be understood as a state agency that receives appropriations from the state. "Voluntary" agencies are those that are self-funded and do not receive state appropriations such as various boards and commissions.

environment are obfuscated by complex, disjointed, federal data security regulations that were issued in a de-centralized and "siloed" fashion.

State CIOs support the mission of state agencies and the federal programs they administer with technology and are rarely, if ever, the direct recipients of federal funds or grants. Because state CIOs deliver enterprise IT services to state agencies that administer federal programs or receive federal funds or grants, state CIOs and the larger IT enterprise must also comply with and abide by federal data security regulations that are imposed on those state agencies. Thus, state CIOs find themselves operating in an increasingly complex regulatory environment driven by disjointed federal regulations. Below are some of the federal data security regulations with which state executive branch agencies and thus the state CIO must comply:

- Internal Revenue Service (IRS) Publication 1075
- FBI Criminal Justice Information Services Security Policy (FBI-CJIS)
- Health Insurance Portability and Accountability Act (HIPAA)
- Office of Child Support Enforcement security requirements[3]
- CMS Minimum Acceptable Risk Standards for Exchanges (MARS-E)
- Electronic Information Exchange Security Requirements and Procedures for State and Local Agencies Exchanging Electronic Information with the Social Security Administration (SSA)
- U.S. Department of Labor - State Quality Service Plan: Agency Assurances
- 42 CFR part 2 - Substance Abuse and Mental Health Services Administration
- Family Educational Rights and Privacy Act (FERPA)
- Gramm Leach Bliley Act
- Child Internet Protection Act of 2000
- Child Online Privacy Protection Rule of 2000

In addition to various federal regulations, state CIOs are also pushed to adopt other standards and frameworks that contracts and federal grants necessitate:

- NIST and FIPS standards (e.g. NIST 800-53 Revision 4)
- NIST Cybersecurity Framework
- NIST Risk Management Framework
- SANS and CIS Top 20 Controls
- Federal Information Security Management Act[4]
- Control Objectives for Information and Related Technologies (COBIT)
- ISO/ISE 27000 Series
- Payment Card Industry Data Security Standard (PCI-DSS)

---

[3] 45 CFR §307.5 Mandatory computerized support enforcement systems.

[4] FISMA applies to federal agencies and "organizations operating 'on behalf of' federal agencies. Determining whether FISMA applies to state agencies is complicated and while OMB has issued guidance clarifying FISMA's scope, which could include state governments, OMB guidance is unclear on when potential entities are acting "on behalf of an agency" and thus subject to FISMA. Many state CIOs comply in an abundance of caution.

While compliance with these regulations can be onerous, state governments and state CIOs understand, appreciate, and share the goal to which these regulations strive: protecting citizen data. From the cradle to the grave, state governments record, retain, and secure data related to all aspects of an individual's life; birth and death certificates, driver's licenses, voting registrations, professional licensing, health data, prison records – these are just some of the everyday data points that state governments must record, retain, *and* protect.

State CIOs invest an inordinate amount of time identifying duplicative regulatory mandates or their differences, participating in federal audits, and responding to inconsistent audit findings. These challenges in and of themselves are not unmanageable; the real issue is that they can and have impeded efforts of state CIOs to introduce efficiencies and generate savings for taxpayers.

REGULATORY SIMILARITIES ARE NOT RECOGNIZED IN THE FEDERAL DATA SECURITY AUDIT PROCESS AND RESULT IN DUPLICATIVE OR INCONSISTENT COMPLIANCE EFFORTS

Many federal data security regulations are similar in organization and substance; data security regulations generally address five common categories: physical safeguards, access controls, awareness and training, disaster recovery, and technical network and system requirements. Federal data security regulations are also similar in that the information that they seek to protect is usually varying levels of "high-risk" data such as federal tax information or health information. However, while data security regulations may share similarities, the federal audit process does not recognize regulatory similarities and puts the state CIO in the position of responding to the same compliance questions for multiple federal auditing entities. This results in an inefficient use of scant state personnel and financial resources.

To illustrate the issue of duplicative audits – in Oklahoma, the IRS audited one state agency twice because it viewed two programmatic elements of the agency as separate entities. My office had to answer questions, attend meetings, and deliver additional explanatory material twice for one state agency because it was seen as two by IRS auditors. Additionally, the audit findings were inconsistent; one audit team had a finding and the other did not, despite only one IT environment being the subject of both audits.

For more illustrations and perspectives from state chief information security officers (CISO) on the federal data security audit processes, please see the attachment.

REGULATORY CONFLICT HINDERS REALIZATION OF IT CONSOLIDATION/OPTIMIZATION BENEFITS

Complicating matters, differences in regulatory policy or regulatory conflict can also impact IT consolidation/optimization efforts negatively. As previously mentioned, federal data security regulations typically address cybersecurity in five common fronts and again, the substance of regulatory mandates can be quite similar. Because of existing overlap and similarities among the different federal data security regulations, even a seemingly minor difference can obscure the goal of IT consolidation/optimization which aims to streamline IT applications and simplify the enterprise IT environment to produce savings for taxpayers.

One example of regulatory conflict is reflected in different standards regarding breach or incident notification. The IRS requires incident notification within 24 hours[5] and the Centers for Medicare and Medicaid Services (CMS) requires notification of a breach "without unreasonable delay."[6] Both tax information and health information are considered high-risk data points and should be treated similarly, again, based on the level of risk and not compliance requirements.

Another example of regulatory conflict involves session lock out, or the time that a computer will block access after periods of inactivity. IRS Publication 1075 requires that session lock out occur after 15 minutes of inactivity; FBI-CJIS regulations require session lock out at 30 minutes. While a 15-minute difference may seem insignificant to the casual observer, in practice this means that the state CIO must configure the enterprise IT environment two different ways for data of similar risk. These kinds of regulatory conflicts introduce unnecessary complexity to state IT and hampers IT consolidation efforts.

INCONSISTENT FEDERAL AUDITS DRIVE STATE CYBERSECURITY INVESTMENTS BASED ON COMPLIANCE AND NOT RISK WHICH RESULTS IN A LESS SECURE POSTURE

When federal data security audits are conducted and produce "findings" of a critical nature, state CIOs must direct their attention and resources to remediating and addressing those "findings" to satisfy federal auditors and avoid any potential negative impact to citizens. This approach is problematic for state government cybersecurity because it encourages state CIOs to make check-the-box compliance investments instead of ones based on *risk,* which is the more secure approach[7] to managing sensitive data.

As states plan for IT consolidation, they will phase out old, less secure technology and schedule their replacement, as IT consolidation is usually a multi-year process. A federal data security audit can be very disruptive to IT consolidation because audit findings of a critical nature must be addressed within a very short period of time that may not align with the state's IT consolidation schedule. Put another way, federal data security auditors can impose their view of the state's risk without the ability to consider the state's comprehensive enterprise risk assessment or schedule for system upgrades.

STATE CIOS STAND READY TO WORK WITH OUR FEDERAL PARTNERS TO HARMONIZE REGULATORY POLICIES AND NORMALIZE THE AUDIT PROCESS

Like our federal partners, state CIOs are acutely aware of the risk inherent in sharing sensitive data. Likewise, we appreciate efforts by the federal government to secure and protect sensitive citizen information because we also share that responsibility at the state level. But, we must accomplish our shared goal without overly burdening state governments, ensuring that we are

[5] https://www.irs.gov/uac/reporting-improper-inspections-or-disclosures

[6] https://www.cms.gov/Research-Statistics-Data-and-Systems/Computer-Data-and-Systems/Privacy/Privacy_Data_Breach.html

[7] "A comprehensive risk management approach provides the ability to identify, assess, respond to, and monitor cybersecurity-related risks and provide organizations with the information to make ongoing risk-based decisions." NIST Cybersecurity Framework, page 3.

delivering government services to citizens in the most efficient and cost-effective manner. In recognition of that shared mission and responsibility, we want to work with our federal government partners to harmonize disparate regulatory requirements and normalize the audit process.

On behalf of our nation's state CIOs, I want to thank the Committee for addressing this issue and inviting NASCIO to share our perspective with you.

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

Attachment

Statements Regarding and Examples of Inconsistent Federal Data Security Regulation and Audit Practices

ARKANSAS

The IRS has onerous requirements that do not contemplate cost and lack a policy justification. The IRS decided that if someone is using a VoIP phone, any phone call containing a discussion of FTI must be recorded and kept for seven years. The storage requirements, alone for this, are huge.

With the recent change from functional audits to IT audits there has not been a corresponding change/upgrade in the technical expertise on the IRS' part. Usually, when addressing a finding, it involves a conference call with the IRS and their technical contractor. When questioned, the contractor does not want to disagree with the IRS, so the state is left with little actual guidance. This contributes to our problems with mitigation.

Frank Andrews, CISO, State of Arkansas

DELAWARE

Federal security regulation pain points include inflexibility from federal auditors. We scheduled a 5 day visit but went home early due to a snow storm forecast. We had a number of documents that were "internal review only" documents; not to be taken offsite. 2-3 months later, those federal auditors picked things up and asked for the internal documents to be emailed. We said no and offered 3 options; they asked again for the internal documents (sensitive) to be emailed. This issue is still unresolved.

Elayne Starkey, CISO, State of Delaware

ILLINOIS

In Illinois, we encounter multiple IRS audits that ask the same questions across five separate agencies. There is also a lack of consistency on certain controls such as encryption rules, password rests, and now background checks. FBI-CJIS has clear guidance and standards on the types of individuals/entities that that must obtain a background check and the access to which they are privileged but IRS Publication 1075 merely states that personnel that have access to federal tax information (FTI) must be fingerprinted but includes no guidance on standards.

The continuous cycle of auditors focusing on different regulations creates an extreme burden on the states. Since each auditing unit requires testing by auditors, weeks if not months of personnel hours are wasted simply repeating the same tasks for each audit event.

Kirk Lonbom, CISO, State of Illinois

COMMONWEALTH OF KENTUCKY

We have 3 agencies (Cabinet for Health and Family Services, Department of Juvenile Justice, and Department of Workforce Investment) that receive Social Security Administration (SSA) data and 4 that receive IRS data (the three mentioned plus the Department of Revenue). This is for the most part all the same data, but is distributed under 7 unique need and use agreements. As such, we have 7 agency level audits for each need and use agreement and 1 additional specific to IT as the state transmission center (STC) for a total of 8 audits for common data, all operating under the same controls and infrastructure.

For the Commonwealth, the core challenge that we encounter is the overlap between all audit and attestation processes related to federal compliance. Even having established responses that can be recycled over and across these audits take considerable time and resources. As an example, we are audited across 4 agencies for the IRS and 3 for the SSA. This is single source data from a common federal repository. Where 1 compliance review would suffice, I have to respond to 7. Adding these to the other requirements within our environment, we respond to 23 to 26 audits annually diverting resources, time, and investment from matters that provide meaningful risk reduction across our infrastructure as a whole.

David Carter, CISO, Commonwealth of Kentucky

LOUISIANA

A clear example of the significant inconsistencies we face with federal audits/assessments/reviews is illustrated in our most recent onsite IRS assessment performed January 2017. Five Louisiana state agencies were assessed by five separate IRS assessors **all auditing the same exact statewide Information Security Policy** with the following breaking down of findings (right).

Findings	
Agency #1	**32**
Agency #2	**27**
Agency #3	**23**
Agency #4	**14**
Agency #5	**11**

As you can see, consistency is lacking and the agencies were audited with the same exact federal regulation.

Dustin Glover, CISO, Louisiana

MAINE

Overview:

1. The complexity of regulatory audit, and the duplication of requirements and reporting from different regulators, represent thousands of hours of opportunity cost. For instance, the State of Maine spent over 2,500 hours on the Social Security Administration audit alone.
2. Redundancy between different regulatory reporting requirements is common, with many questions asking for the same information, but worded slightly differently. We calculate that over 50%of the questions cover the same topics: Cybersecurity, Disaster Recovery, Admin Rights Monitoring, Access Monitoring, etc.

3. The regulatory oversight spans across multiple Federal agencies. Simplifying and combining similar regulatory requirements will enable States to greatly reduce the hours spent addressing compliance.

Regulatory Impact & Burden:

The State of Maine regulatory landscape includes 6 Federal agencies.

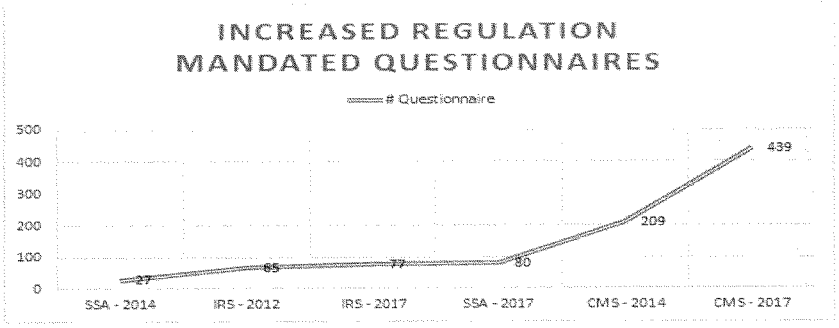
1. The State must analyze over 1,000 pages of Federal audit questionnaire.
2. The single source document for almost all the questions/mandates is the National Institute of Standards and Technology (NIST) Security Controls.

#	Regulatory Agency	State Resources	Total Hours
1	Internal Revenue Service (IRS)	12+	4,000
2	Social Security Administration (SSA)	4+	2,500
3	U.S. Treasury	1	60
4	Health Portability and Accountability Act (HIPAA)	6+	800
5	Criminal Justice Information Service (CJIS)	3+	800
6	Centers for Medicare and Medicaid Services (CMS)	12+	3,000
Total			**11,160**

Published Regulatory Mandate Documents	
Federal Regulatory Publication	**# of pages**
IRS Publication 1075	180
SSA TSSR	85
U.S. Treasury (NIST SP 800-47 & FISMA)	74
HIPAA (Security Rule, plus 6 additional documents)	155
Centers for Medicare and Medicaid Services CMS) (Harmonized Security and Privacy Framework, Minimum Acceptable Risk Standards, Catalog of Security and Privacy Controls, AE ACA SSP)	534
Total	**1028**

Historical Overview of Increasing Regulations:

This graph plots the growth in the number of questions over the last 3 years.



Examples of Duplicate Reports:
Often, the same report must be filed with the same regulatory agency, but on behalf of different State agencies, and sometimes, bureaus within the same agency. For instance, DHHS-DSER, DHHS-OFI, DOL, and MRS all have to file the very same report with the Internal Revenue Service. Maine is spending hundreds of hours reviewing and completing such duplicate reports.

Example of Duplicated Regulatory Deliverables		
Federal Agency	**#**	**Regulatory Deliverable**
Internal Revenue Service	4	Safeguard Security Reports
	4	Corrective Action Plans
SSA	4	Compliance Review Questionnaires

Examples of Duplicated Questions Worded Differently:

#	Internal Revenue Service	Social Security Administration
1	Describe how the agency maintains and disseminates to designated agency officials: A) An identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. Please include details regarding policy review/update.	Does the agency have a published password policy for user of systems and/or applications that receives, processes and stores Social Security provided information?
2	Describe how the agency manages information system authenticators (or passwords). Describe how the agency implements the following authenticator	Does the security software package impose and enforce limitations on password repetition (i.e., will not permit usage of the same password within a specified number of password

	requirements: A) Enforces non-privileged account passwords to be changed at least every 90 days. B) Enforces privileged account passwords to be changed at least every 60 days. C) Prohibits password reuse for 24 generations.	expiration cycles?

Suggested approach to the issue (reduce the over-11,000 person-hours required to complete the audits today):

1. Required reporting for the six Federal agencies could be consolidated and streamlined for similar topics: Ask the question once; Not six times, in slightly different language.
2. Federal agencies could agree on a standardized reporting mechanism that satisfies the needs of all the Federal Agency stakeholders.
3. In addition to the standardized questions, there could be a sub-section in which each Federal agency could ask their specific questions.

Victor Chakravarty, Associate Chief Information Officer, Infrastructure, State of Maine

MONTANA

The State of Montana experiences roughly 9 federal audits every year; the audits cover IRS Publication 1075, Social Security Administration (SSA) requirements, and FBI-CJIS. They all have different requirements related to records retention, passwords, encryption, and physical security. Our largest pain point is the number of audits with different requirements and the need to address each one individually.

We have also experienced inconsistent audits as well as the inflexibility of mitigation efforts that clearly protect the data, but do not "check the box." One other item that is very frustrating is that when we are connecting with some Federal agencies like SSA, we request them to connect in a manner that meets their requirements i.e. through secured connectivity - VPN, but they cannot do it themselves because of cost, resource, or some other limitation.

It is very concerning to me how much money is being spent to complete all of these audits when one audit with consistent requirements could be completed for all Federal agencies.

Lynne Pizzini, CISO and Deputy CIO, State of Montana

NORTH CAROLINA

Issue 1: In addition to IRS engaging 3 different agencies in NC on differing schedules, the IRS findings, when remediated on the same infrastructure are not being closed out consistently. Recommend: Engage once, close once. Provide one Corrective Action Plan (CAP). Federal agencies should agree on the use of a Governance, risk management, and compliance (GRC)

solution to manage CAPs or Plan of Action and Milestones (POAMs); could be similar to U.S. Department of Defense's Enterprise Mission Assurance Support Service (eMASS).

Issue 2: Inconsistent approach to the implementation of security controls and acceptance of compensating controls implemented. Federal agencies tend to interpret their own definition of the controls which can increase cost for implementation. As a result, the North Carolina Department of Revenue (which is subject to IRS Publication 1075) has created a separate on premises email and other stand-alone solutions (as opposed to utilizing central IT services) to meet the "intent" of IRS 1075.

Recommend: Agencies that regulate any sensitive data type should adopt a common framework and add specific details on intended end result. Federal agencies should also review the changing landscape and update control requirements to be more adaptive.

Maria Thompson, CISO, State of North Carolina

WEST VIRGINIA

In my state, we have to spend scarce funding on services to map all federal regulations and requirements together to make them somewhat manageable. We spend valuable human capital and scarce funding to process multiple audits for the same federal regulation such as IRS Publication 1075. This creates complications in drafting and managing local security policy with zero flexibility. The federal approach is not based on risk management but rather "checkbox security" which forces the state to expend funds on low risk issues instead of a high-risk issue to maintain compliance.

I use human capital (i.e. Full Time Equivalents FTE) and scarce funding to manage multiple frameworks. If federal agencies were on the same page, those resources could be used more effectively to improve the state's security posture.

Also, consider FEDRAMP. It was designed so that vendors could provide cloud services with a trusted (3rd party) audit of the security. Why not use the same approach for the relationship between the states and federal agencies? One audit provides the mechanisms by which federal agencies have assurance in security and states have the flexibility to apply a risk management (as opposed to a compliance-based approach).

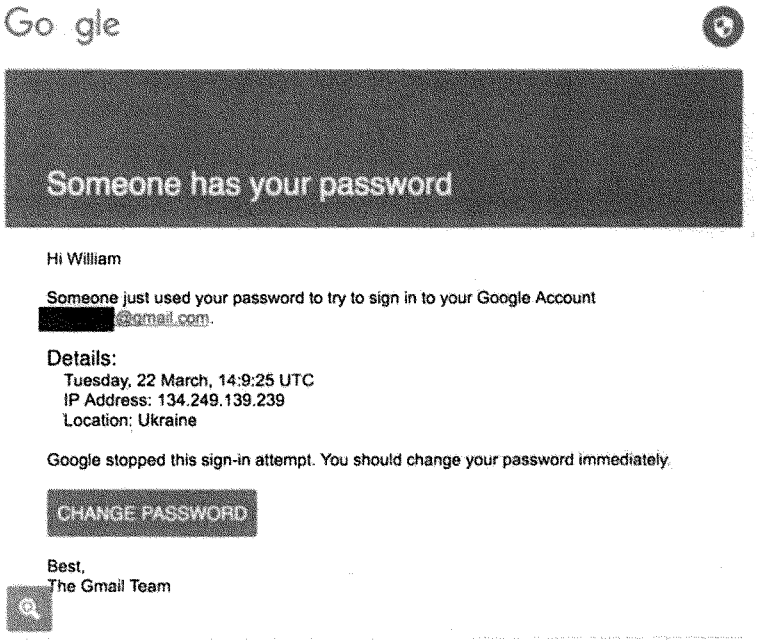
Josh Spence, CISO, State of West Virginia

WISCONSIN

Varying log retention requirements are difficult and costly to maintain. The worst is a 7-year audit trail retention requirement from the IRS. Realistically, what is the value of a 7-year-old log?

In addition to the cost of duplicative audits to the states, there would be a savings at the Federal level if they made one combined audit per State.

Bill Nash, CISO, State of Wisconsin



A screenshot of the phishing email that Billy Rinehart clicked on, unknowingly giving Russian hackers access to his account. The New York Times has redacted Mr. Rinehart's email address.

From: The Perfect Weapon: How Russian Cyberpower Invaded the US. New York Times, Dec. 13, 2016

August 4, 2017

Via electronic submission to: Laura_Kilbride@hsgac.senate.gov

The Honorable Ron Johnson
Committee on Homeland Security and Governmental Affairs
Washington, DC 20510

Dear Chairman Johnson:

Thank you again for the opportunity to testify on June 21, 2017 before your committee at the hearing titled "Cybersecurity Regulation Harmonization." I appreciate the opportunity to respond to the following questions for the record submitted by your colleagues:

Questions from Senator John McCain

Currently, the United States government does not have a clear cyber strategy or policy. In your testimony you stated, "Congress plays an important role in encouraging agencies to meet with the private sector in order to achieve regulatory harmonization. In order to foster this collaboration, we encourage this Committee to recommend that agencies pause any in-process cybersecurity related proposals, rule makings, or other formal activities to allow time for effective collaboration."

1. *Last year the Pentagon stated they received 10 million cyber hacks per day, the longer we go without a clear cyber strategy and policy we are only making ourselves more susceptible and vulnerable for these types of attacks to persist. In your opinion, what are your recommendations on how to move forward in building a strategy in order to protect our national security?*

As the financial sector has learned, the overarching elements of an effective cyber strategy must include public-private collaboration, cross-industry dialogue, the application of advanced technology and effective operational rigor, a harmonized and consistent approach to regulation, and support of a vibrant cyber workforce.

The federal government has taken steps to build a comprehensive cyber strategy through efforts such as Presidential Policy Directive 21 (PPD-21) and successive National Infrastructure Protection Plans (NIPP), which identified the 16 sectors of the economy that provide essential services underpinning American society as "critical infrastructure". PPD-21 and the NIPP also provided a plan for advancing security and resiliency through public-private collaboration. Financial services is one of the identified sectors, with the U.S. Department of Treasury tasked as our sector-specific agency. Collectively we work with the industry, cyber experts at Treasury and other relevant federal agencies such as the Department of Homeland Security to ensure coordination between critical infrastructure sectors and the federal government. These concerted efforts are critical to making progress and an effective way to achieve our shared goal of strengthening the security and resiliency of the economy and protecting American

citizens. Approaches like this, which recognize and embrace the interconnectedness of our economy, are critical pieces of a national cybersecurity strategic foundation.

The Financial sector specifically has worked for years to develop an all-encompassing approach to cybersecurity. For example, our sector recognized early the importance of CEO engagement and the value of establishing an Information Sharing and Analysis Center (i.e., the FS-ISAC), which now has approximately 7,000 financial institution members, ranging from large to small firms. In addition, we continue to pursue coordinative efforts with our government and industry partners through such entities as the Financial Services Sector Coordinating Council (FSSCC, which facilitates coordination amongst industry stakeholders) and the Financial and Banking Information Infrastructure Committee (FBIIC, which facilitates coordination amongst financial regulators). These two bodies meet independently and jointly with frequency. To help set priorities and financial industry action plans, FSR-BITS is also hosting the 10th Joint Trade Associations Cybersecurity Summit in September, with both public and private participation.

My testimony hopefully made clear that the financial sector is faced with a unique set of challenges as it relates to achieving a harmonized regulatory cyber strategy. Having nine federal regulators and all state banking, insurance and securities regulators pursuing different regulatory approaches is incompatible with your efforts to pursue a clear set of cyber policies.

2. *Do you agree that the current state of our government is inadequate given the cyber challenges we face and that dramatic changes are essential to better posture us to address these challenges?*

First, as it relates to the financial sector, I agree that the current approach to cyber regulation is in need of change. The current environment of jurisdictional "turf battles" and regulatory "one-upsmanship" has resulted in a regulatory landscape that can demand upwards of 40% of our cyber professionals' time to interpret and untangle the various requirements that are notionally similar, but semantically different. This lack of a harmonized regulatory approach reallocates already scarce resources to administrative efforts that could otherwise be utilized to protect platforms and secure the financial sector.

Second, as it relates to the federal government itself, it has the opportunity to lead by example. Regulatory agencies, such as those that regulate the financial services sector, collect and maintain significant amounts of sensitive data. However, analyses of agency security controls indicate that cybersecurity remains a challenge at the federal level[1], with agencies exhibiting weakness in basic information security controls such as limitation on employees' ability to copy and remove sensitive information. President Trump's Executive Order 13800 – "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure" is a good first step in assuring proper cyber risk management by elevating this responsibility and accountability to the agency head level and requiring agencies to identify gaps in policy and operational practices. Agencies could take another step forward by

[1] See, for example, GAO report titled "FDIC Implemented Controls over Financial Systems, but further Improvements are Needed," http://www.gao.gov/assets/680/678084.pdf.

embracing security principles, such as those required of financial firms, in areas of governance, chief information security officer reporting to agency heads, data protection and data loss prevention.

Questions from Senator Claire McCaskill

Impact Regulations Have on Rural Communities
Smaller financial institutions, such as community banks, face added challenges when it comes to navigating compliance with numerous federal and state regulations.

1. *While there is certainly work to be done to streamline the current set of cybersecurity compliance requirements facing all financial institutions, are there specific ways that we can help smaller institutions?*

The financial services sector recognized years ago that in an interconnected system, the cybersecurity posture of all firms matters regardless of size. While the compliance burdens on more sophisticated and geographically dispersed financial institutions are generally greater, so are the larger firms' resources and their ability to hire and retain experienced personnel. As a result, smaller firms are faced with even greater challenges in hiring cyber professionals capable of not only maintaining an information security program, but reconciling varying regulatory regimes.

Thus, as I called for in my written testimony, harmonizing cybersecurity regulations to a customized version of the NIST Cybersecurity Framework (a financial "sector profile") would significantly benefit depository institutions of all sizes.

To accomplish this, a risk-tiered "sector profile," tailored to a firm's size, product offerings and complexity, would more effectively focus resources where the need is greatest and align a firm's cyber programs to its risks. As the NIST Cybersecurity Framework emerges as a de facto framework across all other sectors, a regulatory regime that embraces this framework would enable smaller firms to more effectively obtain needed services - such as mobile banking or payments applications from a larger universe of third parties, including technology innovators who utilize NIST. Without access to such services, smaller firms risk falling behind in providing consumer-expected technologies and services.

NIST Cybersecurity Framework
A common theme amongst industry, states, and the Federal government is the importance of the NIST Cybersecurity Framework. If every sector is going to effectively mitigate risk and prepare for cyberattacks everyone needs to be speaking the same language. You testified that since the release of the NIST Cybersecurity Framework, many regulations still do not fully comply with NIST language.

1. *Do you have suggestions on actions NIST should take to continue supporting the financial sector and government to increase cybersecurity?*

The National Institute of Standards and Technology (NIST) continues to be an outstanding partner and collaborator with multiple sectors and specifically the financial sector. FSR-BITS and our members regularly engage with NIST staff on a variety of ongoing projects in both consultative and collaborative ways. Two recent examples of this include their open and multi-stakeholder efforts to update the current version of the NIST Cybersecurity Framework and NIST's support for the development of a financial sector profile. NIST is a critical component of the federal government's cyber activities, and is a leader in promoting public-private collaboration. Their ability to gather input from a broad range of subject matter experts, cyber engineers and operators has been instrumental in fostering wide-spread adoption of its final framework. A similar effort that includes the regulatory community and industry would be an effective method to achieve these goals.

To ensure NIST continues to support efforts of the financial sector and government to strengthen our cyber capabilities, it is critical to provide NIST with the proper resources needed to pursue its mission. The Administration's proposed budget for FY 2018 calls for numerous concerning cuts to NIST. I am hard-pressed to point to another federal department that has done more to help the private sector and government enhance cybersecurity than NIST. As such I would strongly encourage you and your colleagues to ensure the agency is adequately funded to support today's cybersecurity efforts and to ensure continuation of cybersecurity research and development efforts that are critical to our future.

Central Clearinghouse for Cyber-related Regulations

1. *Do you think the Federal government should have a central clearinghouse to harmonize cyber-related regulations and if so, what would that position or office look like if you were designing it?*

The financial services sector is unique in how it is structured for regulatory oversight. As described in my submitted testimony, "[t]he sector is overseen by nine federal regulators, three self-regulatory organizations, the U.S. Department of the Treasury as its sector-specific agency, and every state banking, insurance, and securities agency."

Through the course of their work, agency examiners develop a deep understanding of the financial industry and the institutions they are examining and can more adeptly identify areas of cyber risk, gaps on process, and where improvements can be made. In fact, depending on the size and complexity of the financial institution, agency examiners can have permanent workspace within the examined institution from which they can conduct their work. Disrupting these relationships, and specifically the in-depth knowledge that these agency examiners develop through their field experience, could have an opposite effect and introduce negative cybersecurity consequences.

These relationships could be maintained and harmonization more readily achieved if, as your question suggests, the agencies were required to come together through a clearinghouse or a council-like mechanism to develop cyber-related standards. Such a requirement could: assure a more singular organizational approach; drive commonality of language, meaning and intent; improve the examination process overall and; lead to improved data accuracy and comprehension of the "state of the state" in cyber. Accordingly, freed from reconciling different approaches and language, cyber professionals would be able to devote more time to security activity and substantially reduce time on non-additive

compliance. As I referenced earlier, the U.S. Treasury Department is well situated as the financial industry's lead agency and could be an effective convener and potential body for this effort.

* * * * *

Thank you for considering our views. If you have any questions or would like to discuss further, please feel free to contact me.

Christopher F. Feeney
BITS President
Financial Services Roundtable/BITS
600 13th Street, NW
Suite 400
Washington, DC 20005
Chris.Feeney@FSRoundtable.org

Post-Hearing Questions for the Record
Submitted to Dean Garfield
From Senator John McCain

"Cybersecurity Regulation Harmonization"
June 21, 2017

In your testimony, you state the United States should continue to lead the way in promoting the adoption of industry-led, voluntary, globally recognized cybersecurity standards and best practices that avoid country-specific requirements.

- What are your recommendations for constructing a cybersecurity policy that is held to international standards?

Response:

Cybersecurity is rightly a priority for governments around the world, including the United States government (USG). Our members are global companies, doing business in countries around the world, and we share a common goal with all governments of improving cybersecurity. Most of our companies service the global market via complex supply chains in which products are developed, made, and assembled in multiple countries, servicing customers that typically span the full range of global industry sectors, including banking, telecommunications, energy and healthcare, as well as government customers. As a result, we acutely understand the impact of governments' policies on security innovation and the need for U.S. policies to be compatible with – and drive – global norms, as well as the potential impacts on our customers. As both producers and users of cybersecurity products and services, our members have extensive experience working with governments around the world on cybersecurity policy. In the technology industry and other global industry sectors, when discussing any cybersecurity policy, it is important to consider our connectedness, which is truly global and borderless.

The visionary work led by NIST, in cooperation with the private sector and other stakeholders, to develop the voluntary *Framework for Improving Critical Infrastructure Cybersecurity* (the *Framework*) is an example of the type of cybersecurity policy approach that should not be abandoned by U.S. administrations, but rather should be the basis for domestic cybersecurity policy as well as the policies of other countries. The *Framework* leverages public-private partnerships, is grounded in sound risk management principles, and helps foster innovation due to its flexibility and basis in global standards. The *Framework* has also consistently been lauded for providing a common language to better help organizations comprehend, communicate and manage cybersecurity risks across the globe.

The *Framework's* mapping to international standards such as ISO/IEC 27001 is helpful, as such standards help organizations establish an immediate linkage between their ongoing risk management and certification efforts. This type of mapping provides an extremely persuasive example to share with governments outside of the United States that may be considering their own national cybersecurity frameworks/initiatives. By mapping the *Framework's* security guidance to global standards, the *Framework* demonstrates that national cybersecurity concerns can be addressed in a manner that both protects U.S. security and bolsters global standards.

- You recognize that Italy, Israel, and the UK have incorporated or developed their own version of the Framework into their cybersecurity guidelines. What are your recommendations on implementing and enforcing similar guidelines that are globally recognized?

Response:

To facilitate further global adoption, NIST and its Federal agency partners should promote the *Framework* approach with their global government partners. For example, the Department of State should reference the *Framework* in all its global cybersecurity capacity-building efforts. Likewise, the White House should highlight the *Framework* in its strategic cybersecurity partnerships. International acceptance of industry-led, global cybersecurity standards will help drive even greater competition and innovation in the global marketplace.

NIST should also consider other mechanisms by which to expand the *Framework* approach. For example, given the increasing global acceptance of the *Framework*, we would support NIST exploring, with industry stakeholders, the opportunity for submitting the *Framework* as an international standard. This could be a valuable contribution to further harmonizing cybersecurity practices on a global scale. Today more than 80 countries are in the process of creating new cybersecurity regulations and there are myriad implementing requirements being considered. Adding the *Framework* as an international standard could help propagate a standards-based approach globally.

Outreach to international audiences, including the sharing of best practices, should also be significantly enhanced. It is particularly important that foreign governments who are carefully watching the *Framework's* development better understand its approach. Many governments around the globe are at pivotal points in their own cybersecurity policymaking—examples include the EU's Network and Information Security (NIS) Directive, which must be implemented by all 28 EU member states over the next 18 months, and cybersecurity policies and laws at different stages of development across Asia and Latin America. However, many foreign governments and audiences outside the U.S. generally still do not understand the *Framework's* voluntary, risk management approach or its rationale, and mistakenly believe NIST is writing new standards for the U.S. economy. Thus, international outreach that focuses on the facts underlying the *Framework* and the approach it embodies will continue to be essential. Conducting such outreach in local languages (e.g. with the assistance of our Embassies abroad) would be extremely helpful.

The global ICT industry is heavily invested in developing standards to address important challenges in security management. We urge the USG to continue taking a leadership role in promoting the adoption of industry-led, voluntary, globally recognized cybersecurity standards and best practices, to make the preservation and promotion of a global market a primary goal in any product assurance requirements, and avoid country-specific requirements. We also welcome and encourage all governments to participate in standards development activities, particularly in private fora and consortia.

The USG might also consider greater action in their own (public sector) use of voluntary, globally accepted standards or generally accepted industry practices for cybersecurity risk management. Indeed, government leadership can demonstrate such standards' importance and may be necessary to overcome economic disincentives to adoption of standards that yield benefits to the entire network. We applaud the USG for continuing to invest in global standards development (via the International Standardization Strategy). However, it is worth noting the purpose of furthering international cybersecurity standards is not for governments to turn around and mandate their adoption. From ITI's perspective, any effort to mandate minimum security standards is problematic, in that it is difficult for a minimum-security standards approach to allow for the flexibility for best security practices to evolve as technology advances, or to fully consider the necessary risk management processes at the heart of cybersecurity. ITI thus strongly cautions governments not to set compulsory security standards for the commercial market– whether they are standards vendors must follow as they build their products or services, or standards that would guide consumers when purchasing ICT products and services or conducting business with companies. Such an approach could encourage some firms to invest only in meeting static standards or best practices that are outmoded before they can even be published or cause others to divert scarce resources away from areas requiring greater investment towards lower priority areas. To maintain (rather than restrain) innovation and to prevent the development of single points of failure, any standards should be purely indicative, their use entirely voluntary, and should always allow organizations to adopt alternative solutions. Defining new, country-centric standards has many downsides as such insular standards may conflict with global standards currently in use, interfering with global interoperability.

Post-Hearing Questions for the Record
Submitted to Dean Garfield
From Senator Claire McCaskill

"Cybersecurity Regulation Harmonization"

June 21, 2017

NIST Cybersecurity Framework

A common theme amongst industry, states, and the Federal government is the importance of the NIST Cybersecurity Framework. If every sector is going to effectively mitigate risk and prepare for cyberattacks everyone needs to be speaking the same language.

1. Do you have suggestions on actions NIST should take to continue supporting the financial sector and government to increase cybersecurity?

Response:

We have several suggestions regarding how NIST can support increased cybersecurity across both the financial sector and the USG at-large.

Orient Financial Sector Cybersecurity Approaches around the Cybersecurity Framework. The visionary work led by NIST, in cooperation with the private sector and other stakeholders, including those from the financial sector, to develop the *voluntary Framework for Improving Critical Infrastructure Cybersecurity* (the "*Framework*") should anchor any federal financial agencies' efforts to help financial institutions better manage cybersecurity risk and avoid systemic consequences of those risks, rather than serving as just another layer of inspiration.

The *Framework* leverages public-private partnerships, is grounded in consensus risk management principles, and helps foster innovation due to its flexibility and basis in global standards, including ISO 27001. The *Framework* has also consistently been lauded for providing a common language to better help organizations comprehend, communicate and manage cybersecurity risks, including by other financial sector agencies including the Securities and Exchange Commission (SEC) and Federal Financial Institutions Examination Council (FFIEC).

Financial sector regulators have in recent years indicated that they are considering a prescriptive approach to cybersecurity, including contemplating "regulations that impose specific cyber risk management standards" (*See* Advanced Notice of Proposed Rulemaking jointly issued by the Board of Governors of the Federal Reserve System, Office of the Comptroller of Currency, and Federal Deposit Insurance Corporation regarding Enhanced Cyber Risk Management Standards (ANPR)). Amongst other things, the proposed "regulation would include details on the specific objectives and practices a firm would be required to achieve in each area of concern in order to demonstrate that its cyber risk management program can adapt to changes in a firm's operations and to the evolving cyber environment." (ANPR 45). These proposed requirements contradict existing cybersecurity public policy - such as that embedded in the *Framework* and much of the other guidance cited in the ANPR - that risk management is a continuous process demanding

flexibility to provide reasonable protections that consider the nature and scope of the activities of a given company, including the sensitivity of the data it handles, its threat profile, and the size and complexity of the relevant data operations of the company.

In our view, establishing standards through policy statements and/or guidance is far superior to establishing a rigid regulatory regime, as already illustrated by much of the foregoing. This is particularly the case where the contemplated standards are prescriptive, inflexible, and misaligned with both industry approaches and federal cybersecurity policies.

From ITI's perspective, any effort to mandate minimum security standards is problematic, in that it is difficult for a minimum standards approach to allow for the flexibility for best security practices to evolve as technology advances, or to fully account for the necessary risk management processes at the heart of cybersecurity. ITI thus routinely cautions all governments not to set compulsory security standards for the commercial market – whether they are standards vendors must follow as they build their products or services, or standards that would guide consumers when purchasing ICT products and services or conducting business with companies. Such an approach could encourage some firms to invest only in meeting static standards or best practices that are outmoded before they can even be published or cause organizations to divert scarce resources away from areas requiring greater investment towards areas with lower priority.

To maintain (rather than restrain) innovation and to prevent the development of single points of failure, any standards should be purely indicative, their use entirely voluntary, and they should allow organizations to adopt alternative solutions. Defining new, financial sector specific standards has many downsides as they may conflict with global standards currently in use, interfering with global interoperability. The more resources institutions are required to spend on compliance activities, the less resources they will have available to identify threats to critical assets, and to protect, detect, respond and recover from cybersecurity threats. As stated above, we recommend efforts to reduce redundancy across existing regulations, rather than the creation of new regulations.

In our view, orienting financial sector risk management efforts around the *Framework* represents a superior approach. The *Framework* has already helped and will continue to help improve cybersecurity, and it has had and continues to have an important, valuable impact on organizations' understanding of cyber risks.

Streamline Existing Financial Sector Cybersecurity Regulatory Efforts to avoid Duplicative Requirements. While the *Framework* has frequently been cited as providing a common language which can help companies better communicate risk management to improve cybersecurity internally (for instance with company executives or boards) and externally across their ecosystems (such as with business partners including suppliers), the *Framework* also provides a common language that the federal agencies themselves can leverage. The potential of the *Framework* to provide a common language or taxonomy for policymakers has clearly not yet been fully realized. Promoting the *Framework* as a common language for policymakers can help align the federal agencies' cybersecurity and risk management efforts by orienting them around a common point, and we urge federal agencies to use the *Framework* as such a cyber risk reference

point. The recently issued Executive Order embraces this concept; NIST can help further advance it.

As NIST pointed out in the *Framework* document, "Executive Order [13636] called for the development of a voluntary, risk-based Framework – a set of industry standards and best practices to manage cybersecurity risks." That is exactly what NIST produced, with significant input from industry, in the *Framework*, and we do not suggest that NIST or other stakeholders lose sight of the inherent "voluntariness" of the *Framework*, or stop promoting it as such. However, this is not to say that we should ignore the reality that government policymakers and regulators, including the financial agencies as acknowledged in the ANPR, are increasingly looking to the *Framework* for inspiration as they consider whether and how to exercise their regulatory authorities to help improve cybersecurity.

We believe more can and should be done to reinforce the *Framework* as voluntary, while at the same time embracing its sensible use by regulators such as financial agencies to streamline and on a net basis reduce cybersecurity regulations. How can we accomplish this? The key is that the *Framework* should not serve as the impetus or rationale for extra layers of regulation, as apparently was the case in the ANPR and other recent federal efforts. That's not regulatory streamlining, it's regulatory redundancy, and multiple layers of redundant regulations will not create better cybersecurity for anyone, including regulated entities themselves. Rather, the *Framework* can still be held up as a voluntary risk-management based tool, while also serving as a beacon around which policymakers at every level – including federal financial agencies – should orient their efforts to improve cybersecurity. Doing so will help reduce regulatory redundancy, thus making it easier for financial services institutions to manage cybersecurity risk. NIST is well-positioned to help advance such a streamlining effort across the federal government.

NIST Should Continue to Act as a "Convener" of Private Sector and Other Stakeholders and Help Build on Public-Private Partnerships to Improve Cybersecurity. There has been significant progress on cybersecurity policy development in the U.S. over the past few years, notably EO 13636 that launched the *Framework*, set up a process to designate Critical Infrastructure at Greatest Risk, and directed the streamlining of federal agencies' regulations. These new initiatives complement well-established public-private partnership activities, and, together the public and private sector, have just begun implementing and utilizing many of these policy instruments. ITI believes it is pivotal to continue to replicate this partnership approach in addressing cybersecurity challenges. The NIST *Framework* provides an overarching structure, grounded in proven international standards and consensus best practices, to address organizational security across all critical infrastructure sectors, while providing adaptability and flexibility to meet the unique needs of each sector and address new threats. The US Government at large and the financial sector and other agencies specifically can provide leadership to make certain that efforts to improve cybersecurity leverage public-private partnerships and build upon existing initiatives and resource commitments. The IT industry, along with our peers in other industry sectors including the financial sector, leads and contributes to a range of significant public-private partnerships, including information sharing, analysis, and emergency response with governments and industry peers. Two key examples of public-private partnerships the government can prioritize to ensure greater coordination and collaboration across the

government and industry are information sharing and analysis centers (ISACs), and sector coordinating councils (SCCs). Perhaps federal agencies can establish a process with DHS and impacted private sector stakeholders to more fully examine the sufficiency of the CIAGR designations that have already been made, and to determine whether there is utility in doing more work of this sort in the finance sector, from a risk management standpoint.

NIST and Other Agencies Should Prioritize Helping SMBs Use the Framework. Federal agencies should work with interagency partners including NIST, the Department of Homeland Security (DHS), the Small Business Administration, and others to better understand the cybersecurity and implementation challenges faced by organizations of all sizes, and consider ways to make the *Framework* more approachable for all organizations across the financial sector.

Not all companies have mature programs or the technical expertise to keep up with the latest developments in cybersecurity – such as the *Framework* – to appropriately manage cyber risk. SMBs, in particular, have reported being confused and even overwhelmed by the size and complexity of the current *Framework*. Given the interconnected nature of the cyber ecosystem, we are keenly aware that cyber elements of the critical infrastructure can be compromised by weaknesses in smaller entities to which they are technologically connected. Given this fact, it is critical for us to create a sustainably secure cyber ecosystem for all entities, large and small.

Prioritize Investment in Cybersecurity Workforce Development and Training. The ANPR contemplates several requirements that will necessarily require the hiring of personnel with deep cybersecurity risk management expertise. However, there is currently a demonstrable shortfall of qualified cybersecurity experts in the U.S. Federal agencies should work with federal and industry partners to prioritize paying down the "cyber debt" and reversing the current cybersecurity talent shortage. We recommend that the USG expand initiatives like the CyberCorps Reserve program and stand up a Cyber National Guard to train and recruit new talent to protect public and private digital infrastructure, and we urge the federal agencies to consider lending their support to such initiatives.

Central Clearinghouse for Cyber-Related Regulations

2. Do you think the Federal government should have a central clearinghouse to harmonize cyber-related regulations and if so, what would office look like if you were designing it?

Response:

In 2017, we find our sector and the cybersecurity policy ecosystem at large at an inflection point. While cybersecurity is now acknowledged as a critical priority by government and industry stakeholders alike, the near universal recognition of the problem is spurring often divergent initiatives from policymakers across the USG (as well as at the state and local government level). Unfortunately, these well-intentioned policymaking efforts to address cybersecurity challenges are often uncoordinated, raising the specter of not only siloed but also often prescriptive regulatory proposals, which are increasingly calling for the premature development and implementation of cybersecurity measures or metrics that favor compliance-based cybersecurity models and are disconnected from any clear cybersecurity benefit.

Policy leadership is needed now more than ever to navigate these cybersecurity policy challenges. In our view, reconciling the multiple and often divergent cybersecurity policy efforts across the USG is becoming an increasingly urgent need. Having achieved widespread cybersecurity awareness, seemingly every federal agency is examining a separate piece of the cybersecurity puzzle through its own lens, often developing their own guidance and/or prescriptive requirements, and leading to an overall cybersecurity approach more reminiscent of a patchwork than a coordinated strategy.

A good illustrative example of this problem involves the multiple approaches to addressing Internet of Things (IoT) security currently gaining traction across the USG. It is counterproductive to create siloed approaches to cybersecurity across variegated IT applications simply because more and more "things" become connected to the internet in an increasingly digitized world. Indeed, to fully realize the benefits offered by the IoT and innovations such as Big Data Analytics, the USG should promote policies that help break down barriers to connecting devices and correlating data. Efforts to improve IoT cybersecurity should leverage public-private partnerships and build upon existing initiatives and resource commitments.

We do not believe it is productive to elevate form over substance on this point – in other words, what is most important is that the federal government acknowledges the need for a coordinated approach to streamlining regulations, and sufficiently empowers a coordination point to ensure that such streamlining occurs. Whether an existing agency, department, or office is so designated and authorized to spearhead a regulatory streamlining effort to rationalize not only IoT security initiatives but also for broader USG cybersecurity regulatory efforts, or a new body is created to do so, what is most important is that the task gets done. ITI would be happy to engage in a process with Congress to help identify the best mechanism for achieving this important task.

Post-Hearing Questions for the Record
Submitted to Dean Garfield
From Senator Jon Tester

Homeland Security and Governmental Affairs Hearing: "Cybersecurity Regulation Harmonization"
June 21, 2017

1) Can you give us a general picture of how IT consolidation and optimization looks across the United States? What other states are good examples of IT consolidation and optimization? Which ones have room for improvement?

Response:

Overall IT consolidation provides a great deal of benefit when it comes to security. Having one central agency that has visibility across and within state agencies can help align security practices with industry recognized standards and frameworks. The complex security functions protecting a state should be prioritized in a centralized location that quickly and uniformly adapts to the changing security threat.

In Ohio, the Department of Administrative Services has undergone a significant consolidation effort that has saved the state over $103 million. Centralization allows for agencies to focus on their primary mission as opposed to information security functions. This also naturally provides for an increased cybersecurity posture within the state, saves significant taxpayer dollars, and increases overall agency performance.

For example, the Oregon Legislature, with the support of Governor Kate Brown, recently passed S.B. 90, cybersecurity legislation that centralizes IT functions. S.B. 90 unifies agency information technology security functions within the executive branch under the supervision of the State Chief Information Officer. It is widely believed that this move will help to further secure the state's IT systems under a uniform set of standards that are universally recognized by both government and industry.

2) You are aware of the challenges facing the federal government to both hire and retain cybersecurity professionals. Are states facing similar challenges? Have any states come up with novel or successful practices prevent shortfalls in cybersecurity professionals?

Response:

The private sector, federal, state, and municipal governments have realized the vital importance of cybersecurity professionals, but that realization has created a near-term shortage of workers that requires long-term solutions. States have been hit particularly hard by an increased demand for cybersecurity professionals compounded by an inability to provide competitive wages and are often plagued by issues of retention. Many states have entered a period of fiscal austerity which provides less flexibility when it comes to offering competitive retirement incentives and other

appealing benefits to the younger demographic needed to fill these positions. A recent report by the National Association of State Chief Information Officers points to uncompetitive pay, a shortage of qualified candidates, and slow hiring processes are among the reasons for the increased demand for cybersecurity professionals. Many states have begun to partner with universities through cybersecurity scholarship programs, enhance cybersecurity literacy, and develop partnerships with veterans and international cybersecurity professionals. Below you will find examples of states that are leading the way in cybersecurity professional development.

Congressional Proposal on State Cybersecurity Grant Funding— There is currently a bipartisan legislative effort underway to provide state cybersecurity resiliency funding led by Reps. Barbara Comstock (R-Va.) and Derek Kilmer (D-Wash.), along with Sens. Cory Gardner (R-Colo.) and Mark Warner (D-Va.). S. 516 and H.R. 1344, the *State Cyber Resiliency Act* (the *Act*), requires the Federal Emergency Management Agency to administer grants for cybersecurity planning and implementation. ITI believes this effort is long overdue and would bolster state and city cybersecurity defenses by providing much needed relief to states. The Act would also provide states and cities with the ability to hire additional cybersecurity professionals at some of the most vulnerable levels of government. ITI urges the Senate Homeland Security and Governmental Affairs Committee to advance this legislation swiftly.

Virginia Cybersecurity Public Service Scholarship— Recipients of the Virginia Cybersecurity Public Service Scholarship receive $20,000 a year for studying how to safeguard computer networks, data, and electronic resources. Students funded by the scholarship must agree to work in a Virginia state agency or institution for the number of years that they received the scholarship. Approximately 25 scholarships are awarded on a first-come, first-serve basis, depending on available funding. While the program is relatively small, the benefits of the effort will be noticeable in the long term, especially if the number of eligible scholarships increase over time.

National Integrated Cyber Education Research Center (NICERC)— NICERC was established to address the growing cyber threat and a critical shortage of cybersecurity professionals. NICERC works with K-12 students to build a stronger cybersecurity workforce by developing tools and curricula for educators to obtain and teach confidently in the classroom. The curricula developed by NICERC is free to any K-12 educator within the U.S. and comprises the Cyber Interstate, which is a robust library of cyber-based curricula that provides opportunities for students to become aware of cyber issues, engage in cyber education, and enter cyber career fields. Engaging the next generation is critical to providing a long-term solution to the cybersecurity talent shortage, and organizations like NICERC are important players in ensuring this development.

Maryland iCyberCenter— The Maryland Department of Commerce is establishing the iCyberCenter, which is a 12-month incubator program providing support to companies from the United Kingdom and other allied nations. The goal of the iCyberCenter is to help these companies establish a foothold in the U.S. market. It is anticipated that 10 to 15 companies will participate in the program annually, with a minimum of 100 permanent jobs created in

the U.S. over the next several years. Due to the overwhelming demand for cybersecurity talent, bringing innovative cybersecurity companies into states like Maryland is helping to solidify the U.S. as a thought leader and further the state's ability to gain access and knowledge from the private sector.

Post-Hearing Questions for the Record
Submitted to Daniel Nutkis
From Senator John McCain

"Cybersecurity Regulation Harmonization"
June 21, 2017

You recognized in your prepared remarks a need for government to play a large role in supporting information sharing and ensuring liability protection. You also stated that you are perplexed by the Department of Health and Human Services' unwillingness to partner with industry by leveraging programs already in place.

- What are your recommendations on how government could better support information sharing and ensuring liability protection?

Answer:
We recognize that there is a large role for government to play in supporting information sharing and ensuring liability protection. Our recommendations as to a role of government are 1) fostering transparency by establishing guidelines or other guidance that clarifies roles and responsibilities and encourages end users to determine how to engage with information sharing organizations based on their applicability, level of performance and overall value 2) government should be sensitive to the implications on the private sector from laws, regulations and Executive Orders and once in place should ensure they are consistently implemented across government, such as with exec order for ISAO sharing that established a model to create entities to share cyber threat information between DHS and their communities of interest, be it a sector, segment or other grouping of constituents. HHS in establishing their HCCIC sought to only engage with one which is inconsistent with PPD and confuses market and 3) Government should recognize that the only organization that doesn't benefit from information sharing is the organizations sharing information, therefore, liability protections doesn't act as much of an incentive for organizations to share cyber threat information, government should give consideration to what actual incentives could be.

There is a significant level of effort required for organizations like HITRUST to engage in cyber information sharing programs with the government. Though we anonymize the information shared to protect the contributing organization, the process requires soliciting buy-in, gaining approvals and amending agreements from its thousands of constituents questioning the value, liability and effort to participate in these programs. These efforts should not go unnoticed and should be encouraged. We also feel strongly that the Department of Homeland Security, through the NCCIC, should be the central hub for information sharing.

- What other implementations do you recommend by different governmental departments such as Department of Health and Human Services to better strengthen and harmonize cybersecurity regulation?

Answer:
The answer is simple, government should not duplicate efforts already underway with the private sector and in fact encourage the private sector to develop standards and best practices for cyber risk

management. The pace at which cyber threats evolve and the ability for the federal government to maintain the relevance of a cyber standard or best practice make industry the logical choice. The government's role should only be to offer assistance or fill a void where one exists. Time and time again, we see that government replicating industry efforts to make them their own. Requiring government to survey what is already present in the marketplace and encouraging industry before developing and implementing cyber regulation would be a worthy first step in each of this processes.

Post-Hearing Questions for the Record
Submitted to Bo Reese
From Senator John McCain

"Cybersecurity Regulation Harmonization"
June 21, 2017

Our greatest collective frustration has been the lack of any direction from this administration or the last on how we should be deterring our adversaries abroad and at home in cyberspace. Your testimony stated that inconsistent federal data security regulation and audit practices result in a less secure posture.

Question: What are the impediments to crafting a coherent strategy, is it lack of leadership or focus?

Answer:
The impediment to crafting a coherent cybersecurity strategy lies generally with the fact that there is a lack of recognition that cybersecurity poses a *business risk* to the continuity of government. However, State CIOs continue to lead the effort to develop and implement cybersecurity strategies within their sphere of influence within state government. There are obvious challenges to this effort and according to the 2016 Deloitte-NASCIO Cybersecurity Study, the top five challenges to addressing cybersecurity are:

- Lack of sufficient funding (80 percent)
- Inadequate availability of cybersecurity professionals (51 percent)
- Lack of documented processes (45 percent)
- Increasing sophistication of threats (45 percent)
- Lack of visibility and influence within the enterprise (33 percent)

These challenges have remained constant since the inception of the Deloitte-NASCIO Cybersecurity Study in 2012. From our 2016 study, we have learned that those states with a documented cybersecurity strategy command larger budgets and attract or build staff with the necessary competencies thus obviating some of the challenges listed above.

The majority of state governments have developed cybersecurity plans and are now focusing on implementing those plans and communicating its importance to other state government stakeholders. From NASCIO's 2016 State CIO Survey: The Adaptable State CIO, 72 percent of states report adopting a cybersecurity strategic plan and 94 percent of states have adopted a cybersecurity framework based on national standards and guidelines.

State CIOs have largely crafted a strategy for state governments and as state CIOs are implement the strategy, it would be helpful if our federal partners recognized the limited resources at our disposal and worked with state CIOs to prioritize security over check-the-box compliance.

Question: What are your proposals to ensure that inconsistent federal data security regulation and audit practices do not persist?

Answer:
Ultimately, we would like to work collectively with our federal partners to achieve harmonization across federal regulations and normalization of the federal audit process. The current system of disparate, disjointed federal regulations and the accompanying audit practice are ultimately unsustainable. Some ideas for improving the process and introducing efficiencies include:

- Establish a federal working group to review and harmonize disparate security regulations and consider more efficient processes to the federal audit process
- Auditing by state agency in lieu of auditing per data use/programmatic agreement
- Satisfying multiple agencies' audit requests via one audit with follow up visits from federal agencies with more specific requirements, similar to FedRAMP's "do once, use many times" approach
- Consistent application of compensating controls and acknowledgement of those controls across spectrum of federal auditors
- Require evaluation of existing regulations across federal agencies before issuing updates or new requirements

The potential solutions listed above are not exhaustive but would serve as a sufficient starting point to begin discussions with federal agencies that issue regulations and audit state agencies. We hope to engage with appropriate federal regulators and the Office of Information and Regulatory Affairs at the Office of Management and Budget to ensure a government-wide effort.

Question: What additional thoughts do you have on the continued failure to harmonize our cybersecurity regulations?

Answer:
We appreciate your and the Committee's interest in this topic. We aim to work with our federal partners to develop solutions that assures citizens of the safety of their information. However, the current system of disparate, disjointed federal regulations and their accompanying audit practices are ultimately unsustainable; compliance with federal regulations can be achieved much more efficiently. Again, we hope to work with regulating agencies, as we have begun to do through various NASCIO engagements, to collectively offer solutions that will make the compliance effort more efficient and cost-effective.

Post-Hearing Questions for the Record
Submitted to James Reese
From Senator Claire McCaskill

"Cybersecurity Regulation Harmonization"

June 21, 2017

IT Consolidation

The cost savings achieved by the consolidation of IT services in your state are impressive. Saving over $107 million since 2009 is no small feat.

1. What has been the biggest hurdle to achieving more costs savings and consolidation of IT efforts in your state?

Answer:
Federal cybersecurity regulations were and continue to be a barrier to IT consolidation because of duplication in some areas and conflicting policy in others. The auditing component that accompanies compliance has also proven to be a deterrent to the efficient operation of state government IT initiatives. The audit examples provided in our written testimony are a good reflection of how the audit process impedes the business of IT consolidation.

Specific to Oklahoma, we can share an additional example of how federal compliance audits have deterred the IT consolidation process. We were using a piece of hardware that was nearing end-of-life and because we planned to utilize it until its scheduled replacement (based on the IT consolidation schedule), we purchased extended maintenance to curb the risk that this product would pose. However, when federal auditors examined our systems, they penalized us for utilizing this hardware and mandated that it be replaced immediately, off-schedule. This is despite the fact that we had mitigated the risk by purchasing extended maintenance. Our IT consolidation schedule had to be altered based on the federal auditor's perception of our risk profile even though we had mitigated that risk.

Examples like ours and like those in our written testimony highlight the problem that state governments face regularly. We hope that we can have the Committee's and your support in resolving this issue.

Regulatory compliance appears to consume a large portion of your time and effort. Conflicting or duplicative regulations make it problematic to consolidate data centers.

2. What do you think the Federal government should be doing to alleviate the issues with conflicting and duplicative regulation?

Answer:
In moving forward, it would be helpful if federal agencies would review past regulations and not issue new ones without first identifying areas of harmonization within their agency and across other federal agencies. The federal government may also want to consider establishing a working group to study and focus attention on this issue.

Additionally, now that the Administrator for the Office of Information and Regulatory Affairs (OIRA) at the Office of Management and Budget has been confirmed, we would appreciate an opportunity to start a dialogue and work with OIRA on harmonizing federal cybersecurity regulations and normalizing the audit process. We believe that OIRA has sufficient authority to encourage federal adoption of a more efficient compliance process. We invite federal agencies to work with state CIOs to find solutions to the complicated and complex problem of harmonizing regulations and normalizing the audit process.

We would appreciate support and oversight from the Senate Homeland Security and Governmental Affairs Committee as we continue to advance solutions to address disparate cybersecurity regulations and their audits.

Post-Hearing Questions for the Record
Submitted to Bo Reese
From Senator Jon Tester

Homeland Security and Governmental Affairs Hearing: "Cybersecurity Regulation Harmonization"
June 21, 2017

1) Can you give us a general picture of how IT consolidation and optimization looks across the United States? Including Oklahoma, what other states are good examples of IT consolidation and optimization? Which ones have room for improvement?

Answer:
Every year, NASCIO conducts a survey of state CIOs to identify and prioritize the top policy and technology issues facing state government. IT consolidation/optimization has been included on NASCIO's "State CIO Top Ten Priorities" list every year in the past 10 years and has claimed a first, second, or third priority position in that 10–year window.

	2014				2016			
	DONE	ONGOING	PLANNED	DK/DNA	DONE	ONGOING	PLANNED	DK/DNA
Backup/disaster recovery	39%	47%	12%	2%	32%	52%	13%	3%
Business applications	17%	40%	13%	31%	15%	44%	13%	25%
Content management	18%	30%	26%	26%	21%	42%	13%	26%
Data centers	52%	40%	4%	4%	42%	47%	11%	0%
Desktop support	33%	31%	8%	29%	31%	37%	20%	12%
Email	65%	27%	8%	0%	59%	35%	6%	0%
Imaging	16%	35%	10%	39%	19%	42%	12%	27%
Security	44%	44%	6%	6%	31%	56%	9%	4%
Servers	43%	47%	4%	6%	31%	65%	4%	0%
Staff	33%	29%	4%	35%	29%	33%	15%	24%
Storage	41%	43%	4%	12%	35%	54%	11%	0%
Telecom	67%	27%	4%	2%	57%	35%	7%	0%
Helpdesk	NA	NA	NA	NA	38%	28%	17%	17%
Mobile device management	NA	NA	NA	NA	37%	30%	20%	13%
Identity and Access Management	NA	NA	NA	NA	30%	39%	26%	5%
Data Warehouse/ BI/ Analytics	NA	NA	NA	NA	8%	40%	30%	22%
Project Management Office	NA	NA	NA	NA	39%	30%	17%	15%
State Portal	NA	NA	NA	NA	48%	36%	9%	7%

As you can imagine, IT consolidation is difficult to implement and takes several years to achieve; it's also a continuous process. In Oklahoma, the effort has spanned five years and there is more work to complete. IT consolidation in other states tends also to be a multi-year effort and NASCIO data indicate that generally, consolidation efforts are increasing in a number of areas, most notably data centers, servers, security, and telecommunications (Note: the percentages from 2014 and 2016 may differ because survey respondents change from year to year and because the infrastructure subject to consolidation could also change).

State governments are constantly involved in IT consolidation projects and another great example of how savings were achieved for state taxpayers is reflected in Ohio's data consolidation effort.

In 2011, the state of Ohio embarked on the process of IT consolidation after studies found that the state's IT setup was fragmented and inefficient. The state was supporting more than 32 data centers spread across 26 Cabinet agencies, over 9,000 servers, and 19 different e-mail systems. The state realized that it was spending 70 percent of its IT spending on maintaining aging infrastructures rather than on citizen-facing applications.

Paramount to the IT consolidation strategy was the modernization of the state of Ohio Computing Center (SOCC) which was one of the largest data centers in the country but had not been updated in more than 20 years. The state of Ohio partners with IBM to modernize the SOCC and it is now serving as the primary data center for the state and the cornerstone of Ohio's private cloud.

Ultimately, the state of Ohio would realize a savings of over $100 million through IT consolidation/optimization. This figure does not include the money that state executive branch agencies have been able to save on planned infrastructure investments and reinvest in other projects. For example, Ohio's Department of Transportation was planning to invest $800,000 in its own email platform but by participating in the centralized email system, they were able to spend those funds on plows and other items they needed to serve the citizens of Ohio. Additionally, whereas the State used to spend approximately 70 percent of its IT budget on infrastructure and maintenance, now, approximately half of the IT budget is now focused on citizen-facing applications. A detailed writeup of the process in Ohio is available here.

2) You are aware of the challenges facing the federal government to both hire and retain cybersecurity professionals. Are states facing similar challenges? Have any states come up with novel or successful practices prevent shortfalls in cybersecurity professionals?

Answer:
Similar to the federal government, states are acutely aware of and are striving to mitigate the current and anticipated workforce shortage that will impact the business of state government. NASCIO's survey of 49 states "State IT Workforce: Facing Reality with Innovation," reveals that:

- Nearly 92 percent of states say salary rates and pay grade structures present a challenge in attracting and retaining IT talent

- 86 percent of states are having difficulty recruiting new employees to fill vacant IT positions
- 46 percent of states say that it is taking 3-5 months to fill senior level IT positions
- 66 percent of states report that the shortage of qualified candidates for state IT positions is hindering them from achieving strategic IT initiatives
- Security is the skill that presents the greatest challenge in attracting and retaining IT employees

In response to these challenges, several states are innovating in their approach to hiring IT personnel. In the State of Washington, nearly half of the government workforce is eligible to retire within the next five years. Compounding this reality is the fact that Washington state government competes for talent in a region that is home to "brand name" technology companies like Microsoft, Amazon, Disney, Apple and others. To combat these challenges Washington Technology Solutions (WaTech), the state's consolidated technology agency, implemented the "Technology Employer of Choice" initiative which employs a variety of methods to attract and retain technology talent, these include:

- Experimenting with self-management (Holacracy)
- Piloting physical space changes
- Reclassifying state government technology jobs
- Hiring for value alignment instead of skills
- Finding top talent in innovative ways including participation in local college and university curriculum boards and implementing a work-internship program

Though holacracy, which replaces traditional hierarchical governance with one that organizes work instead of people, WaTech employees report feeling more empowered and the organization made decisions and took action ten times faster. Harvard Business School, in partnership with the State, has launched an experiment to scientifically measure the difference between holacracy and traditional hierarchy.

WaTech is also finding top talent in innovative ways. WaTech's participation in local college and university curriculum boards ensure students are learning contemporary skills and practices. It also recruits through a work-internship program for students and veterans. 26 percent of interns are veterans and of 56 interns, 64 percent have become state technology employees.

Like WaTech, states are employing and developing innovative hiring practices and policies to hire much-needed IT and cybersecurity professionals. However, we also acknowledge the ongoing difficulties in achieving optimal levels of cybersecurity workforce within state government. We invite our federal partners to work with state CIOs to harmonize federal cyber regulations and normalize the audit process so that states can make more efficient use of existing human resources. We would also suggest continuation of successful federal programs like Scholarship for Service that can aid in filling gaps in the state cybersecurity workforce.